acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

26 April, 2011

Detailed Scan Report

Generated by Acunetix WVS Reporter (v7.0 Build 20100921)

Scan of http://localhost:51045/

Scan details

Scan information	
Starttime	26/04/2011 20:41:08
Finish time	26/04/2011 20:47:23
Scan time	6 minutes, 16 seconds
Profile	Default

Server information	
Responsive	True
Server banner	ASP.NET Development Server/10.0.0.0
Server OS	Windows
Server technologies	ASP.NET

Threat level

Acunetix Threat Level 2
One or more medium-severity type vulnerabilities have been by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	**13**
High	0
Medium	6
Low	4
Informational	3

Knowledge base

List of open TCP ports

Open Port **135 / msrpc**
No port banner available.

Open Port **445 / microsoft-ds**
No port banner available.

Open Port **554 / rtsp**
No port banner available.

Open Port **10000 / snet-sensor-mgmt**
Port Banner:
HTTP/1.1 400 ERROR: keep-aliveLength: 17Type: text/html

request

List of file extensions

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

- css => **1** file(s)
- js => **1** file(s)

List of files with inputs

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

- **/account/login** - **1** inputs

Alerts summary

ASP.NET error message	
Affects	Variations
Web Server	1

Error message on page	
Affects	Variations
/a	1
/account/cm6udQp5gO.jsp	1
/content/FaUONFsO6h.jsp	1
/j2cohJLHui.jsp	1
/scripts/oBHT2m7K0j.jsp	1

ASP.NET debugging enabled	
Affects	Variations
/	1
/account	1

Login page password-guessing attack	
Affects	Variations
/account/login	1

Session Cookie without Secure flag set	
Affects	Variations
/	1

Broken links	
Affects	Variations
/a	1

Error page Web Server version disclosure	
Affects	Variations
Web Server	1

Password type input with autocomplete enabled	
Affects	Variations
/account	1

Alert details

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>
```

Affected items

Web Server
Details
Error message pattern found: <title>Illegal characters in path.</title> Version information found: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.225
Request

```
GET /|~.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:10 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 5623
Connection: Close
```

Error message on page

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

Description

This page contains an error/warning message that may disclose sensitive information.The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

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

Recommendation

Review the source code for this script.

Affected items

/a

Details

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

Request

```
GET /a HTTP/1.1
Pragma: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Referer: http://localhost:51045/
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
```

Response

```
HTTP/1.1 404 Not Found
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:16 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3169
Connection: Close
```

/account/cm6udQp5gO.jsp

Details

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

Request

```
GET /account/cm6udQp5gO.jsp HTTP/1.1
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1
```

```
CE016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

Response

```
HTTP/1.1 404 Not Found
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:30 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3336
Connection: Close
```

/content/FaUONFsO6h.jsp

Details

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

Request

```
GET /content/FaUONFsO6h.jsp HTTP/1.1
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
```

Response

```
HTTP/1.1 404 Not Found
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:28 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3211
Connection: Close
```

/j2cohJLHui.jsp

Details

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

Request

```
GET /j2cohJLHui.jsp HTTP/1.1
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
```

Response

```
HTTP/1.1 404 Not Found
Server: ASP.NET Development Server/10.0.0.0
```

```
Date: Tue, 26 Apr 2011 23:41:17 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3195
```

/scripts/oBHT2m7K0j.jsp

Details

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

Request

```
GET /scripts/oBHT2m7K0j.jsp HTTP/1.1
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
```

Response

```
HTTP/1.1 404 Not Found
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:53 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3211
Connection: Close
```

ASP.NET debugging enabled

Severity	**Low**
Type	Validation
Reported by module	Scripting (ASP-NET_Debugging_Enabled.script)

Description

ASP.NET debugging is enabled on this application. It is recommended to disable debug mode before deploying a production application. By default, debugging is disabled, and although debugging is frequently enabled to troubleshoot a problem, it is also frequently not disabled again after the problem is resolved.

Impact

It may be possible to disclose sensitive information about the web sever the ASP.NET application.

Recommendation

Check References for details on how to fix this problem.

Affected items

/

Details

No details are available.

Request

```
DEBUG /acunetix_invalid_filename.aspx HTTP/1.1
Command: stop-debug
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
```

```
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

Response

```
HTTP/1.1 200 OK
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:17 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 2
Connection: Close
```

/account

Details

No details are available.

Request

```
DEBUG /account/acunetix_invalid_filename.aspx HTTP/1.1
Command: stop-debug
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
```

Response

```
HTTP/1.1 200 OK
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:29 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 2
Connection: Close
```

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.

Affected items

/account/login
Details
The scanner tested 10 invalid credentials and no account lockout was detected.
Request

```
POST /account/login HTTP/1.1
Content-Length: 35
Content-Type: application/x-www-form-urlencoded
Host: localhost:51045
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)

password=Gitz3Gz6&username=8BethseI
```

Response

```
HTTP/1.1 302 Found
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:19 GMT
X-AspNet-Version: 4.0.30319
X-AspNetMvc-Version: 3.0
Location: /account
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 125
Connection: Close
```

Session Cookie without Secure flag set

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

Description

This session cookie doesn't 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: "localhost"
Request

```
GET / HTTP/1.1
Pragma: no-cache
Acunetix-Aspect: enabled
```

```
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
```

Response

```
HTTP/1.1 200 OK
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:08 GMT
X-AspNet-Version: 4.0.30319
X-AspNetMvc-Version: 3.0
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 395
Connection: Close
```

Broken links

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

Description

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/a

Details

No details are available.

Request

```
GET /a HTTP/1.1
Pragma: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Referer: http://localhost:51045/
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
```

Response

```
HTTP/1.1 404 Not Found
Server: ASP.NET Development Server/10.0.0.0
```

```
Date: Tue, 26 Apr 2011 23:41:16 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3169
```

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.

Affected items

Web Server

Details

Information disclosure pattern found: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.225

Request

```
GET /XlYKYbD4sp HTTP/1.1
Cookie: ASP.NET_SessionId=p1yvpgvtdryc3d3wch5b2gmb;
.ASPXAUTH=CCAEB590D7C98A0713C3F4ABEBD1ECA222D721F5FABE04FA5A323E9AF8A0E9DF035560C4B6BF6A
DB37449B24A1599CC76CD50D19A57CF8CDE29501049D5BFA2CF757A242DEA8FC0A1FA6AFF32BEB954189EDA8
B1D075C5A09A93B6F306D8787568BCAC7FDDEF6D0961175AF7D84A98CB7675D26806D6A11A9694445B88EC1C
E016FC748156071BDEC4C89057E0EC0A6661B023F9223E5E9C29AB2566CBF5D7EB
Host: localhost:51045
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
```

Response

```
HTTP/1.1 404 Not Found
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:09 GMT
X-AspNet-Version: 4.0.30319
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3187
Connection: Close
```

Password type input with autocomplete 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 autocomplete should be disabled in sensitive applications.
To disable autocomplete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

Affected items

/account
Details
Password type input named **password** from **unnamed form** with action **/Account/Login** has autocomplete enabled.
Request

```
GET /Account HTTP/1.1
Host: localhost:51045
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
Connection: Keep-alive
```

Response

```
HTTP/1.1 200 OK
Server: ASP.NET Development Server/10.0.0.0
Date: Tue, 26 Apr 2011 23:41:08 GMT
X-AspNet-Version: 4.0.30319
X-AspNetMvc-Version: 3.0
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 769
Connection: Close
```