acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

28 November, 2014

Developer Report

Generated by Acunetix WVS Reporter (v9.5 Build 20140602)

Scan of http://immortal-yiiframework.rhcloud.com:80/

Scan details

Scan information	
Start time	11/27/2014 11:44:53 PM
Finish time	11/27/2014 11:50:40 PM
Scan time	5 minutes, 47 seconds
Profile	XSS

Server information	
Responsive	True
Server banner	Apache/2.2.15 (Red Hat)
Server OS	Unix
Server technologies	

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	**3**
High	0
Medium	1
Low	0
Informational	2

Knowledge base

List of client scripts

These files contain Javascript code referenced from the website.

- /js/lightbox/js/lightbox.js
- /js/lightbox/js/jquery-1.7.2.min.js
- /js/lightbox/js/jquery-ui-1.8.18.custom.min.js
- /js/lightbox/js/jquery.smooth-scroll.min.js
- /js/nivo-slider/jquery.nivo.slider.pack.js
- /js/jquery-1.7.1.min.js
- /js/swfobject/swfobject.js
- /js/styleswitcher.js
- /js/bootstrap-transition.js
- /js/bootstrap-alert.js
- /js/bootstrap-modal.js
- /js/bootstrap-dropdown.js
- /js/bootstrap-scrollspy.js
- /js/bootstrap-tab.js
- /js/bootstrap-tooltip.js
- /js/bootstrap-popover.js
- /js/bootstrap-button.js
- /js/bootstrap-collapse.js
- /js/bootstrap-carousel.js
- /js/bootstrap-typeahead.js

- /assets/bd89a515/jquery.js
- /assets/bd89a515/jquery.yiiactiveform.js

List of files with inputs

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

- / - 2 inputs
- /index.php/site/page - 1 inputs
- /index.php/site/login - 1 inputs
- /index.php/site/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).

- fonts.googleapis.com
- ajax.googleapis.com
- placehold.it
- maps.google.com
- vimeo.com
- player.vimeo.com
- www.paypal.com
- jquery.com
- lokeshdhakar.com
- www.lokeshdhakar.com
- twitter.com
- github.com

Alerts summary

User credentials are sent in clear text

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-310

Affected items	Variation
/index.php/site/login	1

Broken links

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/index.php/site/index.php (8cadd22a9ed8800381bbe0cff85a9a7a)	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/index.php/site/login	1

Alert details

User credentials are sent in clear text

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

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

/index.php/site/login

Details

Form name: <empty>
Form action: http://immortal-yiiframework.rhcloud.com/index.php/site/login
Form method: POST

Form inputs:

- LoginForm[username] [Text]
- LoginForm[password] [Password]
- LoginForm[rememberMe] [Hidden]
- LoginForm[rememberMe] [Checkbox]
- yt0 [Submit]

Request headers

```
GET /index.php/site/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://immortal-yiiframework.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=3s349uht6fjob6nkobem4jhra1
Host: immortal-yiiframework.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Broken links

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

Description

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

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/index.php/site/index.php (8cadd22a9ed8800381bbe0cff85a9a7a)

Details

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

Request headers

```
GET /index.php/site/index.php?page=blog-item HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://immortal-yiiframework.rhcloud.com/index.php/site/page
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=3s349uht6fjob6nkobem4jhra1
Host: immortal-yiiframework.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Password type input with auto-complete enabled

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

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:
<INPUT TYPE="password" AUTOCOMPLETE="off">

Affected items

/index.php/site/login

Details

Password type input named LoginForm[password] from form with ID login-form with action /index.php/site/login has autocomplete enabled.

Request headers

```
GET /index.php/site/login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://immortal-yiiframework.rhcloud.com/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=3s349uht6fjob6nkobem4jhra1
Host: immortal-yiiframework.rhcloud.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Scanned items (coverage report)

Scanned 72 URLs. Found 1 vulnerable.

URL: http://immortal-yiiframework.rhcloud.com/

No vulnerabilities has been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
.php/	Path Fragment
/	Path Fragment
/	Path Fragment

Input scheme 2	
Input name	Input type
Host	HTTP Header

URL: http://immortal-yiiframework.rhcloud.com/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/css/style3.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/css/style2.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/css/style1.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/css/style6.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/css/style5.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/css/style4.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/css/template.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/css/bootstrap.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/css/bootstrap-responsive.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/ico/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/icons/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/icons/social/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/icons/fatcow/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/icons/smashing/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/icons/smashing/60px/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/slider/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/slider/flickr/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/customers/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/backgrounds/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/portfolio/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/img/blog/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/index.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/index.php/site

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/index.php/site/page

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
view	URL encoded GET

URL: http://immortal-yiiframework.rhcloud.com/index.php/site/login

Vulnerabilities has been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
LoginForm%5bpassword%5d	URL encoded POST
LoginForm%5brememberMe%5d	URL encoded POST
LoginForm%5busername%5d	URL encoded POST
yt0	URL encoded POST

URL: http://immortal-yiiframework.rhcloud.com/index.php/site/index

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/index.php/site/img

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/index.php/site/img/portfolio

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/index.php/site/index.php

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
page	URL encoded GET

URL: http://immortal-yiiframework.rhcloud.com/js/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/css/lightbox.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/css/screen.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/js/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/js/lightbox.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/js/jquery-1.7.2.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/js/jquery-ui-1.8.18.custom.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/js/jquery.smooth-scroll.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/images/examples

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/releases

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/lightbox/img

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/nivo-slider/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/nivo-slider/nivo-slider.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/nivo-slider/themes/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/nivo-slider/themes/default/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/nivo-slider/themes/default/default.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/nivo-slider/jquery.nivo.slider.pack.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/jquery-1.7.1.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/swfobject/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/swfobject/swfobject.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/styleswitcher.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-transition.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-alert.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-modal.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-dropdown.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-scrollspy.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-tab.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-tooltip.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-popover.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-button.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-collapse.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-carousel.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/js/bootstrap-typeahead.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/assets/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/assets/bd89a515/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/assets/bd89a515/jquery.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://immortal-yiiframework.rhcloud.com/assets/bd89a515/jquery.yiiactiveform.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL