Developer Report

Acunetix Security Audit

27 May 2019

Generated by Acunetix

Scan of www.vbboy.com

Scan details

Scan information	
Start time	27/05/2019, 03:22:02
Start url	http://www.vbboy.com
Host	www.vbboy.com
Scan time	71 minutes, 48 seconds
Profile	Full Scan
Server information	cloudflare
Responsive	True
Server OS	Unknown
Server technologies	PHP

Threat level

Acunetix Threat Level 2

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

Alerts distribution

Total alerts found	37
High	0
Medium	19
Low	10
Informational	8

Alerts summary

Application error message

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: Low Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1
/zb_system/cmd.php	7

Error message on page

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: Low Integrity Impact: None Availability Impact: None

CWE	CWE-200

Affected items	Variation
/zb_system/admin/	1
/zb_system/cmd.php	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
/index.php	1
/zb_system/admin/	1
/zb_system/cmd.php	1
/zb_system/login.php	1

URL rewrite vulnerability

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None 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-436

Affected items	Variation
Web Server	1
/index.php	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
/zb_system/login.php	1

Vulnerable Javascript library

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: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None

CWE	CWE-16

Affected items	Variation
/zb_system/script/common.js	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

Cookie(s) without HttpOnly flag set

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

Cookie(s) without Secure flag set

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

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
/zb_system/login.php	1

Possible relative path overwrite

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-20

Affected items	Variation
/zb_system/login.php	1

ⓘ Possible sensitive directories

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: 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	5

ⓘ 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

Email address found

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
/feed.php	1
/zb_system/css/admin.css	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

Possible internal IP address 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
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
/feed.php	1

Possible server path disclosure (Unix)

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: 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
/feed.php	1

Alerts details

Application error message

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

Description

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

Web Server

Details

URL encoded GET input **id** was set to **"" (empty)**

Pattern found:

```
Internal Server Error
```

Request headers

```
GET /?id= HTTP/1.1
Referer: http://www.vbboy.com/
Connection: keep-alive
Cookie: __cfduid=d43ae5e468ec3f365b9d50b98456d83f81558927330
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/zb_system/cmd.php

Details

Cookie input **__cfduid** was set to
VVEwS2Yyb3daYVdobFZ2bjdySG5waVRLc1hWZTZ2cTZDb3JZc1hJMUxPbQ==

Pattern found:

```
Internal Server Error
```

Request headers

```
GET /zb_system/cmd.php HTTP/1.1
Referer: https://www.google.com/search?hl=en&q=testing
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Cookie: __cfduid=VVEwS2Yyb3daYVdobFZ2bjdySG5waVRLc1hWZTZ2cTZDb3JZc1hJMUxPbQ==
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.com
```

/zb_system/cmd.php

Details

URL encoded GET input **act** was set to **"" (empty)**

Pattern found:

```
Internal Server Error
```

Request headers

```
GET /zb_system/cmd.php?act=&type=vrs HTTP/1.1
Referer: http://www.vbboy.com/
Connection: keep-alive
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/zb_system/cmd.php

Details

URL encoded GET input **act** was set to **"" (empty)**

Pattern found:

```
Internal Server Error
```

Request headers

```
GET /zb_system/cmd.php?act= HTTP/1.1
Referer: http://www.vbboy.com/
Connection: keep-alive
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/zb_system/cmd.php

Details

URL encoded GET input **act** was set to **"" (empty)**

Pattern found:

```
Internal Server Error
```

Request headers

```
GET /zb_system/cmd.php?act=&src= HTTP/1.1
Referer: http://www.vbboy.com/
Connection: keep-alive
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_1336931493=8595f002250d3e8932b0d7f765d8fb9d;captcha_3688958368=58301bc0f6a8f39ed1dcd
9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/zb_system/cmd.php

Details

Cookie input **captcha_1336931493** was set to **aUtDa0M0THpZVTVNdlU2QnQ1TkpURTdpeEFXalB0S1E=**

Pattern found:

```
Internal Server Error
```

Request headers

```
GET /zb_system/cmd.php HTTP/1.1
Referer: https://www.google.com/search?hl=en&q=testing
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_1336931493=aUtDa0M0THpZVTVNdlU2QnQ1TkpURTdpeEFXalB0S1E=;captcha_3688958368=58301bc0f
6a8f39ed1dcd9484ef2131c
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.com
```

/zb_system/cmd.php

Details

Cookie input **captcha_3688958368** was set to **clUyb0FsWGZrTkZqb1BhUG13cGVZMjZLSktKSFBxMlU=**

Pattern found:

```
Internal Server Error
```

Request headers

```
GET /zb_system/cmd.php HTTP/1.1
Referer: https://www.google.com/search?hl=en&q=testing
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_1336931493=9ef3524f7b76d0b91855655bd0f01c1c;captcha_3688958368=clUyb0FsWGZrTkZqb1BhU
G13cGVZMjZLSktKSFBxMlU=
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.com
```

/zb_system/cmd.php

Details

URL encoded POST input **sumbit** was set to
dUEwQ0NEV0x3RUFTOFZjalZmaHJTTlpnZ1lPZmhCWUM=

Pattern found:

```
Internal Server Error
```

Request headers

```
POST /zb_system/cmd.php?act=sample%40email.tst&key=http://www.vulnweb.com&postid=2
HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 183
Host: www.vbboy.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
inpEmail=%E8%AE%BF%E5%AE%A2&inpHomePage=0&inpId=g00dPa%24%24w0rD&inpName=sumbit=%E6%8F%9
0%E4%BA%A4&inpRevID=555&inpVerify=cmt&dUEwQ0NEV0x3RUFTOFZjalZmaHJTTlpnZ1lPZmhCWUM=&txaAr
ticle=2
```

Error message on page

Severity	**Medium**
Reported by module	/Scripts/PerFolder/Text_Search_Dir.script

Description

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (http://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

/zb_system/admin/

Details

Pattern found:

```
Internal Server Error
```

Request headers

/zb_system/cmd.php

Details

Pattern found:

```
Internal Server Error
```

Request headers

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/)
Cross-Site Request Forgery (CSRF) Prevention Cheatsheet (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)
Cross-site Request Forgery (https://en.wikipedia.org/wiki/Cross-site_request_forgery)

Affected items

Web Server

Details

Request headers

```
GET / HTTP/1.1
Cookie: __cfduid=d589445540f537ce52b017dec798734701558927323
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/index.php

Details

Request headers

```
GET /index.php HTTP/1.1
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/zb_system/admin/

Details

Request headers

```
GET /zb_system/admin/ HTTP/1.1
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_1336931493=8595f002250d3e8932b0d7f765d8fb9d;captcha_3688958368=58301bc0f6a8f39ed1dcd
9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/zb_system/cmd.php

Details

Request headers

```
GET /zb_system/cmd.php?act=misc&type=vrs HTTP/1.1
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/zb_system/login.php

Details

Request headers

```
GET /zb_system/login.php HTTP/1.1
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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 rewrite vulnerability

Severity	**Medium**
Reported by module	/httpdata/request_url_override.js

Description

It was identified that this application supports the legacy headers **X-Original-URL** and/or **X-Rewrite-URL**.

Support for these headers lets users override the path in the request URL via the X-Original-URL or X-Rewrite-URL HTTP request header and allows a user to access one URL but have web application return a different one which can bypass restrictions on higher level caches and web servers.

Many web frameworks such as Symfony 2.7.0 to 2.7.48, 2.8.0 to 2.8.43, 3.3.0 to 3.3.17, 3.4.0 to 3.4.13, 4.0.0 to 4.0.13 and 4.1.0 to 4.1.2 , zend-diactoros up to 1.8.4, zend-http up to 2.8.1, zend-feed up to 2.10.3 are affected by this security issue.

Impact

The impact of this vulnerability depends on the affected web application/framework.

Recommendation

Upgrade the affected web frameworks to their latest versions.

References

[CVE-2018-14773: Remove support for legacy and risky HTTP headers](https://symfony.com/blog/cve-2018-14773-remove-support-for-legacy-and-risky-http-headers) (https://symfony.com/blog/cve-2018-14773-remove-support-for-legacy-and-risky-http-headers)
[ZF2018-01: URL Rewrite vulnerability](https://framework.zend.com/security/advisory/ZF2018-01) (https://framework.zend.com/security/advisory/ZF2018-01)

Affected items

Web Server

Details

Request headers

```
GET /?cb762117=1 HTTP/1.1
X-Original-URL: /sgoxxalhcd
X-Rewrite-URL: /sgoxxalhcd
Cookie: __cfduid=d43ae5e468ec3f365b9d50b98456d83f81558927330
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/index.php

Details

Request headers

```
GET /index.php?cb155626=1 HTTP/1.1
X-Original-URL: /mnagniskxy
X-Rewrite-URL: /mnagniskxy
Cookie: __cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;captcha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

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

/zb_system/login.php

Details

Request headers

```
GET /zb_system/login.php HTTP/1.1
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

Vulnerable Javascript library

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

Recommendation

Upgrade to the latest version.

Affected items

/zb_system/script/common.js

Details

Detected Javascript library **jquery** version **1.8.3**.
The version was detected from **file content**.

References:

- https://github.com/jquery/jquery/issues/2432
- http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/

Request headers

```
GET /zb_system/script/common.js HTTP/1.1
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_1336931493=8595f002250d3e8932b0d7f765d8fb9d;captcha_3688958368=58301bc0f6a8f39ed1dcd
9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

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: __cfduid=d43ae5e468ec3f365b9d50b98456d83f81558927330
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

Cookie(s) without HttpOnly flag set

Severity	**Low**
Reported by module	/RPA/Cookie_Without_HttpOnly.js

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

Cookies can be accessed by client-side scripts.

Recommendation

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

Affected items

Web Server
Details
captcha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c; path=/
Request headers

```
GET /zb_system/script/c_validcode.php?id=cmt&tm=0.36580236262377785 HTTP/1.1
Host: www.vbboy.com
X-WVS-ID: 2
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.vbboy.com/?id=2
Accept-Encoding: gzip,deflate
Accept-Language: en-US
Cookie: UM_distinctid=16af752a58b298-0f3603aa1ec26f-1e1c7f57-75300-16af752a58c6e4;
CNZZDATA1260370248=404584257-1558924339-%7C1558924339; timezone=8;
__cfduid=d43ae5e468ec3f365b9d50b98456d83f81558927330;
captcha_3688958368=834caaf8f26f9fd3ab36d8b247a6b338
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Cookie(s) without Secure flag set

Severity	**Low**
Reported by module	/RPA/Cookie_Without_Secure.js

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/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

Recommendation

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

Affected items

Web Server
Details
captcha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c; path=/
Request headers

```
GET /zb_system/script/c_validcode.php?id=cmt&tm=0.36580236262377785 HTTP/1.1
Host: www.vbboy.com
X-WVS-ID: 2
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.vbboy.com/?id=2
Accept-Encoding: gzip,deflate
Accept-Language: en-US
Cookie: UM_distinctid=16af752a58b298-0f3603aa1ec26f-1e1c7f57-75300-16af752a58c6e4;
CNZZDATA1260370248=404584257-1558924339-%7C1558924339; timezone=8;
__cfduid=d43ae5e468ec3f365b9d50b98456d83f81558927330;
captcha_3688958368=834caaf8f26f9fd3ab36d8b247a6b338
Connection: keep-alive
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

/zb_system/login.php

Details

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

Request headers

```
POST /zb_system/login.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://www.vbboy.com/
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 127
Host: www.vbboy.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
btnPost=%E7%99%BB%E5%BD%95&chkRemember=on&dishtml5=0&edtPassWord=UVbAwemc&edtUserName=0r
zVbhmE&password=1&savedate=0&username=1
```

Possible relative path overwrite

Severity	**Low**
Reported by module	/Scripts/PerFile/Relative_Path_Overwrite.script

Description

Manual confirmation is required for this alert.

Gareth Heyes introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS stylesheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.

Impact

On older versions of Internet Explorer it's possible to execute arbitrary JavaScript code using Internet Explorer's expression() function. An attacker can also extract the page source and potentially steal CSRF tokens using CSS selectors.

Recommendation

If possible, it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.

References

Relative Path Overwrite (http://www.thespanner.co.uk/2014/03/21/rpo/)

Affected items

/zb_system/login.php

Details

A CSS import from a relative path was found on this page:

```
<link rel="stylesheet" href="css/admin.css" type="text/css" media="screen" />
```

The same relative CSS import is present even when a random string was placed after the filename. Also, the response is frameable.

Request headers

```
GET /zb_system/login.php/iBdxJ/ HTTP/1.1
Connection: keep-alive
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

Possible sensitive directories

Severity	**Low**
Reported by module	/Scripts/PerFolder/Possible_Sensitive_Directories.script

Description

A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

References

[Web Server Security and Database Server Security](http://www.acunetix.com/websitesecurity/webserver-security/) (http://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

Web Server

Details

Request headers

```
GET /zb_system/admin HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Connection: keep-alive
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

Web Server

Details

Request headers

```
GET /zb_users/upload HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Connection: keep-alive
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

Web Server

Details

Request headers

```
GET /zb_users/logs HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Connection: keep-alive
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

Web Server

Details

Request headers

```
GET /zb_system/image/admin HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Connection: keep-alive
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

Web Server

Details

Request headers

```
GET /zb_users/theme/default/include HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Connection: keep-alive
Cookie:
__cfduid=d3f5d33b183b3b3f53002811e82d04ee81558928503;bdshare_firstime=1558927572005;capt
cha_1011327024=2496c699565832d5cc83e1aa7d6b0fc3;captcha_1082452901=1bbf21e1fbc209e54b503
2db60d0c398;captcha_1103369702=b420844c9e566bbedd307911c65e0f54;captcha_1104051602=2807a
a6a40ed4781c960c4221cec74c2;captcha_1116892633=4d9977de0184b5f7eb1f216b20d05faa;captcha_
1131309426=ffbe7ccc7e7d2cfe2a07461102c66209;captcha_115220709=7fc075f08ff39292959bdca053
1c449f;captcha_1186595569=74bce5df33d83a7f28f8c74098a297fa;captcha_1210086391=1ed7cede30
82e44e481794118a8c8621;captcha_1217504333=a67b1a6876d2dacbf16b4edebc0158cb;captcha_12345
40984=ae479f4f0335c494c12ad03b66485e1f;captcha_1241489002=bf5c22371111cad4c5edfd38ee099a
97;captcha_12518970=b874118d1f1603bb994e5c2705d05dc2;captcha_127078804=b5fc2287b28798f00
19f6502e284ed20;captcha_1279390267=f82fa5ed3eae2805cc802fe42d05abff;captcha_1334070963=3
ace49417756dcdbb351596bf69f2bd9;captcha_1336931493=a00bec469789bba98d0a72c934d15bcb;capt
cha_1355328901=3d376dd2b77b100456992aea595ca289;captcha_1379791612=0af57508e89532c95a73a
d2215dee389;captcha_1413759057=0ef904133399f68478ff3c7c7065a200;captcha_1429911420=268de
af6494767332184f862b2adb89f;captcha_1434836030=6265d6d9e1c6721d20756684eb625be0;captcha_
1440250097=b2866ac1f51e3a01e40bd506aac20319;captcha_144192806=9a214881f9c12c573c67fe02d0
73b873;captcha_1464587709=d2fd83b74b50b273812ec822715caa72;captcha_1475160777=2579379001
33e803f2f4102579435cbb;captcha_1529040715=105cc8c68cba944f51af2f4bc25c2a22;captcha_15303
37627=5948a670560829c08185bafc70d34d59;captcha_1531356072=c2187bab3c4c7f3dc7b38b6f7ca692
b3;captcha_1532558294=3543e8165baab4193a258076f3b01cce;captcha_154661706=ad0b23353aab6d3
32aadf8532d96da92;captcha_155308162=6332ad6cf17b5e26d12059928b692167;captcha_1592048086=
1a4935542fe7e71f4dbb7a2198035942;captcha_161498738=fa660dc78ec7633ea8421434a11ddfa4;capt
cha_1665876433=0c16a25c70845435309febffd051d439;captcha_1676784899=6f3b08bc812234ecc43fe
e3d55892970;captcha_1679807654=1f30d5d9ceb5424d3908808c895f2d5e;captcha_1707954924=86cea
a94535999455986cdba9871e89e;captcha_1730938613=d033672c065e435247a57cf81ba08c35;captcha_
175914233=955ba9ca649adc65f50e7ca255b3b5c9;captcha_1817530600=6b5aa5b7d362f4b4750d8474ea
6d5ec5;captcha_1817815486=49bd633f7b137da3de9bb1f69109d992;captcha_1860418669=6c203a04ca
cb3ed230f462f0d494c3fa;captcha_1874549362=7f38f230255fb62f397c4fcdc23c5413;captcha_19396
70967=dab8fe8121a452ecfe62c3dd4e826828;captcha_2052025707=6e29b2730efff5c4156677aa71c834
6b;captcha_2066882207=4069a67f6601c29dd7a95e91c4511b57;captcha_2067703337=497c546743475b
```

```
a81285a4b9ac295e93;captcha_2111607095=9347d554686643cbb703c0a600d94914;captcha_213080157
1=5a00eeacef931dda509c7abc8b23043a;captcha_2136135556=5359e3cccdf96be79d7efb21a397b7d3;c
aptcha_2141595092=c6634c3228e3ac0ef15af916f55d13fa;captcha_2142555102=42ddd33c9398129511
df8f979af82bfa;captcha_2159971306=89a1c17d51f176b582ba6ee40ae4bbec;captcha_2173180877=77
e1c78fe7f38a488cb22c808b76ef39;captcha_2183497084=aa388960432f067b2371ebbb60ff7ab4;captc
ha_2195207972=7f5f127be8f7ba6160c0b2ef77a4acf9;captcha_2205365612=5017030db991197fc2df1a
621d8a86d8;captcha_2207834062=a1ab11b7902bd41d9c37c73117126a8a;captcha_2232817345=ad86aa
91e8db3fa85f8aebb340ef2567;captcha_2253173837=d28dd19767a88868e86f66065a746340;captcha_2
263834180=70f212dfa26f2fcd41ea80ca9e39fba3;captcha_2280483596=464174c9464b4ae2ac0fd8fb6f
e92fc6;captcha_2289070005=ee87a7f9ace9fbe27b5d49cf24fef00b;captcha_2292104284=6e5bb7a5f2
7ec126d2833f2345891390;captcha_2300978108=3fdc5669216c02f94231f2db4caa7cb8;captcha_23312
71195=692437fefa76d01cc821485d8f1c1624;captcha_2353490639=4a4192527a732126b68f37589c7374
92;captcha_2364688447=714ccaef84dc812591f6a306443c71c0;captcha_2365993734=f5d30c957ea4ac
a2d4db3528dd0ef2b8;captcha_2376336438=57f4cafb8c62be1891dc91ee873ece11;captcha_238251077
=02cf65cb30755e5cd5d7f4161df5bb15;captcha_2403188839=9a49aeefd123570adfe34589d1a070ff;ca
ptcha_2409610939=921bbbe5690b5be9ee68477f41b93bb9;captcha_2441863277=c1695525ffbd9913971
259a9b3cfb564;captcha_2452765270=5232cf7b74ceff0c3bca9fc5b3999c93;captcha_2529921305=560
f75d38fd5b77f315c65b4fdabda83;captcha_2613019998=5fb75049fc77d228340df6425b2ea915;captch
a_2617799305=a608808b9eaef4e3a7da2b04cdb9ff43;captcha_2620064255=eeaae5c43ae324d077529ba
1b6e95657;captcha_2634655296=f01a4e5fb4f0cac913468c562524c230;captcha_263944924=bff296b8
cf49d98ad60131fce50443b2;captcha_2711960060=6ac2682c3cccacede14e5468ddb314ff;captcha_272
6223322=94f5d77932e133d0dfb01be0d470920a;captcha_273250838=3f31b6ae3c897f1493354c2fbc2af
06a;captcha_2778196471=3e405b486d3b67b3ab75a9caf7148901;captcha_2796421357=c6bd389c15887
1dbee36daf0e656db97;captcha_2857583908=b1ad353464adb020f34080a9b5e50e4d;captcha_29001089
13=b71cca225635bafd7ad66d8a0f9210ce;captcha_2901517053=e9cbfb226d0c41b633d75ccbae08f6b9;
captcha_2963235947=38bc92c860866d9c4b6e9924a58e9b2b;captcha_3031874652=d8b530ed78c393fd4
49238cfb10ba3c7;captcha_3049099879=bff839994a68a2f9d6f2d0857d2558a9;captcha_3067096139=0
67f3e4e391410108cd8ebd66af4c3da;captcha_3085507923=4c9508a1e71c28372e488e2c2a6e5b50;capt
cha_3108597002=6a4d7439c6e3cec6ed0fc635677903d1;captcha_3124196677=aca28f1cb2ed7244dfd5a
c5c8c7b2e02;captcha_319564018=dcfb25b014c2063e959493ee46dcc2ed;captcha_3225910356=6b7afc
1f0e339185dee13f4607aa34eb;captcha_324749524=15f69306315570a8811076632014a7d2;captcha_32
89293872=feed5d78c267770989f9f4ec85a2aa2f;captcha_3299556771=05042d38e5c37d3d9c13b832c76
907df;captcha_3310931585=04f50ba247e2618c29043293867faf21;captcha_3428703844=5fd20c49001
a0befa035bb856803e3c0;captcha_3472242410=acf9f70b31d8a7089af3fecc34aa47a5;captcha_348056
2853=bd9cb1756b45031e48ca858e2d552953;captcha_348125050=93c7061a48284b109f5f82ee85c8ffdd
;captcha_348764843=6b5bd1d5b3715a80f808845f504a51b9;captcha_3517715818=3f37d1c126c03cb32
4f6b7ade388070a;captcha_3557069902=c09aabdb0077026406382dae4ccf2b12;captcha_3565863737=d
fb3f94b042283e281a3951eb97cf347;captcha_3569370549=b26e61e11df1ec8955447afc5cc9855c;capt
cha_3576105621=45a4318ad2ba01188e60c1f079a48f1c;captcha_3682208558=b26d21c949a8612db5a4d
2610d3cb6c6;captcha_3688958368=bedc235f2f763260e68a3221b2483004;captcha_371985089=4ad3ae
8f969601f8c915b7500719420a;captcha_3740378515=9ea3ba6be5895ae218b90904306b8913;captcha_3
76822226=c7c51d38a779dba64ec77e5481bc4c9d;captcha_3779738114=b8b619c5f7f27d51daddbbe4747
fbe5f;captcha_3843063205=1abd4b894db3349de273e4f11847588e;captcha_3907972154=ad0e5debb2b
8b62f471ee91e7c8c3a75;captcha_3907972451=768278b13841728006431922 79d8eada;captcha_403664
1499=80d952cdddb2f9af03ec82f07f96cbf3;captcha_4058747297=25504072dd7ca30b0b7962a3e78657a
d;captcha_4060584242=9d30ced208689910b5b1c82861dbe348;captcha_4096029475=a70dd5dac23d63b
3088af9cf095bb726;captcha_4096097755=ec62b0e78e15626517a81083f7b6b84d;captcha_4106793126
=065c3534275a886b5bcee946389ac078;captcha_4166959769=765c70942736402729cd8a3cff1574b4;ca
ptcha_4169293783=31bfaf0ebd5d7b4da2cfcff40d11f4df;captcha_4247816259=9f8814ab2b4eeadd506
8bae8db468656;captcha_4253722906=f888e2917739c59b0457981220e32b91;captcha_42904443=53bde
396737553a2dd5d7fbe7dc1129b;captcha_520689506=74d380e5a31cbc1481dcef4e13fe5b9f;captcha_5
76703527=1ca81a72f3322bf49bd2d22b167c423c;captcha_606585252=8152d685f315608365a6699cbb26
6345;captcha_642499349=82891dcc174513470df360981a3816aa;captcha_668782712=ab986a19aab986
767545b0d60ebac11e;captcha_697141547=850b1e27696627ba56eeb04c8e95225d;captcha_720627141=
f15149a7f4643caa1fbcb4cb079c66f4;captcha_75606263=4617b9b5705866b60dc1f15aa524c6b8;captc
ha_835960449=a0e6e5203dd6f5ad088211cd93077e19;captcha_856651966=6be1b1aed066243164de9ab7
d8d51e10;captcha_857026554=5a8328e484f084c3f4af82b281a48f96;captcha_900836064=a7d237788d
834b8c762bcc091951e72a;captcha_910397298=5948220011f3e0755f5abacfd8ed053e
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

ⓘ 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)
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: __cfduid=d589445540f537ce52b017dec798734701558927323
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

ⓘ Email address found

Severity	**Informational**
Reported by module	/Scripts/PerFolder/Invalid_Page_Text_Search.script

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)](https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

Web Server

Details

Pattern found:

```
mat_wu@163.com
```

Request headers

```
GET /feed.php/pd3eRCvneI.jsp HTTP/1.1
Connection: keep-alive
Cookie: __cfduid=d43ae5e468ec3f365b9d50b98456d83f81558927330
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/feed.php

Details

Pattern found:

```
mat_wu@163.com
```

Request headers

/zb_system/css/admin.css

Details

Pattern found:

```
u2lei@yahoo.com.cn
xinxr@msn.com
```

Request headers

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 /zb_system/login.php HTTP/1.1
Cookie:
__cfduid=d49d060cf82d9f3d08d666cfbffb709ce1558927586;bdshare_firstime=1558927572005;capt
cha_3688958368=58301bc0f6a8f39ed1dcd9484ef2131c
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

Possible internal IP address disclosure

Severity	**Informational**
Reported by module	/Scripts/PerFolder/Invalid_Page_Text_Search.script

Description

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

Web Server

Details

Pattern found:

```
192.168.2.168
```

Request headers

```
GET /feed.php/pd3eRCvneI.jsp HTTP/1.1
Connection: keep-alive
Cookie: __cfduid=d43ae5e468ec3f365b9d50b98456d83f81558927330
Accept: */*
Accept-Encoding: gzip,deflate
Host: www.vbboy.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
```

/feed.php

Details

Pattern found:

```
192.168.2.168
```

Request headers

Possible server path disclosure (Unix)

Severity	**Informational**
Reported by module	/Scripts/PerFile/Text_Search_File.script

Description

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

References

[Full Path Disclosure (https://www.owasp.org/index.php/Full_Path_Disclosure)](https://www.owasp.org/index.php/Full_Path_Disclosure)

Affected items

/feed.php

Details

Pattern found:

```
/usr/share/applications/
```

Request headers

Scanned items (coverage report)

```
http://www.vbboy.com/
http://www.vbboy.com/cdn-cgi/
http://www.vbboy.com/cdn-cgi/images/
http://www.vbboy.com/cdn-cgi/l/
http://www.vbboy.com/cdn-cgi/l/email-protection
http://www.vbboy.com/cdn-cgi/scripts/
http://www.vbboy.com/cdn-cgi/scripts/5c5dd728/
http://www.vbboy.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/
http://www.vbboy.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js
http://www.vbboy.com/cdn-cgi/scripts/cf.common.js
http://www.vbboy.com/cdn-cgi/scripts/zepto.min.js
http://www.vbboy.com/cdn-cgi/styles/
http://www.vbboy.com/cdn-cgi/styles/cf.errors.css
http://www.vbboy.com/cdn-cgi/styles/fonts/
http://www.vbboy.com/feed.php
http://www.vbboy.com/index.php
http://www.vbboy.com/zb_system/
http://www.vbboy.com/zb_system/admin/
http://www.vbboy.com/zb_system/cmd.php
http://www.vbboy.com/zb_system/css/
http://www.vbboy.com/zb_system/css/admin.css
http://www.vbboy.com/zb_system/image/
http://www.vbboy.com/zb_system/image/admin/
http://www.vbboy.com/zb_system/image/common/
http://www.vbboy.com/zb_system/login.php
http://www.vbboy.com/zb_system/script/
http://www.vbboy.com/zb_system/script/c_admin_js_add.php
http://www.vbboy.com/zb_system/script/c_html_js_add.php
http://www.vbboy.com/zb_system/script/c_validcode.php
http://www.vbboy.com/zb_system/script/common.js
http://www.vbboy.com/zb_system/script/md5.js
http://www.vbboy.com/zb_system/xml-rpc/
http://www.vbboy.com/zb_system/xml-rpc/wlwmanifest.xml
http://www.vbboy.com/zb_users/
http://www.vbboy.com/zb_users/cache/
http://www.vbboy.com/zb_users/data/
http://www.vbboy.com/zb_users/logs/
http://www.vbboy.com/zb_users/plugin/
http://www.vbboy.com/zb_users/plugin/UEditor/
http://www.vbboy.com/zb_users/plugin/UEditor/php/
http://www.vbboy.com/zb_users/plugin/UEditor/themes/
http://www.vbboy.com/zb_users/plugin/UEditor/themes/default/
http://www.vbboy.com/zb_users/plugin/UEditor/themes/default/images/
http://www.vbboy.com/zb_users/plugin/UEditor/third-party/
http://www.vbboy.com/zb_users/plugin/UEditor/third-party/prism/
http://www.vbboy.com/zb_users/plugin/UEditor/third-party/prism/prism.css
http://www.vbboy.com/zb_users/plugin/UEditor/third-party/prism/prism.js
http://www.vbboy.com/zb_users/theme/
http://www.vbboy.com/zb_users/theme/default/
http://www.vbboy.com/zb_users/theme/default/include/
http://www.vbboy.com/zb_users/theme/default/script/
http://www.vbboy.com/zb_users/theme/fengyan/
http://www.vbboy.com/zb_users/theme/fengyan/style/
http://www.vbboy.com/zb_users/theme/fengyan/style/font-awesome-4.3.0/
http://www.vbboy.com/zb_users/theme/fengyan/style/font-awesome-4.3.0/css/
http://www.vbboy.com/zb_users/theme/fengyan/style/font-awesome-4.3.0/css/font-awesome.min.css
http://www.vbboy.com/zb_users/theme/fengyan/style/font-awesome-4.3.0/fonts/
http://www.vbboy.com/zb_users/theme/fengyan/style/font-awesome-4.3.0/fonts/fontawesome-webfont.woff2
http://www.vbboy.com/zb_users/theme/fengyan/style/iconfont/
http://www.vbboy.com/zb_users/theme/fengyan/style/images/
http://www.vbboy.com/zb_users/theme/fengyan/style/img/
http://www.vbboy.com/zb_users/theme/fengyan/style/js/
http://www.vbboy.com/zb_users/theme/fengyan/style/js/com.js
http://www.vbboy.com/zb_users/theme/fengyan/style/style.css
```

http://www.vbboy.com/zb_users/upload/
http://www.vbboy.com/zb_users/upload/2017/
http://www.vbboy.com/zb_users/upload/2017/12/
http://www.vbboy.com/zb_users/upload/2018/
http://www.vbboy.com/zb_users/upload/2018/03/
http://www.vbboy.com/zb_users/upload/2018/12/
http://www.vbboy.com/zb_users/upload/2019/
http://www.vbboy.com/zb_users/upload/2019/02/