acunetix WEB APPLICATION SECURITY

Acunetix Website Audit

5 November, 2014

Developer Report

Generated by Acunetix WVS Reporter (v8.0 Build 20120808)

Scan of http://filesbi.go.id:80/

Scan details

Scan information	
Starttime	05/11/2014 14:44:06
Finish time	05/11/2014 14:47:02
Scan time	2 minutes, 56 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.2.25 (Win32) PHP/5.2.3
Server OS	Windows
Server technologies	PHP

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	**2**	
● **High**	2	🟥

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 => 2 file(s)
- txt => 3 file(s)
- js => 2 file(s)
- php => 1 file(s)

Top 10 response times

The files listed bellow had the slowest response times measured during the crawling process. The average response time for this site was 16,97 ms. These files could be targetted in denial of service attacks.

1. /scripts/extjs3/ext-all.js, response time 2386 ms

```
GET /scripts/extjs3/ext-all.js HTTP/1.1
Pragma: no-cache
Referer: http://filesbilateral.bilateral.go.id/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: eXtplorer=NSVgTBm94TJCxKdAcx0QwRUrbwsYdo4P
```

```
Host: filesbilateral.bilateral.go.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

List of client scripts

These files contain Javascript code referenced from the website.

- /scripts/extjs3/adapter/ext/ext-base.js
- /scripts/extjs3/ext-all.js

List of files with inputs

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

- /index.php - 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).

- extplorer.net
- www.google.com

List of email addresses

List of all email addresses found on this host.

- colonelxc@users.sourceforge.net
- licensing@extjs.com
- licensing@sencha.com

Alerts summary

Cross Site Scripting

Affects	Variations
/index.php	1

Cross Site Scripting (verified)

Affects	Variations
/index.php	1

Alert details

Cross Site Scripting

Severity	**High**
Type	Validation
Reported by module	Scripting (XSS_in_URI.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

Cross site scripting
How To: Prevent Cross-Site Scripting in ASP.NET
Allowing HTML and Preventing XSS
Microsoft ASP.NET request filtering flaw
OWASP PHP Top 5
XSS cheat sheet
XSS Annihilation
OWASP Cross Site Scripting
The Cross Site Scripting Faq
Security Focus - Penetration Testing for Web Applications (Part Two)
Acunetix Cross Site Scripting Attack
ASP.NET Unicode Character Conversion XSS

Affected items

/index.php

Details

URI was set to 957266"():;988165
The input is reflected inside <script> tag between double quotes.

Request headers

```
GET /index.php/957266%22():;988165 HTTP/1.1
Cookie: eXtplorer=MKCO3s0cmVG8cB5ERO6gtsFC73uVoU9W
Host: filesbilateral.bilateral.go.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

Cross Site Scripting (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (XSS_in_URI.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

ASP.NET Unicode Character Conversion XSS
Acunetix Cross Site Scripting Attack
Security Focus - Penetration Testing for Web Applications (Part Two)
The Cross Site Scripting Faq
OWASP Cross Site Scripting
XSS Annihilation
XSS cheat sheet
Cross site scripting
Microsoft ASP.NET request filtering flaw
Allowing HTML and Preventing XSS
How To: Prevent Cross-Site Scripting in ASP.NET
OWASP PHP Top 5

Affected items

/index.php

Details

URI was set to ö" onmouseover=prompt(930630) //
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /index.php/%F6%22%20onmouseover=prompt(930630)%20// HTTP/1.1
Cookie: eXtplorer=MKCO3s0cmVG8cB5ERO6gtsFC73uVoU9W
Host: filesbilateral.bilateral.go.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

URL: http://filesbilateral.bilateral.go.id/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://filesbilateral.bilateral.go.id/scripts/extjs3/resources/css/xtheme-blue.css

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://filesbilateral.bilateral.go.id/scripts/extjs3/resources/css/ext-all.css

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://filesbilateral.bilateral.go.id/scripts/extjs3/adapter/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://filesbilateral.bilateral.go.id/scripts/extjs3/ext-all.js

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://filesbilateral.bilateral.go.id/index.php

Vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

URL: http://filesbilateral.bilateral.go.id/changelog.txt

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://filesbilateral.bilateral.go.id/readme.txt

Vulnerabilities has been identified for this URL

No input(s) found for this URL