acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

31 October, 2014

Developer Report

Generated by Acunetix WVS Reporter (v9.0 Build 20140422)

Scan of http://testaspnet.vulnweb.com:80/

Scan details

Scan information	
Start time	31/10/2014 13:23:47
Finish time	31/10/2014 13:30:11
Scan time	6 minutes, 24 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Microsoft-IIS/6.0
Server OS	Windows
Server technologies	ASP.NET

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	**52**
High	20
Medium	13
Low	7
Informational	12

Knowledge base

List of file extensions

File extensions can provide information on what technologies are being used on this website.
List of file extensions detected:

- aspx => 9 file(s)
- css => 4 file(s)
- html => 1 file(s)
- dll => 2 file(s)
- bak => 1 file(s)
- pdb => 1 file(s)
- js => 9 file(s)
- htm => 1 file(s)
- txt => 3 file(s)
- rnd => 1 file(s)
- cs => 14 file(s)
- csproj => 2 file(s)
- webinfo => 2 file(s)
- resx => 12 file(s)
- asax => 1 file(s)
- ascx => 2 file(s)
- config => 1 file(s)

Top 10 response times

The files listed below had the slowest response times measured during the crawling process. The average response time for this site was 411.10 ms. These files could be targetted in denial of service attacks.

1. /comments.aspx, response time 5812 ms

```
GET /comments.aspx?id=2 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63
Safari/537.36
Accept: */*
```

2. /readnews.aspx, response time 3859 ms

```
GET /readnews.aspx?id=0&NewsAd=ads/def.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63
Safari/537.36
Accept: */*
```

3. /about.aspx, response time 984 ms

```
POST /about.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/about.aspx
Content-Length: 953
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63
Safari/537.36
Accept: */*

__EVENTARGUMENT=&__EVENTTARGET=&__EVENTVALIDATION=/wEWVwKNioOoAwLxkKSLCQLbp9qKDAKok6/
oDAKok6/oDAKok8OMBAKok8OMBAKok/ejDQKok/ejDQKok%2bvGBgKok%2bvGBgKok9%2bvAwKok9%2bvAwKok/PC
DAKok/PCDAKNut3rDwKNut3rDwKNuvGOBwKNuvGOBwKNuuUlAo265SUCjbqZ%2bAkCjbqZ%2bAkCjbqNnwECjbqNn
wECjbqhsgoCjbqhsgoCjbrV1gMCjbrV1gMCjbrJ7QwCjbrJ7QwCjbq91QkCjbq91QkCjbrR6QICjbrR6QICwNmQngcCwNm
QngcCwNmENQLA2YQ1AsDZuMgJAsDZuMgJAsDZrO8CAsDZrO8CAsDZwIMKAsDZwIMKAsDZ9KYDAsDZ
```

List of files with inputs

These files have at least one input (GET or POST).

- / - 1 inputs
- /default.aspx - 3 inputs
- /about.aspx - 1 inputs
- /login.aspx - 1 inputs
- /signup.aspx - 1 inputs
- /readnews.aspx - 4 inputs
- /comments.aspx - 2 inputs

List of external hosts

These hosts were linked from this website but they were not scanned because they are not listed in the list of hosts allowed.(Settings->Scanners settings->Scanner->List of hosts allowed).

- www.acunetix.com

Alerts summary

Blind SQL Injection

Affects	Variation
/comments.aspx	3
/login.aspx	1
/readnews.aspx	3

Cross site scripting (verified)

Affects	Variation
/comments.aspx	1
/readnews.aspx	2

Microsoft IIS tilde directory enumeration

Affects	Variation
/images	1

SQL injection (verified)

Affects	Variation
/comments.aspx	3
/login.aspx	1
/readnews.aspx	4

Unicode transformation issues

Affects	Variation
/comments.aspx	1

ASP.NET error message

Affects	Variation
Web Server	1

Cross frame scripting

Affects	Variation
/readnews.aspx	2

Unencrypted __VIEWSTATE parameter

Affects	Variation
/about.aspx	1
/comments.aspx (cfbc7026028fd30e88c94fcdc534d6ba)	1
/default.aspx	1
/login.aspx	1
/readnews.aspx (54db37c887f8663f3ac272fd57842c59)	1
/readnews.aspx (cfbc7026028fd30e88c94fcdc534d6ba)	1
/readnews.aspx (f6272bf70dcf239f162f7915a4e4b3b8)	1
/signup.aspx	1

User credentials are sent in clear text

Affects	Variation
/login.aspx	1
/signup.aspx	1

Clickjacking: X-Frame-Options header missing

Affects	Variation
Web Server	1

Login page password-guessing attack

Affects	Variation
/login.aspx	1
/signup.aspx	1

OPTIONS method is enabled

Affects	Variation
Web Server	1

Session Cookie without Secure flag set

Affects	Variation
/	1

Slow response time

Affects	Variation
/comments.aspx (cfbc7026028fd30e88c94fcdc534d6ba)	1
/readnews.aspx (54db37c887f8663f3ac272fd57842c59)	1

Error page web server version disclosure

Affects	Variation
Web Server	1

GHDB: Frontpage extensions for Unix

Affects	Variation
/_vti_cnf	1
/_vti_cnf/acublog.csproj	1
/_vti_cnf/acublog.csproj.webinfo	1

GHDB: Possible ASP.NET sensitive file (web.config)

Affects	Variation
/web.config	1

GHDB: Typical login page

Affects	Variation
/login.aspx	1
/login.aspx (2fec518265dc38aa79e37dedfb7283ba)	1
/login.aspx (a3554b8379542c0a2c94292fa63307a7)	1
/login.aspx.cs	1
/login.aspx.resx	1

Password type input with auto-complete enabled

Affects	Variation
/login.aspx	1
/signup.aspx	1

Alert details

Blind SQL Injection

Severity	**High**
Type	Validation
Reported by module	Scripting (Blind_Sql_Injection.script)

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

[How to check for SQL injection vulnerabilities]
[SQL Injection Walkthrough]
[OWASP Injection Flaws]
[VIDEO: SQL Injection tutorial]
[Acunetix SQL Injection Attack]
[OWASP PHP Top 5]

Affected items

/comments.aspx

Details

URL encoded GET input id was set to -1; waitfor delay '0:0:0' --

Tests performed:
- -1; waitfor delay '0:0:3' -- => 3.062 s
- -1; waitfor delay '0:0:6' -- => 6.062 s
- -1; waitfor delay '0:0:0' -- => 0.063 s
- -1; waitfor delay '0:0:9' -- => 9.094 s
- -1; waitfor delay '0:0:0' -- => 0.062 s
- -1; waitfor delay '0:0:0' -- => [... (line truncated)

Request headers

```
POST /comments.aspx?id=-1;%20waitfor%20delay%20'0:0:0'%20--%20 HTTP/1.1
Content-Length: 1842
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testaspnet.vulnweb.com:80/
```

```
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...dG9vbCB0byBhdXRvbWF0aWNhbGx5IGF1ZGl0IHdlYnNpdGUgc2VjdXJpdHkuIEFjdW5ldGl4IFdlYiBWdWxuZ
XJhYmlsaXR5IFNjYW5uZXIgMiBjcmF3bHMgYW4gZW50aXJlIHdlYnNpdGUsIGxhdW5jaGVzIHBvcHVsYXIgd2ViI
GF0dGFja3MgKFNRTCBJbmplY3Rpb24gZXRjLikgYW5kIGlkZW50aWZpZXMgdnVsbmVyYWJpbGl0aWVzIHRoYXQgb
mVlZCB0byBiZSBmaXhlZC5kAgkPZBYCAgEPZBYGZg9kFgJmDxYCHwEFJTxJTUcgc3JjPSJpbWFnZXMvY29tbWVud
C1iZWZvcmUuZ2lmIj5kAgEPZBYCZg8WAh4FY2xhc3MFB0NvbW1lbnRkAgIPZBYCZg8WAh8BBSQ8SU1HIHNyYz0ia
W1hZ2VzL2NvbW1lbnQtYWZ0ZXIuZ2lmIj5kZGSoHpWphtzTswdbPBZo9EUslZHj
```

/comments.aspx

Details

URL encoded GET input id was set to 3 AND 3*2*1=6 AND 505=505

Tests performed:
- 0+0+0+3 => TRUE
- 0+505*500+3 => FALSE
- 13-5-2-999 => FALSE
- 13-5-2-3 => TRUE
- 13-2*5+0+0+1-1 => TRUE
- 13-2*6+0+0+1-1 => FALSE
- 3 AND 2+1-1-1=1 AND 505=505 => TRUE
- 3 AND 3+1-1-1=1 AND 505=505 => FALSE[/ ... (line truncated)

Request headers

```
GET /comments.aspx?id=3%20AND%203*2*1%3d6%20AND%20505%3d505 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/comments.aspx

Details

URL encoded POST input tbComment was set to I0d9dV9s'); waitfor delay '0:0:0' --

Tests performed:
- rdg5422B'); waitfor delay '0:0:6' -- => 6.078 s
- y1fTUzRt'); waitfor delay '0:0:0' -- => 0.079 s
- nqh0yWJt'); waitfor delay '0:0:9' -- => 9.562 s
- ZzmY4lxr'); waitfor delay '0:0:3' -- => 3.078 s
- RhqNzMji'); waitfor delay '0:0:0' -- => 0 ... (line truncated)

Request headers

```
POST /comments.aspx?id=2 HTTP/1.1
Content-Length: 1888
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

```
(line truncated)
...dG9vbCB0byBhdXRvbWF0aWNhbGx5IGF1ZGl0IHdlYnNpdGUgc2VjdXJpdHkuIEFjdW5ldGl4IFdlYiBWdWxuZXJhYmlsaXR5IFNjYW5uZXIgMiBjcmF3bHMgYW4gZW50aXJlIHdlYnNpdGUsIGxhdW5jaGVzIHBvcHVsYXIgd2ViIGF0dGFja3MgKFNRTCBJbmplY3Rpb24gZXRjLikgYW5kIGlkZW50aWZpZXMgdnVsbmVyYWJpbGl0aWVzIHRoYXQgbmVlZCB0byByZSBmaXhlZC5kAgkPZBYCAgEPZBYGZg9kFgJmDxYCHwEFJTxJTUcgc3JjPSJpbWFnZXMvY29tbWVud C1iZWZvcmUuZ2lmIj5kAgEPZBYCZg8WAh4FY2xhc3MFB0NvbW1lbnRkAgIPZBYCZg8WAh8BBSQ8SU1HIHNyYz0iaW1hZ2VzL2NvbW1lbnQtYWZ0ZXIuZ2lmIj5kZGSoHpWphtzTswdbPBZo9EUslZHj
```

/login.aspx

Details

URL encoded POST input tbUsername was set to -1' OR 3*2*1=6 AND 000815=000815 --

Tests performed:
- -1' OR 2+815-815-1=0+0+0+1 -- => TRUE
- -1' OR 3+815-815-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+815-815) -- => FALSE
- -1' OR 3*2>(0+5+815-815) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000815=000815 -- => TRUE
- -1' OR 000815=000815 ... (line truncated)

Request headers

```
POST /login.aspx HTTP/1.1
Content-Length: 1191
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...GAqXgnv8PAqXgnv8PAqXgspIHAqXgspIHAqXgpikCpeCmKQKl4NrNCQKl4NrNCQKl4M7gAgKl4M7gAgKl4OKH
CgKl4OKHCgKl4NbsCAKl4NbsCAKl4MoDAqXgygMCvvfUqAMCvvfUqAMCvvfIzwwCvvfIzwwCvvf84gUCvvf84gUC
vveQuQ0CvveQuQ0CvveE3AYCvveE3AYCvve48w8Cvve48w%2bjoDhiRcLa6hfwDsQ4gtQSupKMrg%3d%3d&__VIE
WSTATE=/wEPDwUKLTIyMzk2OTgxMQ9kFgICAQ9kFgICAQ9kFgQCAQ8WBB4EaHJlZgUKbG9naW4uYXNweB4JaW5uZ
XJodG1sBQVsb2dpbmQCAw8WBB8AZB4HVmlzaWJsZWhkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfX
xYBBQ9jYlBlcnNpc3RDb29raWWL1W%2bw%2b8Zj9n0mGriLs0UbfzYNdg%3d%3d
```

/readnews.aspx

Details

URL encoded GET input id was set to 2 AND 3*2*1=6 AND 41=41

Tests performed:
- 0+0+0+2 => TRUE
- 0+41*36+2 => FALSE
- 12-5-2-999 => FALSE
- 12-5-2-3 => TRUE
- 12-2*5+0+0+1-1 => TRUE
- 12-2*6+0+0+1-1 => FALSE
- 2 AND 2+1-1-1=1 AND 41=41 => TRUE
- 2 AND 3+1-1-1=1 AND 41=41 => FALSE[/l ... (line truncated)

Request headers

```
GET /readnews.aspx?id=2%20AND%203*2*1%3d6%20AND%2041%3d41&NewsAd=ads/def.html HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/readnews.aspx

Details

URL encoded GET input id was set to 2 AND 3*2*1=6 AND 14=14

Tests performed:
- 0+0+0+2 => TRUE
- 0+14*9+2 => FALSE
- 12-5-2-999 => FALSE
- 12-5-2-3 => TRUE
- 12-2*5+0+0+1-1 => TRUE
- 12-2*6+0+0+1-1 => FALSE
- 2 AND 2+1-1-1=1 AND 14=14 => TRUE
- 2 AND 3+1-1-1=1 AND 14=14 => FALSE[/li ... (line truncated)

Request headers

```
GET /readnews.aspx?id=2%20AND%203*2*1%3d6%20AND%2014%3d14 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/readnews.aspx

Details

URL encoded GET input id was set to -1; waitfor delay '0:0:0' --

Tests performed:
- -1; waitfor delay '0:0:3' -- => 3.109 s
- -1; waitfor delay '0:0:6' -- => 6.562 s
- -1; waitfor delay '0:0:9' -- => 9.578 s
- -1; waitfor delay '0:0:0' -- => 0.078 s
- -1; waitfor delay '0:0:0' -- => 0.578 s
- -1; waitfor delay '0:0:0' -- => [... (line truncated)

Request headers

```
POST /readnews.aspx?id=-1;%20waitfor%20delay%20'0:0:0'%20--%20&NewsAd=ads/def.html
HTTP/1.1
Content-Length: 7509
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...AgICAgICAgICAgICAgICAgU2Nhbm5lciwgaXMgdGhlIHJlc3VsdCBvZiBzZXZlcmFsIHllYXJzIG9mIGRldmV
sb3BtZW50ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIGJ5IGEgdGVhbSBvZiBoaWdobHkgZXhwZXJpZW5jZWQ
gc2VjdXJpdHkgZGV2ZWxvcGVycy4gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgQWN1bmV0aXggaXMgYSBwcml
2YXRlbHkgaGVsZCBjb21wYW55IHdpdGggaXRzIG9mZmljZXMgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgaW4
gTWFsdGEgYW5kIHRoZSBVSy4gPC9wPmQCCQ8PFgIeC05hdmlnYXRlVXJsBRJDb21tZW50cy5hc3B4P2lkPTBkZAI
LDxYCHgNzcmMFDGFkcy9kZWYuaHRtbGRkYi3h0SoV2zJcWbXe2WEK/dQDL54%3d
```

Cross site scripting (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

OWASP PHP Top 5
How To: Prevent Cross-Site Scripting in ASP.NET
Cross site scripting
XSS Filter Evasion Cheat Sheet
XSS Annihilation
OWASP Cross Site Scripting
The Cross Site Scripting Faq
VIDEO: How Cross-Site Scripting (XSS) Works
Acunetix Cross Site Scripting Attack

Affected items

/comments.aspx

Details

URL encoded POST input tbComment was set to 1--><ScRiPt >prompt(990800)</ScRiPt><!--
The input is reflected inside a comment element.

Request headers

```
POST /comments.aspx?id=2 HTTP/1.1
Content-Length: 1885
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...dG9vbCB0byBhdXRvbWF0aWNhbGx5IGF1ZGl0IHdlYnNpdGUgc2VjdXJpdHkuIEFjdW5ldGl4IFdlYiBWdWxuZ
XJhYmlsaXR5IFNjYW5uZXIgMiBjcmF3bHMgYW4gZW50aXJlIHdlYnNpdGUsIGxhdW5jaGVzIHBvcHVsYXIgd2ViI
GF0dGFja3MgKFNRTCBJbmplY3Rpb24gZXRjLikgYW5kIGlkZW50aWZpZXMgdnVsbmVyYWJpbGl0aWVzIHRoYXQgb
mVlZCB0byBiZSBmaXhlZC5kAgkPZBYCAgEPZBYGZg9kFgJmDxYCHwEFJTxJTUcgc3JjPSJpbWFnZXMvY29tbWVud
C1iZWZvcmUuZ2lmIj5kAgEPZBYCZg8WAh4FY2xhc3MFB0NvbW1lbnRkAgIPZBYCZg8WAh8BBSQ8SU1HIHNyYz0ia
W1hZ2VzL2NvbW1lbnQtYWZ0ZXIuZ2lmIj5kZGSoHpWphtzTswdbPBZo9EUslZHj
```

/readnews.aspx

Details

URL encoded GET input NewsAd was set to javascript:prompt(919032);
The input is reflected inside A tag href parameter, a FORM tag action parameter or (I)FRAME src parameter.

Request headers

```
GET /readnews.aspx?id=0&NewsAd=javascript:prompt(919032); HTTP/1.1
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/readnews.aspx

Details

URL encoded GET input NewsAd was set to javascript:prompt(972287);
The input is reflected inside A tag href parameter, a FORM tag action parameter or (I)FRAME src parameter.

Request headers

```
POST /readnews.aspx?id=0&NewsAd=javascript:prompt(972287); HTTP/1.1
Content-Length: 7509
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...AgICAgICAgICAgICAgICAgU2Nhbm5lciwgaXMgdGhlIHJlc3VsdCBvZiBzZXZlcmFsIHllYXJzIG9mIGRldmV
sb3BtZW50ICAgICAgICAgICAgICAgICAgICAgICAgICAgIGJ5IGEgdGVhbSBvZiBoaWdobHkgZXhwZXJpZW5jZWQ
gc2VjdXJpdHkgZGV2ZWxvcGVycy4gICAgICAgICAgICAgICAgICAgICAgICAgICAgQWN1bmV0aXggaXMgYSBwcml
2YXRlbHkgaGVsZCBjb21wYW55IHdpdGggaXRzIG9mZmljZXMgICAgICAgICAgICAgICAgICAgICAgICAgICAgaW4
gTWFsdGEgYW5kIHRoZSBVSy4gPC9wPmQCCQ8PFgIeC05hdmlnYXRlVXJsBRJDb21tZW50cy5hc3B4P2lkPTBkZAI
LDxYCHgNzcmMFDGFkcy9kZWYuaHRtbGRkYi3h0SoV2zJcWbXe2WEK/dQDL54%3d
```

Microsoft IIS tilde directory enumeration

Severity	**High**
Type	Configuration
Reported by module	Scripting (IIS_Tilde_Dir_Enumeration.script)

Description

It is possible to detect short names of files and directories which have an 8.3 file naming scheme equivalent in Windows by using some vectors in several versions of Microsoft IIS. For instance, it is possible to detect all short-names of ".aspx" files as they have 4 letters in their extensions. This can be a major issue especially for the .Net websites which are vulnerable to direct URL access as an attacker can find important files and folders that they are not normally visible.

Impact

Possible sensitive information disclosure.

Recommendation

Consult the "Prevention Technique(s)" section from Soroush Dalili's paper on this subject. A link to this paper is listed in the Web references section below.

References

Microsoft IIS Shortname Scanner PoC
Windows Short (8.3) Filenames - A Security Nightmare?

Affected items

/images

Details

No details are available.

Request headers

```
GET /images/*~1*/a.aspx?aspxerrorpath=/ HTTP/1.1
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

SQL injection (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (Sql_Injection.script)

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

OWASP PHP Top 5
Acunetix SQL Injection Attack
VIDEO: SQL Injection tutorial
OWASP Injection Flaws
How to check for SQL injection vulnerabilities
SQL Injection Walkthrough

Affected items

/comments.aspx

Details

URL encoded GET input id was set to 1ACUSTART'"hOPcwACUEND
Additional details:

Source file: C:\Websites\AspNet\comments.aspx

SQL query: SELECT (max(CommentId)+1)as m, (COUNT(CommentId)) as n FROM comments WHERE NewsId=1ACUSTART'"hOPcwACUEND Stack trace: Method: Void btnSend_Click(System.Object, System.EventArgs) Method: Void OnClick(System.EventArgs) Method: Void RaisePostBackEvent(System.String) Method: Void RaisePostBackEvent(System.Web.UI.IPostBackEventHandler, System.String) Method: Void ProcessRequestMain(Boolean, Boolean) Method: Void ProcessRequest(Boolean, Boolean) Method: Void ProcessRequest() Method: Void ProcessRequest(System.Web.HttpContext) Method: Void ProcessRequest(System.Web.HttpContext) Method: Void System.Web.HttpApplication.IExecutionStep.Execute() Method: System.Exception ExecuteStep(IExecutionStep, Boolean ByRef) Method: Void ResumeSteps(System.Exception) Method: Void ResumeStepsFromThreadPoolThread(System.Exception) Method: Void ResumeStepsWithAssert(System.Exception) Method: Void OnAsyncEventCompletion(System.IAsyncResult) Method: Void Complete(Boolean, System.Object, System.Exception, System.Web.RequestNotificationStatus) Method: Void PollLockedSessionCallback(System.Object) Method: Void runTryCode(System.Object) Method: Void ExecuteCodeWithGuaranteedCleanup(TryCode, CleanupCode, System.Object) Method: Void Run(System.Threading.ExecutionContext, System.Threading.ContextCallback, System.Object) Method: Void PerformTimerCallback(System.Object)

Request headers

```
POST /comments.aspx?id=1ACUSTART'%22hOPcwACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 1842
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...dG9vbCB0byBhdXRvbWF0aWNhbGx5IGF1ZGl0IHdlYnNpdGUgc2VjdXJpdHkuIEFjdW5ldGl4IFdlYiBWdWxuZ
XJhYmlsaXR5IFNjYW5uZXIgMiBjcmF3bHMgYW4gZW50aXJlIHdlYnNpdGUsIGxhdW5jaGVzIHBvcHVsYXIgd2ViI
GF0dGFja3MgKFNRTCBJbmplY3Rpb24gZXRjLikgYW5kIGlkZW50aWZpZXMgdnVsbmVyYWJpbGl0aWVzIHRoYXQgb
mVlZCB0byBiZSBmaXhlZC5kAgkPZBYCAgEPZBYGZg9kFgJmDxYCHwEFJTxJTUcgc3JjPSJpbWFnZXMvY29tbWVud
C1iZWZvcmUuZ2lmIj5kAgEPZBYCZg8WAh4FY2xhc3MFB0NvbW1lbnRkAgIPZBYCZg8WAh8BBSQ8SU1HIHNyYz0ia
W1hZ2VzL2NvbW1lbnQtYWZ0ZXIuZ2lmIj5kZGSoHpWphtzTswdbPBZo9EUslZHj
```

/comments.aspx

Details

URL encoded GET input id was set to 1ACUSTART'"lLIOFACUEND
Additional details:

Source file: C:\Websites\AspNet\comments.aspx

SQL query: SELECT NewsDate, NewsTitle, NewsShort, AuthorId, NewsId FROM news WHERE NewsId=1ACUSTART'"lLIOFACUEND Stack trace: Method: Void ReadData() Method: Void OnLoad(System.EventArgs) Method: Void LoadRecursive() Method: Void ProcessRequestMain(Boolean, Boolean) Method: Void ProcessRequest(Boolean, Boolean) Method: Void ProcessRequest() Method: Void ProcessRequest(System.Web.HttpContext) Method: Void ProcessRequest(System.Web.HttpContext) Method: Void System.Web.HttpApplication.IExecutionStep.Execute() Method: System.Exception ExecuteStep(IExecutionStep, Boolean ByRef) Method: Void ResumeSteps(System.Exception) Method: Void ResumeStepsFromThreadPoolThread(System.Exception) Method: Void ResumeStepsWithAssert(System.Exception) Method: Void OnAsyncEventCompletion(System.IAsyncResult) Method: Void Complete(Boolean, System.Object, System.Exception, System.Web.RequestNotificationStatus) Method: Void PollLockedSessionCallback(System.Object) Method: Void runTryCode(System.Object) Method: Void ExecuteCodeWithGuaranteedCleanup(TryCode, CleanupCode, System.Object) Method: Void Run(System.Threading.ExecutionContext, System.Threading.ContextCallback, System.Object) Method: Void PerformTimerCallback(System.Object)

Request headers

```
GET /comments.aspx?id=1ACUSTART'%22lLIOFACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/comments.aspx

Details

URL encoded POST input tbComment was set to 1ACUSTART'"xal18ACUEND
Additional details:

Source file: C:\Websites\AspNet\comments.aspx

SQL query: INSERT INTO comments (NewsId, CommentId, AuthorName, CommentDate, CommentText) VALUES (2, 78, '89.149.50.115', GETDATE(), '1ACUSTART'"xal18ACUEND') Stack trace: Method: Void btnSend_Click(System.Object, System.EventArgs) Method: Void OnClick(System.EventArgs) Method: Void RaisePostBackEvent(System.String) Method: Void RaisePostBackEvent(System.Web.UI.IPostBackEventHandler, System.String) Method: Void ProcessRequestMain(Boolean, Boolean) Method: Void ProcessRequest(Boolean, Boolean) Method: Void ProcessRequest() Method: Void ProcessRequest(System.Web.HttpContext) Method: Void ProcessRequest(System.Web.HttpContext) Method: Void System.Web.HttpApplication.IExecutionStep.Execute() Method: System.Exception ExecuteStep(IExecutionStep, Boolean ByRef) Method: Void ResumeSteps(System.Exception) Method: Void ResumeStepsFromThreadPoolThread(System.Exception) Method: Void ResumeStepsWithAssert(System.Exception) Method: Void OnAsyncEventCompletion(System.IAsyncResult) Method: Void Complete(Boolean, System.Object, System.Exception, System.Web.RequestNotificationStatus) Method: Void PollLockedSessionCallback(System.Object) Method: Void runTryCode(System.Object) Method: Void ExecuteCodeWithGuaranteedCleanup(TryCode, CleanupCode, System.Object) Method: Void Run(System.Threading.ExecutionContext, System.Threading.ContextCallback, System.Object) Method: Void PerformTimerCallback(System.Object)

Request headers

```
POST /comments.aspx?id=2 HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 1865
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
```

```
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...dG9vbCB0byBhdXRvbWF0aWNhbGx5IGF1ZGl0IHdlYnNpdGUgc2VjdXJpdHkuIEFjdW5ldGl4IFdlYiBWdWxuZ
XJhYmlsaXR5IFNjYW5uZXIgMiBjcmF3bHMgYW4gZW50aXJlIHdlYnNpdGUsIGxhdW5jaGVzIHBvcHVsYXIgd2ViI
GF0dGFja3MgKFNRTCBJbmplY3Rpb24gZXRjLikgYW5kIGlkZW50aWZpZXMgdnVsbmVyYWJpbGl0aWVzIHRoYXQgb
mVlZCB0byBiZSBmaXhlZC5kAgkPZBYCAgEPZBYGZg9kFgJmDxYCHwEFJTxJTUcgc3JjPSJpbWFnZXMvY29tbWVud
C1iZWZvcmUuZ2lmIj5kAgEPZBYCZg8WAh4FY2xhc3MFB0NvbW1lbnRkAgIPZBYCZg8WAh8BBSQ8SU1HIHNyYz0ia
W1hZ2VzL2NvbW1lbnQtYWZ0ZXIuZ2lmIj5kZGSoHpWphtzTswdbPBZo9EUslZHj
```

/login.aspx

Details

URL encoded POST input tbUsername was set to 1ACUSTART'"Zp6UyACUEND
Additional details:

Source file: C:\Websites\AspNet\login.aspx

SQL query: SELECT uname, alevel FROM users WHERE uname='1ACUSTART'"Zp6UyACUEND' AND upass='32cc5886dc1fa8c106a02056292c4654' Stack trace: Method: Boolean Authenticate(System.String ByRef, System.String, Int32 ByRef) Method: Void btnLogin_Click(System.Object, System.EventArgs) Method: Void OnClick(System.EventArgs) Method: Void RaisePostBackEvent(System.String) Method: Void RaisePostBackEvent(System.Web.UI.IPostBackEventHandler, System.String) Method: Void ProcessRequestMain(Boolean, Boolean) Method: Void ProcessRequest(Boolean, Boolean) Method: Void ProcessRequest() Method: Void ProcessRequest(System.Web.HttpContext) Method: Void ProcessRequest(System.Web.HttpContext) Method: Void System.Web.HttpApplication.IExecutionStep.Execute() Method: System.Exception ExecuteStep(IExecutionStep, Boolean ByRef) Method: Void ResumeSteps(System.Exception) Method: System.IAsyncResult System.Web.IHttpAsyncHandler.BeginProcessRequest(System.Web.HttpContext, System.AsyncCallback, System.Object) Method: Void ProcessRequestInternal(System.Web.HttpWorkerRequest) Method: Void ProcessRequestNoDemand(System.Web.HttpWorkerRequest) Method: Int32 ProcessRequest(IntPtr, Int32)

Request headers

```
POST /login.aspx HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 1163
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...GAqXgnv8PAqXgnv8PAqXgspIHAqXgspIHAqXgpikCpeCmKQKl4NrNCQKl4NrNCQKl4M7gAgKl4M7gAgKl4OKH
CgKl4OKHCgKl4NbsCAKl4NbsCAKl4MoDAqXgygMCvvfUqAMCvvfUqAMCvvfIzwwCvvfIzwwCvvf84gUCvvf84gUC
vveQuQ0CvveQuQ0CvveE3AYCvveE3AYCvve48w8Cvve48w%2bjoDhiRcLa6hfwDsQ4gtQSupKMrg%3d%3d&__VIE
WSTATE=/wEPDwUKLTIyMzk2OTgxMQ9kFgICAQ9kFgICAQ9kFgQCAQ8WBB4EaHJlZgUKbG9naW4uYXNweB4JaW5uZ
XJodG1sBQVsb2dpbmQCAw8WBB8AZB4HVmlzaWJsZWhkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfX
xYBBQ9jYlBlcnNpc3RDb29raWWL1W%2bw%2b8Zj9n0mGriLs0UbfzYNdg%3d%3d
```

/readnews.aspx

Details

URL encoded GET input id was set to 1ACUSTART'"mFrleACUEND
Additional details:

Source file: C:\Websites\AspNet\readnews.aspx

SQL query: SELECT NewsDate, NewsTitle, NewsLong, AuthorId FROM news WHERE NewsId=1ACUSTART'"mFrleACUEND Stack trace: Method: Void Page_Load(System.Object, System.EventArgs) Method: Void OnLoad(System.EventArgs) Method: Void LoadRecursive() Method: Void ProcessRequestMain(Boolean, Boolean) Method: Void ProcessRequest(Boolean, Boolean) Method: Void ProcessRequest() Method: Void ProcessRequest(System.Web.HttpContext) Method: Void ProcessRequest(System.Web.HttpContext) Method: Void System.Web.HttpApplication.IExecutionStep.Execute() Method: System.Exception ExecuteStep(IExecutionStep, Boolean ByRef) Method: Void ResumeSteps(System.Exception) Method: Void ResumeStepsFromThreadPoolThread(System.Exception) Method: Void ResumeStepsWithAssert(System.Exception) Method: Void OnAsyncEventCompletion(System.IAsyncResult) Method: Void Complete(Boolean, System.Object, System.Exception, System.Web.RequestNotificationStatus) Method: Void PollLockedSessionCallback(System.Object) Method: Void runTryCode(System.Object) Method: Void ExecuteCodeWithGuaranteedCleanup(TryCode, CleanupCode, System.Object) Method: Void Run(System.Threading.ExecutionContext, System.Threading.ContextCallback, System.Object) Method: Void PerformTimerCallback(System.Object)

Request headers

```
GET /readnews.aspx?id=1ACUSTART'%22mFrleACUEND&NewsAd=ads/def.html HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/readnews.aspx

Details

URL encoded GET input id was set to 1ACUSTART'"V8uDVACUEND
Additional details:

Source file: C:\Websites\AspNet\readnews.aspx

SQL query: SELECT NewsDate, NewsTitle, NewsLong, AuthorId FROM news WHERE NewsId=1ACUSTART'"V8uDVACUEND Stack trace: Method: Void Page_Load(System.Object, System.EventArgs) Method: Void OnLoad(System.EventArgs) Method: Void LoadRecursive() Method: Void ProcessRequestMain(Boolean, Boolean) Method: Void ProcessRequest(Boolean, Boolean) Method: Void ProcessRequest() Method: Void ProcessRequest(System.Web.HttpContext) Method: Void ProcessRequest(System.Web.HttpContext) Method: Void System.Web.HttpApplication.IExecutionStep.Execute() Method: System.Exception ExecuteStep(IExecutionStep, Boolean ByRef) Method: Void ResumeSteps(System.Exception) Method: System.IAsyncResult System.Web.IHttpAsyncHandler.BeginProcessRequest(System.Web.HttpContext, System.AsyncCallback, System.Object) Method: Void ProcessRequestInternal(System.Web.HttpWorkerRequest) Method: Void ProcessRequestNoDemand(System.Web.HttpWorkerRequest) Method: Int32 ProcessRequest(IntPtr, Int32)

Request headers

```
POST /readnews.aspx?id=1ACUSTART'%22V8uDVACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 10761
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...ICAgICAgICAgICAgIGJ5IGEgdGVhbSBvZiBoaWdobHkgZXhwZXJpZW5jZWQgc2VjdXJpdHkgZGV2ZWxvcGVyc
y4gICAgICAgICAgICAgICAgICAgICAgICAgICAgQWN1bmV0aXggaXMgYSBwcml2YXRlbHkgaGVsZCBjb21wYW55I
HdpdGggaGVhZHF1YXJ0ZXJzICAgICAgICAgICAgICAgICAgICAgICAgICAgIGJhc2VkIGluIEV1cm9wZSAoTWFsd
GEpIHdpdGggaXRzIE5ldyBZb3JrIFVTIG9mZmljZSAgICAgICAgICAgICAgICAgICAgICAgICBzY2hlZHVsZ
WQgdG8gb3BlbiBpbiBRMyBvZiAyMDA1LiA8L3A%2bIGQCCQ8PFgIeC05hdmlnYXRlVXJsBRJDb21tZW50cy5hc3B
4P2lkPTJkZAILDxYCHgNzcmNkZGS78tg0yYdYIrm%2b7bJhr2ToTj/BEA%3d%3d
```

/readnews.aspx

Details

URL encoded GET input id was set to 1ACUSTART'"q0SWxACUEND
Additional details:

Source file: C:\Websites\AspNet\readnews.aspx

SQL query: SELECT NewsDate, NewsTitle, NewsLong, AuthorId FROM news WHERE NewsId=1ACUSTART'"q0SWxACUEND Stack trace: Method: Void Page_Load(System.Object, System.EventArgs) Method: Void OnLoad(System.EventArgs) Method: Void LoadRecursive() Method: Void ProcessRequestMain(Boolean, Boolean) Method: Void ProcessRequest(Boolean, Boolean) Method: Void ProcessRequest() Method: Void ProcessRequest(System.Web.HttpContext) Method: Void ProcessRequest(System.Web.HttpContext) Method: Void System.Web.HttpApplication.IExecutionStep.Execute() Method: System.Exception ExecuteStep(IExecutionStep, Boolean ByRef) Method: Void ResumeSteps(System.Exception) Method: Void ResumeStepsFromThreadPoolThread(System.Exception) Method: Void ResumeStepsWithAssert(System.Exception) Method: Void OnAsyncEventCompletion(System.IAsyncResult) Method: Void Complete(Boolean, System.Object, System.Exception, System.Web.RequestNotificationStatus) Method: Void PollLockedSessionCallback(System.Object) Method: Void runTryCode(System.Object) Method: Void ExecuteCodeWithGuaranteedCleanup(TryCode, CleanupCode, System.Object) Method: Void Run(System.Threading.ExecutionContext, System.Threading.ContextCallback, System.Object) Method: Void PerformTimerCallback(System.Object)

Request headers

```
POST /readnews.aspx?id=1ACUSTART'%22q0SWxACUEND&NewsAd=ads/def.html HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Content-Length: 7509
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...AgICAgICAgICAgICAgICAgU2Nhbm5lciwgaXMgdGhlIHJlc3VsdCBvZiBzZXZlcmFsIHllYXJzIG9mIGRldmV
sb3BtZW50ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIGJ5IGEgdGVhbSBvZiBoaWdobHkgZXhwZXJpZW5jZWQ
gc2VjdXJpdHkgZGV2ZWxvcGVycy4gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgQWN1bmV0aXggaXMgYSBwcml
2YXRlbHkgaGVsZCBjb21wYW55IHdpdGggaXRzIG9mZmljZXMgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgaW4
gTWFsdGEgYW5kIHRoZSBVSy4gPC9wPmQCCQ8PFgIeC05hdmlnYXRlVXJsBRJDb21tZW50cy5hc3B4P2lkPTBkZAI
LDxYCHgNzcmMFDGFkcy9kZWYuaHRtbGRkYi3h0SoV2zJcWbXe2WEK/dQDL54%3d
```

/readnews.aspx

Details

URL encoded GET input id was set to 1ACUSTART"'aIfSnACUEND
Additional details:

Source file: C:\Websites\AspNet\readnews.aspx

SQL query: SELECT NewsDate, NewsTitle, NewsLong, AuthorId FROM news WHERE NewsId=1ACUSTART"'aIfSnACUEND Stack trace: Method: Void Page_Load(System.Object, System.EventArgs) Method: Void OnLoad(System.EventArgs) Method: Void LoadRecursive() Method: Void ProcessRequestMain(Boolean, Boolean) Method: Void ProcessRequest(Boolean, Boolean) Method: Void ProcessRequest() Method: Void ProcessRequest(System.Web.HttpContext) Method: Void ProcessRequest(System.Web.HttpContext) Method: Void System.Web.HttpApplication.IExecutionStep.Execute() Method: System.Exception ExecuteStep(IExecutionStep, Boolean ByRef) Method: Void ResumeSteps(System.Exception) Method: System.IAsyncResult System.Web.IHttpAsyncHandler.BeginProcessRequest(System.Web.HttpContext, System.AsyncCallback, System.Object) Method: Void ProcessRequestInternal(System.Web.HttpWorkerRequest) Method: Void ProcessRequestNoDemand(System.Web.HttpWorkerRequest) Method: Int32 ProcessRequest(IntPtr, Int32)

Request headers

```
GET /readnews.aspx?id=1ACUSTART'%22aIfSnACUEND HTTP/1.1
Acunetix-Aspect-Password: *****
Acunetix-Aspect: enabled
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Unicode transformation issues

Severity	**High**
Type	Configuration
Reported by module	Scripting (XSS.script)

Description

This page is vulnerable to various Unicode transformation issues such as Best-Fit Mappings, Overlong byte sequences, Ill-formed sequences.

Best-Fit Mappings occurs when a character X gets transformed to an entirely different character Y. In general, best-fit mappings occur when characters are transcoded between Unicode and another encoding.

Overlong byte sequences (non-shortest form) - UTF-8 allows for different representations of characters that also have a shorter form. For security reasons, a UTF-8 decoder must not accept UTF-8 sequences that are longer than necessary to encode a character. For example, the character U+000A (line feed) must be accepted from a UTF-8 stream only in the form 0x0A, but not in any of the following five possible overlong forms:
- 0xC0 0x8A
- 0xE0 0x80 0x8A
- 0xF0 0x80 0x80 0x8A
- 0xF8 0x80 0x80 0x80 0x8A
- 0xFC 0x80 0x80 0x80 0x80 0x8A

Ill-Formed Subsequences As REQUIRED by UNICODE 3.0, and noted in the Unicode Technical Report #36, if a leading byte is followed by an invalid successor byte, then it should NOT consume it.

Impact

Software vulnerabilities arise when Best-Fit mappings occur. For example, characters can be manipulated to bypass string handling filters, such as cross-site scripting (XSS) or SQL Injection filters, WAF's, and IDS devices. Overlong UTF-8 sequence could be abused to bypass UTF-8 substring tests that look only for the shortest possible encoding.

Recommendation

Identify the source of these Unicode transformation issues and fix them. Consult the web references below for more information.

References

Unicode Security
Unicode Security Considerations
UTF-8 and Unicode FAQ for Unix/Linux
A couple of unicode issues on PHP and Firefox

Affected items

/comments.aspx

Details

URL encoded POST input tbComment was set to acu6557%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6557

List of issues:
- Unicode character U+FF1C FULLWIDTH LESS-THAN SIGN (encoded as %EF%BC%9C) was transformed into U+003C LESS-THAN SIGN (<)
- Unicode character U+02BA MODIFIER LETTER DOUBLE PRIME (encoded as %CA%BA[/da ... (line truncated)

Request headers

```
POST /comments.aspx?id=2 HTTP/1.1
Content-Length: 1891
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...dG9vbCB0byBhdXRvbWF0aWNhbGx5IGF1ZGl0IHdlYnNpdGUgc2VjdXJpdHkuIEFjdW5ldGl4IFdlYiBWdWxuZ
XJhYmlsaXR5IFNjYW5uZXIgMiBjcmF3bHMgYW4gZW50aXJlIHdlYnNpdGUsIGxhdW5jaGVzIHBvcHVsYXIgd2ViI
GF0dGFja3MgKFNRTCBJbmplY3Rpb24gZXRjLikgYW5kIGlkZW50aWZpZXMgdnVsbmVyYWJpbGl0aWVzIHRoYXQgb
mVlZCB0byByZSBmaXhlZC5kAgkPZBYCAgEPZBYGZg9kFgJmDxYCHwEFJTxJTUcgc3JjPSJpbWFnZXMvY29tbWVud
C1iZWZvcmUuZ2lmIj5kAgEPZBYCZg8WAh4FY2xhc3MFB0NvbW1lbnRkAgIPZBYCZg8WAh8BBSQ8SU1HIHNyYz0ia
W1hZ2VzL2NvbW1lbnQtYWZ0ZXIuZ2lmIj5kZGSoHpWphtzTswdbPBZo9EUslZHj
```

ASP.NET error message

Severity	**Medium**
Type	Validation
Reported by module	Scripting (ASP_NET_Error_Message.script)

Description

By requesting a specially crafted URL is possible to generate an ASP.NET error message. The message contains the complete stack trace and Microsoft .NET Framework Version.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Adjust web.config to enable custom errors for remote clients. Set customErrors mode to Off or RemoteOnly. customErrors is part of system.web Element. RemoteOnly specifies that custom errors are shown only to the remote clients, and that ASP.NET errors are shown to the local host. This is the default value.

```
<configuration>
   <system.web>
     <customErrors mode="RemoteOnly" />
  </system.web>
</configuration>
```

References

customErrors Element (ASP.NET Settings Schema)

Affected items

Web Server

Details

Error message pattern found: <title>Illegal characters in path.</title>
Version information found: Microsoft .NET Framework Version:2.0.50727.3053; ASP.NET Version:2.0.50727.3053

Request headers

```
GET /|~.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Cross frame scripting

Severity	**Medium**
Type	Validation
Reported by module	Scripting (XFS_and_Redir.script)

Description

This script is possibly vulnerable to Cross Frame Scripting (XFS) attacks.

This is an attack technique used to trick a user into thinking that fake web site content is legitimate data.

Impact

Malicious users may poison a frame allowing them to conduct phishing attacks.

Recommendation

Your script should filter metacharacters from user input.

References

Cross Frame Scripting

Affected items

/readnews.aspx

Details

URL encoded GET input NewsAd was set to http://www.acunetix.com

Request headers

```
GET /readnews.aspx?id=0&NewsAd=http://www.acunetix.com HTTP/1.1
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/readnews.aspx

Details

URL encoded GET input NewsAd was set to http://www.acunetix.com

Request headers

```
POST /readnews.aspx?id=0&NewsAd=http://www.acunetix.com HTTP/1.1
Content-Length: 7509
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...AgICAgICAgICAgICAgICAgU2Nhbm5lciwgaXMgdGhlIHJlc3VsdCBvZiBzZXZlcmFsIHllYXJzIG9mIGRldmV
sb3BtZW50ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIGJ5IGEgdGVhbSBvZiBoaWdobHkgZXhwZXJpZW5jZWQ
gc2VjdXJpdHkgZGV2ZWxvcGVycy4gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgQWN1bmV0aXggaXMgYSBwcml
2YXRlbHkgaGVsZCBjb21wYW55IHdpdGggaXRzIG9mZmljZXMgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgaW4
gTWFsdGEgYW5kIHRoZSBVSy4gPC9wPmQCCQ8PFgIeC05hdmlnYXRlVXJsBRJDb21tZW50cy5hc3B4P2lkPTBkZAI
LDxYCHgNzcmMFDGFkcy9kZWYuaHRtbGRkYi3h0SoV2zJcWbXe2WEK/dQDL54%3d
```

Unencrypted __VIEWSTATE parameter

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

The __VIEWSTATE parameter is not encrypted. To reduce the chance of someone intercepting the information stored in the ViewState, it is good design to encrypt the ViewState. To do this, set the machineKey validation type to AES. This instructs ASP.NET to encrypt the ViewState value using the Advanced Encryption Standard.

Impact

Possible sensitive information disclosure.

Recommendation

Open Web.Config and add the following line under the <system.web> element:
<machineKey validation="AES"/>

Affected items

/about.aspx

Details

form name: "Form1"
form action: "about.aspx"
Strings extracted from VIEWSTATE: "-10524290
login.asp
innerhtm
login
Visiblehdd
"

Request headers

```
GET /about.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/comments.aspx (cfbc7026028fd30e88c94fcdc534d6ba)

Details

form name: "Form1"
form action: "comments.aspx?id=2"
Strings extracted from VIEWSTATE: "-86270316
login.asp
innerhtm
login
Visibleh
"

Request headers

```
GET /comments.aspx?id=2 HTTP/1.1
```

```
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/default.aspx

Details

form name: "Form1"
form action: "Default.aspx"
Strings extracted from VIEWSTATE: "-10524290
login.asp
innerhtm
login
Visiblehdd
"

Request headers

```
GET /Default.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/login.aspx

Details

form name: "frmLogin"
form action: "login.aspx"
Strings extracted from VIEWSTATE: "-22396981
login.asp
innerhtm
login
Visibleh
"

Request headers

```
GET /login.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

```
Accept: */*
```

/readnews.aspx (54db37c887f8663f3ac272fd57842c59)

Details

form name: "Form1"
form action: "readnews.aspx?id=0&NewsAd=ads%2fdef.html"
Strings extracted from VIEWSTATE: "-35223256
login.asp
innerhtm
login
Visibleh
"

Request headers

```
GET /readnews.aspx?id=0&NewsAd=ads/def.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/readnews.aspx (cfbc7026028fd30e88c94fcdc534d6ba)

Details

form name: "Form1"
form action: "readnews.aspx?id=2"
Strings extracted from VIEWSTATE: "-35223256
login.asp
innerhtm
login
Visibleh
"

Request headers

```
GET /readnews.aspx?id=2 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/comments.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/readnews.aspx (f6272bf70dcf239f162f7915a4e4b3b8)

Details

form name: "Form1"
form action: "readnews.aspx?id=2&NewsAd=ads%2fdef.html"
Strings extracted from VIEWSTATE: "-35223256
login.asp
innerhtm
login
Visibleh
"

Request headers

```
GET /readnews.aspx?id=2&NewsAd=ads/def.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/signup.aspx

Details

form name: "Form1"
form action: "signup.aspx"
Strings extracted from VIEWSTATE: "-64328658
login.asp
innerhtm
login
Visiblehdd
"

Request headers

```
GET /signup.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

User credentials are sent in clear text

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

/login.aspx

Details

Form name: frmLogin
Form action: http://testaspnet.vulnweb.com/login.aspx
Form method: POST

Form inputs:

- __EVENTTARGET [Hidden]
- __EVENTARGUMENT [Hidden]
- __VIEWSTATE [Hidden]
- __EVENTVALIDATION [Hidden]
- tbUsername [Text]
- tbPassword [Password]
- cbPersistCookie [Checkbox]
- btnLogin [Submit]

Request headers

```
GET /login.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/signup.aspx

Details

Form name: Form1
Form action: http://testaspnet.vulnweb.com/signup.aspx
Form method: POST

Form inputs:

- __EVENTTARGET [Hidden]
- __EVENTARGUMENT [Hidden]
- __VIEWSTATE [Hidden]
- __EVENTVALIDATION [Hidden]
- tbUsername [Text]
- tbPassword [Password]
- btnSignup [Submit]

Request headers

```
GET /signup.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
Clickjacking
Original Clickjacking paper

Affected items

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Login page password-guessing attack

Severity	**Low**
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks

Affected items

/login.aspx

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /login.aspx HTTP/1.1
Content-Length: 1120
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...GAqXgnv8PAqXgnv8PAqXgspIHAqXgspIHAqXgpikCpeCmKQKl4NrNCQKl4NrNCQKl4M7gAgKl4M7gAgKl4OKH
CgKl4OKHCgKl4NbsCAKl4NbsCAKl4MoDAqXgygMCvvfUqAMCvvfUqAMCvvfIzwwCvvfIzwwCvvf84gUCvvf84gUC
vveQuQ0CvveQuQ0CvveE3AYCvveE3AYCvve48w8Cvve48w%2bjoDhiRcLa6hfwDsQ4gtQSupKMrg%3d%3d&__VIE
WSTATE=/wEPDwUKLTIyMzk2OTgxMQ9kFgICAQ9kFgICAQ9kFgQCAQ8WBB4EaHJlZgUKbG9naW4uYXNweB4JaW5uZ
XJodG1sBQVsb2dpbmQCAw8WBB8AZB4HVmlzaWJsZWhkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfX
xYBBQ9jYlBlcnNpc3RDb29raWWL1W%2bw%2b8Zj9n0mGriLs0UbfzYNdg%3d%3d
```

/signup.aspx

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /signup.aspx HTTP/1.1
Content-Length: 1042
Content-Type: application/x-www-form-urlencoded
Referer: http://testaspnet.vulnweb.com:80/
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...P0MAsDZnJAEAsDZnJAEAsDZ8PkCAsDZ8PkCAsDZ5JwKAsDZ5JwKAqXg9oUNAqXg9oUNAqXg6tgGAqXg6tgGAq
Xgnv8PAqXgnv8PAqXgspIHAqXgspIHAqXgpikCpeCmKQKl4NrNCQKl4NrNCQKl4M7gAgKl4M7gAgKl4OKHCgKl4O
KHCgKl4NbsCAKl4NbsCAKl4MoDAqXgygMCvvfUqAMCvvfUqAMCvvfIzwwCvvfIzwwCvvf84gUCvvf84gUCvveQuQ
0CvveQuQ0CvveE3AYCvveE3AYCvve48w8Cvve48w9GaUZb1cPl1r5cQ5c05bz4T0rKdg%3d%3d&__VIEWSTATE=/
wEPDwUKLTY0MzI4NjU4Mw9kFgICAQ9kFgICAQ9kFgQCAQ8WBB4EaHJlZgUKbG9naW4uYXNweB4JaW5uZXJodG1sB
QVsb2dpbmQCAw8WBB8AZB4HVmlzaWJsZWhkZHEZ3VN6SP/C2xESDN/Y3p8zhfSB
```

OPTIONS method is enabled

Severity	**Low**
Type	Validation
Reported by module	Scripting (Options_Server_Method.script)

Description

HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

Impact

The OPTIONS method may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

It's recommended to disable OPTIONS Method on the web server.

References

Testing for HTTP Methods and XST (OWASP-CM-008)

Affected items

Web Server

Details

Methods allowed: OPTIONS, TRACE, GET, HEAD

Request headers

```
OPTIONS / HTTP/1.1
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Session Cookie without Secure flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

/
Details
Cookie name: "ASP.NET_SessionId" Cookie domain: "testaspnet.vulnweb.com"
Request headers
`GET / HTTP/1.1`

Slow response time

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This page had a slow response time. The response time for this page was 5812 ms while the average response time for this site is 411.10 ms. This types of files can be targeted in denial of service attacks. An attacker can request this page repeatedly from multiple computers until the server becomes overloaded.

Impact

Possible denial of service.

Recommendation

Investigate if it's possible to reduce the response time for this page.

Affected items

/comments.aspx (cfbc7026028fd30e88c94fcdc534d6ba)

Details

No details are available.

Request headers

```
GET /comments.aspx?id=2 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/readnews.aspx (54db37c887f8663f3ac272fd57842c59)

Details

No details are available.

Request headers

```
GET /readnews.aspx?id=0&NewsAd=ads/def.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Error page web server version disclosure

Severity	**Informational**
Type	Configuration
Reported by module	Scripting (Error_Page_Path_Disclosure.script)

Description

By requesting a page that doesn't exist, an error page was returned. This error page contains the web server version number and a list of modules enabled on this server. This information can be used to conduct further attacks.

Impact

Possible sensitive information disclosure.

Recommendation

If you are using Apache, you can setup a custom 404 page by following the instructions provided in the References section.

References

Custom error responses
Creating Custom Error Pages on Apache Servers

Affected items

Web Server

Details

Information disclosure pattern found: Microsoft .NET Framework Version:2.0.50727.3053; ASP.NET Version:2.0.50727.3053

Request headers

```
GET /0a3KBg51BA.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

GHDB: Frontpage extensions for Unix

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Sensitive Directories

Frontpage extensions for Unix ? So be it..

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

The Google Hacking Database (GHDB) community
Acunetix Google hacking

Affected items

/_vti_cnf

Details

We found allinurl:("/*/_vti_pvt/" | "/*/_vti_cnf/")

Request headers

```
GET /_vti_cnf/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/_vti_cnf/acublog.csproj

Details

We found allinurl:("/*/_vti_pvt/" | "/*/_vti_cnf/")

Request headers

```
GET /_vti_cnf/acublog.csproj HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/_vti_cnf/acublog.csproj.webinfo

Details

We found allinurl:("/*/_vti_pvt/" | "/*/_vti_cnf/")

Request headers

```
GET /_vti_cnf/acublog.csproj.webinfo HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

GHDB: Possible ASP.NET sensitive file (web.config)

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Files containing juicy info

Through Web.config an IIS adminstrator can specify settings like custom 404 error pages, authentication and authorization settings for the Web site. This file can hold a plaintext password in the worst case or just reveil the full path info on a 404 error.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

Acunetix Google hacking
The Google Hacking Database (GHDB) community

Affected items

/web.config

Details

We found filetype:config web.config -CVS

Request headers

```
GET /web.config HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

GHDB: Typical login page

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Pages containing login portals

This is a typical login page. It has recently become a target for SQL injection. Comsec's article at http://www.governmentsecurity.org/articles/SQLinjectionBasicTutorial.php brought this to my attention.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

Acunetix Google hacking
The Google Hacking Database (GHDB) community

Affected items

/login.aspx

Details

We found inurl:login.asp

Request headers

```
GET /login.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/login.aspx (2fec518265dc38aa79e37dedfb7283ba)

Details

We found inurl:login.asp

Request headers

```
POST /login.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/login.aspx
Content-Length: 1128
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
```

```
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...GAqXgnv8PAqXgnv8PAqXgspIHAqXgspIHAqXgpikCpeCmKQKl4NrNCQKl4NrNCQKl4M7gAgKl4M7gAgKl4OKH
CgKl4OKHCgKl4NbsCAKl4NbsCAKl4MoDAqXgygMCvvfUqAMCvvfUqAMCvvfIzwwCvvfIzwwCvvf84gUCvvf84gUC
vveQuQ0CvveQuQ0CvveE3AYCvveE3AYCvve48w8Cvve48w%2bjoDhiRcLa6hfwDsQ4gtQSupKMrg%3d%3d&__VIE
WSTATE=/wEPDwUKLTIyMzk2OTgxMQ9kFgICAQ9kFgICAQ9kFgQCAQ8WBB4EaHJlZgUKbG9naW4uYXNweB4JaW5uZ
XJodG1sBQVsb2dpbmQCAw8WBB8AZB4HVmlzaWJsZWhkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfX
xYBBQ9jYlBlcnNpc3RDb29raWWL1W%2bw%2b8Zj9n0mGriLs0UbfzYNdg%3d%3d
```

/login.aspx (a3554b8379542c0a2c94292fa63307a7)

Details

We found inurl:login.asp

Request headers

```
POST /login.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/login.aspx
Content-Length: 1147
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

(line truncated)
...GAqXgnv8PAqXgnv8PAqXgspIHAqXgspIHAqXgpikCpeCmKQKl4NrNCQKl4NrNCQKl4M7gAgKl4M7gAgKl4OKH
CgKl4OKHCgKl4NbsCAKl4NbsCAKl4MoDAqXgygMCvvfUqAMCvvfUqAMCvvfIzwwCvvfIzwwCvvf84gUCvvf84gUC
vveQuQ0CvveQuQ0CvveE3AYCvveE3AYCvve48w8Cvve48w%2bjoDhiRcLa6hfwDsQ4gtQSupKMrg%3d%3d&__VIE
WSTATE=/wEPDwUKLTIyMzk2OTgxMQ9kFgICAQ9kFgICAQ9kFgQCAQ8WBB4EaHJlZgUKbG9naW4uYXNweB4JaW5uZ
XJodG1sBQVsb2dpbmQCAw8WBB8AZB4HVmlzaWJsZWhkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfX
xYBBQ9jYlBlcnNpc3RDb29raWWL1W%2bw%2b8Zj9n0mGriLs0UbfzYNdg%3d%3d
```

/login.aspx.cs

Details

We found inurl:login.asp

Request headers

```
GET /login.aspx.cs HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/login.aspx.resx

Details

We found inurl:login.asp

Request headers

```
GET /login.aspx.resx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Password type input with auto-complete enabled

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:
<INPUT TYPE="password" AUTOCOMPLETE="off">

Affected items

/login.aspx

Details

Password type input named tbPassword from form named frmLogin with action login.aspx has autocomplete enabled.

Request headers

```
GET /login.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/signup.aspx

Details

Password type input named tbPassword from form named Form1 with action signup.aspx has autocomplete enabled.

Request headers

```
GET /signup.aspx HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testaspnet.vulnweb.com/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: aspectalerts
Cookie: ASP.NET_SessionId=zvdzseb35q1ugcblg0jdzo55
Host: testaspnet.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Scanned items (coverage report)

Scanned 77 URLs. Found 12 vulnerable.

URL: http://testaspnet.vulnweb.com/Default.aspx

Vulnerabilities has been identified for this URL

10 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
delete	URL encoded GET

Input scheme 2	
Input name	Input type
__EVENTARGUMENT	URL encoded POST
__EVENTTARGET	URL encoded POST
__EVENTVALIDATION	URL encoded POST
__VIEWSTATE	URL encoded POST

Input scheme 3	
Input name	Input type
delete	URL encoded GET
__EVENTARGUMENT	URL encoded POST
__EVENTTARGET	URL encoded POST
__EVENTVALIDATION	URL encoded POST
__VIEWSTATE	URL encoded POST

URL: http://testaspnet.vulnweb.com/about.aspx

Vulnerabilities has been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
__EVENTARGUMENT	URL encoded POST
__EVENTTARGET	URL encoded POST
__EVENTVALIDATION	URL encoded POST
__VIEWSTATE	URL encoded POST

URL: http://testaspnet.vulnweb.com/login.aspx

Vulnerabilities has been identified for this URL

8 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
__EVENTARGUMENT	URL encoded POST
__EVENTTARGET	URL encoded POST
__EVENTVALIDATION	URL encoded POST
__VIEWSTATE	URL encoded POST
btnLogin	URL encoded POST
cbPersistCookie	URL encoded POST
tbPassword	URL encoded POST
tbUsername	URL encoded POST

URL: http://testaspnet.vulnweb.com/styles.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/signup.aspx

Vulnerabilities has been identified for this URL

7 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
__EVENTARGUMENT	URL encoded POST
__EVENTTARGET	URL encoded POST
__EVENTVALIDATION	URL encoded POST
__VIEWSTATE	URL encoded POST
btnSignup	URL encoded POST
tbPassword	URL encoded POST
tbUsername	URL encoded POST

URL: http://testaspnet.vulnweb.com/rssfeed.aspx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/readnews.aspx

Vulnerabilities has been identified for this URL

14 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET
NewsAd	URL encoded GET

Input scheme 2	
Input name	Input type
id	URL encoded GET

Input scheme 3	
Input name	Input type
id	URL encoded GET
NewsAd	URL encoded GET
__EVENTARGUMENT	URL encoded POST
__EVENTTARGET	URL encoded POST
__EVENTVALIDATION	URL encoded POST
__VIEWSTATE	URL encoded POST

Input scheme 4	
Input name	Input type
id	URL encoded GET
__EVENTARGUMENT	URL encoded POST
__EVENTTARGET	URL encoded POST
__EVENTVALIDATION	URL encoded POST
__VIEWSTATE	URL encoded POST

URL: http://testaspnet.vulnweb.com/comments.aspx

Vulnerabilities has been identified for this URL

8 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

Input scheme 2	
Input name	Input type
id	URL encoded GET
__EVENTARGUMENT	URL encoded POST
__EVENTTARGET	URL encoded POST
__EVENTVALIDATION	URL encoded POST
__VIEWSTATE	URL encoded POST
btnSend	URL encoded POST
tbComment	URL encoded POST

URL: http://testaspnet.vulnweb.com/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/ads/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/ads/def.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/aspnet_client/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/aspnet_client/system_web/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/aspnet_client/system_web/2_0_50727/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/bin/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/bin/acublog.dll

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/bin/acublog.dll.bak

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/bin/acublog.pdb

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/bin/acuweaver.dll

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/langs/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/langs/en.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/themes/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/themes/simple/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/themes/simple/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/themes/simple/css/editor_content.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/themes/simple/css/editor_popup.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/themes/simple/css/editor_ui.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/themes/simple/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/themes/simple/editor_template.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/themes/simple/editor_template_src.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/utils/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/utils/form_utils.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/utils/mctabs.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/utils/validate.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/blank.htm

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/license.txt

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/tiny_mce.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/tiny_mce_popup.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/jscripts/tiny_mce/tiny_mce_src.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/temp/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/temp/.rnd

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/utils/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/utils/usermanager.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/_vti_cnf/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/_vti_cnf/acublog.csproj

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/_vti_cnf/acublog.csproj.webinfo

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/about.aspx.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/about.aspx.resx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/acublog.csproj

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/acublog.csproj.webinfo

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/assemblyinfo.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/comments.aspx.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/comments.aspx.resx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/default.aspx.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/default.aspx.resx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/global.asax

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/global.asax.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/global.asax.resx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/login.aspx.cs

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/login.aspx.resx

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/logout.aspx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/logout.aspx.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/logout.aspx.resx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/mainmenu.ascx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/mainmenu.ascx.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/mainmenu.ascx.resx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/postnews.aspx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/postnews.aspx.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/postnews.aspx.resx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/rssfeed.aspx.resx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/signup.aspx.cs

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/signup.aspx.resx

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/test.txt

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/web.config

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testaspnet.vulnweb.com/robots.txt

No vulnerabilities has been identified for this URL

No input(s) found for this URL