acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

15 September, 2017

Developer Report

Generated by Acunetix WVS Reporter (v9.0 Build 20131107)

Scan of http://apps.career.undip.ac.id:80/

Scan details

Scan information	
Start time	15/09/2017 14.04.18
Finish time	15/09/2017 14.59.09
Scan time	54 minutes, 52 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache
Server OS	Unknown
Server technologies	

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been 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	**43**
High	0
Medium	15
Low	11
Informational	17

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:

- gitignore => 1 file(s)
- js => 13 file(s)
- css => 7 file(s)
- ttf => 3 file(s)
- svg => 3 file(s)
- eot => 3 file(s)
- woff => 3 file(s)
- woff2 => 2 file(s)
- html => 1 file(s)
- txt => 1 file(s)
- config => 1 file(s)

Top 10 response times

The files listed below had the slowest response times measured during the crawling process. The average response time for this site was 334,37 ms. These files could be targetted in denial of service attacks.

1. /index.php/uploads/2017-07, response time 609 ms

GET /index.php/uploads/2017-07 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie:
XSRF-TOKEN=eyJpdiI6ImtqMjVsY09NYkE3QSs3TnhTcnBYMVE9PSIsInZhbHVlIjoiMloxM0NqVEN2MUlyVDdLQXRKdmJ3RnlyYnAxYTR5c2lyTXdSaENrTmhwbDJvcWpPSnZnWXZEZStGZzBJZk40UzJINDc1WjlQb29ENGVNVEFFRmJxRXc9PSIsIm1hYyI6IjQ0NzI2MzdmNWIwMmNiZjhlMzBmMmY3YjlkN2ZmZmQ0NDk2YmYxYzQ4MDc5N2Y2ZmUyODhlNWU5MGJmOTRjMjYifQ%3D%3D;
laravel_session=eyJpdiI6ImNzNHRQd2JZRFZNS3Y0TlpBdlpGaFE9PSIsInZhbHVlIjoiK29NWU5QMjJJK3Bqd3JQODB2WkJPR2dSZkNuMnRqZ0xmWDE4VGh5aWQxaU5ScEVUTGJra2xYSEdWQ2Q0WG9aUmxURU9VM09xaW1HeXNLdmQwZTNia2c9PSIsIm1hYyI6Ijk3NmUwMzdiNTY4MTMwODM5NTI4ZDViOTE4MzQwMTQ1ODJiNDY3NjYzZDdlNjU0YWQ1NDExYmNmOGQyMWJmNjUifQ%3D%3D
Host: apps.career.undip.ac.id
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
2. /index.php/Respond.js, response time 531 ms

GET /index.php/Respond.js HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/index.php/search
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie:
XSRF-TOKEN=eyJpdiI6ImtqMjVsY09NYkE3QSs3TnhTcnBYMVE9PSIsInZhbHVlIjoiMloxM0NqVEN2MUlyVDdLQXRKdmJ3RnlyYnAxYTR5c2lyTXdSaENrTmhwbDJvcWpPSnZnWXZEZStGZzBJZk40UzJINDc1WjlQb29ENGVNVEFFRmJxRXc9PSIsIm1hYyI6IjQ0NzI2MzdmNWIwMmNiZjhlMzBmMmY3YjlkN2ZmZmQ0NDk2YmYxYzQ4MDc5N2Y2ZmUyODhlNWU5MGJmOTRjMjYifQ%3D%3D;
laravel_session=eyJpdiI6ImNzNHRQd2JZRFZNS3Y0TlpBdlpGaFE9PSIsInZhbHVlIjoiK29NWU5QMjJJK3Bqd3JQODB2WkJPR2dSZkNuMnRqZ0xmWDE4VGh5aWQxaU5ScEVUTGJra2xYSEdWQ2Q0WG9aUmxURU9VM09xaW1HeXNLdmQwZTNia2c9PSIsIm1hYyI6Ijk3NmUwMzdiNTY4MTMwODM5NTI4ZDViOTE4MzQwMTQ1ODJiNDY3NjYzZDdlNjU0YWQ1NDExYmNmOGQyMWJmNjUifQ%3D%3D
Host: apps.career.undip.ac.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (

List of client scripts

These files contain Javascript code referenced from the website.

- /plugins/flexslider/jquery.flexslider-min.js
- /plugins/bootstrap/js/bootstrap.min.js
- /plugins/pretty-photo/js/jquery.prettyPhoto.js
- /plugins/jquery-1.12.3.min.js
- /plugins/bootstrap-hover-dropdown.min.js
- /plugins/back-to-top.js
- /plugins/jquery-placeholder/jquery.placeholder.js
- /plugins/jquery-placeholder/tests/tests.js
- /plugins/jflickrfeed/jflickrfeed.min.js
- /js/main.js

List of files with inputs

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

- / - 4 inputs
- /search - 1 inputs
- /contact - 1 inputs
- /plugins/font-awesome/fonts/icomoon.ttf - 1 inputs

- /plugins/font-awesome/fonts/icomoon.svg - 1 inputs
- /plugins/font-awesome/fonts/icomoon.eot - 1 inputs
- /plugins/font-awesome/fonts/icomoon.woff - 1 inputs
- /plugins/font-awesome/fonts/fontawesome-webfont.svg - 1 inputs
- /plugins/font-awesome/fonts/fontawesome-webfont.ttf - 1 inputs
- /plugins/font-awesome/fonts/fontawesome-webfont.eot - 1 inputs
- /plugins/font-awesome/fonts/fontawesome-webfont.woff - 1 inputs
- /plugins/font-awesome/fonts/fontawesome-webfont.woff2 - 1 inputs
- /plugins/pretty-photo/xhr_response.html - 1 inputs
- /plugins/jquery-placeholder/tests - 4 inputs
- /index.php/search - 1 inputs
- /index.php/contact - 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
- www.google.com
- twitter.com
- plus.google.com
- www.linkedin.com
- www.facebook.com
- localhost
- youtu.be
- www.youtube.com
- nmfe.co
- www.google.ca
- vimeo.com
- www.adobe.com
- trailers.apple.com
- www.no-margin-for-errors.com
- ajax.googleapis.com
- maps.google.com
- code.jquery.com

List of email addresses

List of all email addresses found on this host.

- address@example.ext

Alerts summary

Application error message

Affects	Variation
/	1
/contact	3
/index.php/contact	3

Error message on page

Affects	Variation
/index.php/news/%20kategori-a	1
/news/%20kategori-a	1

HTML form without CSRF protection

Affects	Variation
/	1
/plugins/jquery-placeholder/tests	1

Password field submitted using GET method

Affects	Variation
/plugins/jquery-placeholder/tests	1

Source code disclosure

Affects	Variation
/index.php/responses	1
/responses	1

User credentials are sent in clear text

Affects	Variation
/plugins/jquery-placeholder/tests	1

Clickjacking: X-Frame-Options header missing

Affects	Variation
Web Server	1

Documentation file

Affects	Variation
/plugins/pretty-photo/README	1

OPTIONS method is enabled

Affects	Variation
Web Server	1

Possible sensitive directories

Affects	Variation
/plugins/jquery-placeholder/tests	1
/uploads	1

Possible sensitive files

Affects	Variation
/uploads/.gitignore	1
/web.config	1

Sensitive page could be cached

Affects	Variation
/plugins/jquery-placeholder/tests (cbd4237ed51ff081eb8f66f230b05f50)	1

Session Cookie without HttpOnly flag set

Affects	Variation
/	1

Session Cookie without Secure flag set

Affects	Variation
/	2

Content type is not specified

Affects	Variation
/plugins/bootstrap/fonts/glyphicons-halflings-regular.woff2	1
/plugins/font-awesome/fonts/fontawesome-webfont.woff2	1
/plugins/font-awesome/fonts/fontawesome-webfont.woff2 (5862d25f39771f43cac31b2a71d2973f)	1
/plugins/pretty-photo/README	1
/uploads/.gitignore	1
/web.config	1

Email address found

Affects	Variation
/plugins/jquery-placeholder/tests	1

Password type input with auto-complete enabled

Affects	Variation
/plugins/jquery-placeholder/tests	1

Possible internal IP address disclosure

Affects	Variation
/index.php/news/	1
/index.php/news/%20kategori-a	1
/index.php/news/%20kategori-a/	1
/index.php/news/kategori-a/	1
/news/	1
/news/%20kategori-a	1
/news/%20kategori-a/	1
/news/kategori-a/	1

Possible username or password disclosure

Affects	Variation
/plugins/font-awesome/css/font-awesome.css	1

Alert details

Application error message

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

Description

This page contains an error/warning message that may disclose sensitive information.The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

PHP Runtime Configuration

Affected items

/

Details

Path Fragment input / was set to 268435455
Error message found: Internal Server Error

Request headers

```
GET /news/%20kategori-a/268435455 HTTP/1.1
Referer: http://apps.career.undip.ac.id:80/
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*
```

/contact

Details

URL encoded POST input message was set to 268435455
Error message found: Internal Server Error

Request headers

```
POST /contact HTTP/1.1
Content-Length: 123
Content-Type: application/x-www-form-urlencoded
Referer: http://apps.career.undip.ac.id:80/
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVM
```

```
yc3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE
4elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzB
hZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*

email=sample%40email.tst&message=268435455&name=fpusbmxk&phone=555-666-0606&_token=VezIb
YRtz0J2S0bqQ03zS70OYnQtLHsJoA5RuONL
```

/contact

Details

URL encoded POST input name was set to %e3h
Error message found: Internal Server Error

Request headers

```
POST /contact HTTP/1.1
Content-Length: 112
Content-Type: application/x-www-form-urlencoded
Referer: http://apps.career.undip.ac.id:80/
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*

email=sample%40email.tst&message=20&name=%e3h&phone=555-666-0606&_token=VezIbYRtz0J2S0bq
Q03zS70OYnQtLHsJoA5RuONL
```

/contact

Details

URL encoded POST input phone was set to %e3h
Error message found: Internal Server Error

Request headers

```
POST /contact HTTP/1.1
Content-Length: 108
Content-Type: application/x-www-form-urlencoded
Referer: http://apps.career.undip.ac.id:80/
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*

email=sample%40email.tst&message=20&name=fpusbmxk&phone=%e3h&_token=VezIbYRtz0J2S0bqQ03
```

```
zS70OYnQtLHsJoA5RuONL
```

/index.php/contact

Details

URL encoded POST input message was set to %e3h
Error message found: Internal Server Error

Request headers

```
POST /index.php/contact HTTP/1.1
Content-Length: 118
Content-Type: application/x-www-form-urlencoded
Referer: http://apps.career.undip.ac.id:80/
(line truncated)
...YTFhWGtlWDZuTjNXT2p3Zk5USXhwQmNielwvdytscTNSYTFhdlk4U09WakJTU040XC9lcFZkZThDb2tXN2NsW
VhlTEcyRWVXUndCUT09IiwibWFjIjoiMzU2NDg3ZjEwNjkzOTcwZjQ2MmI2ZGVjMmRkMjA5ZmYxZTYwZjU3YTFhZ
jVjZTBkMzEwZjY4YWYzNTNkZWRhZCJ9;
laravel_session=eyJpdiI6Img4NFl1bHFcL0pyb1NtNEtaSE84czRRPT0iLCJ2YWx1ZSI6ImpyUElON2FZSVJ1
elhSKzV4TU83UDV1NkVXTVlwMm9pTlMyMERRdm9VZVhrUXpSMVVYNGFmZURJRnhrdndlTDUwT2V3RCthT2l3SlB0
NTVueUw4Z3lnPT0iLCJtYWMiOiIyZDc0NjhlZjAxZWMzYjVkOThkZjgzZDgyNjc1YzJjNDZhODlhNTdjZjZiZDI3
NDA5NTY3NzZhYjQ2YzUwMTg2In0%3D
Host: apps.career.undip.ac.id
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: */*

email=sample%40email.tst&message=%e3h&name=nimtkmgx&phone=555-666-0606&_token=VezIbYRtz0
J2S0bqQ03zS70OYnQtLHsJoA5RuONL
```

/index.php/contact

Details

URL encoded POST input name was set to %e3h
Error message found: Internal Server Error

Request headers

```
POST /index.php/contact HTTP/1.1
Content-Length: 112
Content-Type: application/x-www-form-urlencoded
Referer: http://apps.career.undip.ac.id:80/
(line truncated)
...YTFhWGtlWDZuTjNXT2p3Zk5USXhwQmNielwvdytscTNSYTFhdlk4U09WakJTU040XC9lcFZkZThDb2tXN2NsW
VhlTEcyRWVXUndCUT09IiwibWFjIjoiMzU2NDg3ZjEwNjkzOTcwZjQ2MmI2ZGVjMmRkMjA5ZmYxZTYwZjU3YTFhZ
jVjZTBkMzEwZjY4YWYzNTNkZWRhZCJ9;
laravel_session=eyJpdiI6Img4NFl1bHFcL0pyb1NtNEtaSE84czRRPT0iLCJ2YWx1ZSI6ImpyUElON2FZSVJ1
elhSKzV4TU83UDV1NkVXTVlwMm9pTlMyMERRdm9VZVhrUXpSMVVYNGFmZURJRnhrdndlTDUwT2V3RCthT2l3SlB0
NTVueUw4Z3lnPT0iLCJtYWMiOiIyZDc0NjhlZjAxZWMzYjVkOThkZjgzZDgyNjc1YzJjNDZhODlhNTdjZjZiZDI3
NDA5NTY3NzZhYjQ2YzUwMTg2In0%3D
Host: apps.career.undip.ac.id
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: */*

email=sample%40email.tst&message=20&name=%e3h&phone=555-666-0606&_token=VezIbYRtz0J2S0bq
Q03zS70OYnQtLHsJoA5RuONL
```

/index.php/contact

Details

URL encoded POST input phone was set to %e3h
Error message found: Internal Server Error

Request headers

```
POST /index.php/contact HTTP/1.1
Content-Length: 108
Content-Type: application/x-www-form-urlencoded
Referer: http://apps.career.undip.ac.id:80/
```

```
(line truncated)
...YTFhWGtlWDZuTjNXT2p3Zk5USXhwQmNielwvdytscTNSYTFhdlk4U09WakJTU040XC9lcFZkZThDb2tXN2NsW
VhlTEcyRWVXUndCUT09IiwibWFjIjoiMzU2NDg3ZjEwNjkzOTcwZjQ2MmI2ZGVjMmRkMjA5ZmYxZTYwZjU3YTFhZ
jVjZTBkMzEwZjY4YWYzNTNkZWRhZCJ9;
laravel_session=eyJpdiI6Img4NFl1bHFcL0pyb1NtNEtaSE84czRRPT0iLCJ2YWx1ZSI6ImpyUElON2FZSVJ1
elhSKzV4TU83UDV1NkVXTVlwMm9pTlMyMERRdm9VZVhrUXpSMVVYNGFmZURJRnhrdndlTDUwT2V3RCthT2l3SlB0
NTVueUw4Z3lnPT0iLCJtYWMiOiIyZDc0NjhlZjAxZWMzYjVkOThkZjgzZDgyNjc1YzJjNDZhODlhNTdjZjZiZDI3
NDA5NTY3NzZhYjQ2YzUwMTg2In0%3D
Host: apps.career.undip.ac.id
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: */*

email=sample%40email.tst&message=20&name=nimtkmgx&phone=%e3h&_token=VezIbYRtz0J2S0bqQ03z
S70OYnQtLHsJoA5RuONL
```

Error message on page

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Text_Search_Dir.script)

Description

This page contains an error/warning message that may disclose sensitive information.The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

PHP Runtime Configuration

Affected items

/index.php/news/%20kategori-a

Details

Pattern found: Internal Server Error

Request headers

```
GET /index.php/news/%20kategori-a HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...RKdmJ3RnlyYnAxYTR5c2lyTXdSaENrTmhwbDJvcWpPSnZnWXZEZStGZzBJZk40UzJINDc1WjlQb29ENGVNVEF
FRmJxRXc9PSIsIm1hYyI6IjQ0NzI2MzdmNWIwMmNiZjhlMzBmMmY3YjlkN2ZmZmQ0NDk2YmYxYzQ4MDc5N2Y2ZmU
yODhlNWU5MGJmOTRjMjYifQ%3D%3D;
laravel_session=eyJpdiI6ImNzNHRQd2JZRFZNS3Y0TlpBdlpGaFE9PSIsInZhbHVlIjoiK29NWU5QMjJJK3Bq
d3JQODB2WkJPR2dSZkNuMnRqZ0xmWDE4VGh5aWQxaU5ScEVUTGJra2xYSEdWQ2Q0WG9aUmxURU9VM09xaW1HeXNL
dmQwZTNia2c9PSIsIm1hYyI6Ijk3NmUwMzdiNTY4MTMwODM5NTI4ZDViOTE4MzQwMTQ1ODJiNDY3NjYzZDdlNjU0
YWQ1NDExYmNmOGQyMWJmNjUifQ%3D%3D
Host: apps.career.undip.ac.id
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: */*
```

/news/%20kategori-a

Details

Pattern found: Internal Server Error

Request headers

```
GET /news/%20kategori-a HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
```

```
...dcLzY0ZWlDWk94YlwvUktxNUZZU01vcnpxZ0xOMldhVHZWc3RNeGh6OUpuOWhYMFgyc25yYUtNUjlaTmxYSjR
ybkdXQ2N2a2c9PSIsIm1hYyI6IjQ5MDlhMzg1M2FjNGViZTc1MDhlNmIyYmI1ZGFhYjJiNTg3NTgzMDU0ZDY2Zjg
wMmY4MjY0ZmU3MzRiNDYzNzEifQ%3D%3D;
laravel_session=eyJpdiI6ImtHM2VjYXNzUENZdldUbitVZ3gzdVE9PSIsInZhbHVlIjoiXC9rUmo0KzZhdE9w
SVJXcDNaOXU0bmZ5YWJVRlpEVStKTTd1Yk1ZY0FyQmRcL0NlWTZaZ3VTdFlWYVVRd2V3eXpDUGFZUHFMVUdvK2F2
dnFKV013NDJEZz09IiwibWFjIjoiNWJiMWJlZTViM2I3YzhhZjgxZDI1Y2E4OGMyYTI3ZDEwZDgwMTYzYTA0ZTUx
NjEwY2I0NzgwYThlNWY2YzQ1MCJ9
Host: apps.career.undip.ac.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

HTML form without CSRF protection

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

Description

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

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

Impact

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

Recommendation

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

Affected items

/

Details

Form name: <empty>
Form action: http://apps.career.undip.ac.id/search
Form method: GET

Form inputs:

- q [Text]

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...NWRnZlMwWHVqbkZpeVRERTc4NVVOMVVqcWV2WGw5TGtxeHRaTGRSY2ZIcE4wUkt1Z3B2NmlYaWdKcVwvZWt3T
GxRdTM3TDh5ZVwvUT09IiwibWFjIjoiMmYxODFiNjY4MTk2Y2EzOTcxOWE5ZWJjN2MzM2RkNjA2ZmVlNTUyZDQ2M
Tk0OTYzODNjYTA4MjE5YmY0YzQ4OCJ9;
laravel_session=eyJpdiI6Ik9UNVoyYU9uVHNTNWhUVFUwVnc0SlE9PSIsInZhbHVlIjoiMUNUXC9NS1paRmpj
bjhSeVZOSDlpdkZhV096VDB4Z0xzTnEybzNvN0VjY21qbUhjdWl2RWVQdlJOTGwzcXJ4NUMxaHVKM3h0QzJKajYw
dDNFakhKRlBRPT0iLCJtYWMiOiJiNDE3MTMwOTAxMDQ0M2U2YzVkYzVkNjI0YjE2OTI3NjNhMjNmNmY0MzA2Y2Mx
NTUwOWZmMDQyNDc3YmMzNDE0In0%3D
Host: apps.career.undip.ac.id
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: */*
```

/plugins/jquery-placeholder/tests

Details

Form name: <empty>
Form action: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/
Form method: GET

Form inputs:

- search [Text]
- name [Text]
- email [Text]
- url [Text]
- tel [Text]
- password [Password]
- message [TextArea]

Request headers

```
GET /plugins/jquery-placeholder/tests/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...R2SGd5RElpNW03RXBmSzR2NjlSekNScGQrNEhPSzhRZFhoUWVWTnR6NGdPa1U3OTFJQlZzYUlNNHRqYUV0OHp
2Q2F1UW5ldz09IiwibWFjIjoiMGU5MmM2ZTJmYWM3ZDVhODgyYTAwNjk0ZjE3ZjBjNDEzNTYxMzhkYzY0NTJhNTN
jMTA5MTg1MGRlYjM0NDk3ZSJ9;
laravel_session=eyJpdiI6IndWMFVPcnQ0VGxxamJJeUMyS0RcL3hRPT0iLCJ2YWx1ZSI6InV1M1dVOW9tY1wv
SzdHT3pLY3FXOEJVYXBKeHlFamxDSVYwXC9hVENtQURVTUl1aTRaWkdVdVpCMEoxQXA5RHRNWmdRT2JNbXZPcGpK
OTRNcHBObmFyUFE9PSIsIm1hYyI6ImJkYTE1ODUwMTE5YjU0NDYzZDRiMTE2YTUwNWI5MzNlMTYwZWI2MWY3MzIy
ZjM4YzBhNGYxMWQ3OWFmYmY0YTMifQ%3D%3D
Host: apps.career.undip.ac.id
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 field submitted using GET method

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

Description

This page contains a form with a password field. This form submits user data using the GET method, therefore the contents of the password field will appear in the URL. Sensitive information should not be passed via the URL. URLs could be logged or leaked via the Referer header.

Impact

Possible sensitive information disclosure.

Recommendation

The password field should be submitted through POST instead of GET.

Affected items

/plugins/jquery-placeholder/tests

Details

form name: "<unnamed>"
form action: ""
password input: "password"

Request headers

```
GET /plugins/jquery-placeholder/tests/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...R2SGd5RElpNW03RXBmSzR2NjlSekNScGQrNEhPSzhRZFhoUWVWTnR6NGdPa1U3OTFJQlZzYUlNNHRqYUV0OHp
2Q2F1UW5ldz09IiwibWFjIjoiMGU5MmM2ZTJmYWM3ZDVhODgyYTAwNjk0ZjE3ZjBjNDEzNTYxMzhkYzY0NTJhNTN
jMTA5MTg1MGRlYjM0NDk3ZSJ9;
laravel_session=eyJpdiI6IndWMFVPcnQ0VGxxamJJeUMyS0RcL3hRPT0iLCJ2YWx1ZSI6InV1M1dVOW9tY1wv
SzdHT3pLY3FXOEJVYXBKeHlFamxDSVYwXC9hVENtQURVTUl1aTRaWkdVdVpCMEoxQXA5RHRNWmdRT2JNbXZPcGpK
OTRNcHBObmFyUFE9PSIsIm1hYyI6ImJkYTE1ODUwMTE5YjU0NDYzZDRiMTE2YTUwNWI5MzNlMTYwZWI2MWY3MzIy
ZjM4YzBhNGYxMWQ3OWFmYmY0YTMifQ%3D%3D
Host: apps.career.undip.ac.id
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: */*
```

Source code disclosure

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Text_Search_File.script)

Description

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

Impact

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

Recommendation

Remove this file from your website or change its permissions to remove access.

References

Source Code Disclosure Can Be Exploited On Your Website

Affected items

/index.php/responses

Details

Pattern found: <%-([\s\S]+?)%>

Request headers

```
GET /index.php/responses HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...R2SGd5RElpNW03RXBmSzR2NjlSekNScGQrNEhPSzhRZFhoUWVWTnR6NGdPa1U3OTFJQlZzYUlNNHRqYUV0OHp
2Q2F1UW5ldz09IiwibWFjIjoiMGU5MmM2ZTJmYWM3ZDVhODgyYTAwNjk0ZjE3ZjBjNDEzNTYxMzhkYzY0NTJhNTN
jMTA5MTg1MGRlYjM0NDk3ZSJ9;
laravel_session=eyJpdiI6IndWMFVPcnQ0VGxxamJJeUMyS0RcL3hRPT0iLCJ2YWx1ZSI6InV1M1dVOW9tY1wv
SzdHT3pLY3FXOEJVYXBKeHlFamxDSVYwXC9hVENtQURVTUl1aTRaWkdVdVpCMEoxQXA5RHRNWmdRT2JNbXZPcGpK
OTRNcHBObmFyUFE9PSIsIm1hYyI6ImJkYTE1ODUwMTE5YjU0NDYzZDRiMTE2YTUwNWI5MzNlMTYwZWI2MWY3MzIy
ZjM4YzBhNGYxMWQ3OWFmYmY0YTMifQ%3D%3D
Host: apps.career.undip.ac.id
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: */*
```

/responses

Details

Pattern found: <%-([\s\S]+?)%>

Request headers

```
GET /responses HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
```

```
(line truncated)
...pTenhZNDhmbWhKUDlnVFwvd1MrWVFlaXozSFwvV3h4ek1iTE9JNkZNWFMzcXJWQXBCQUhXRjRPUkt2U1JQT3d
QV3VuY2lrN0E9PSIsIm1hYyI6ImQ4NGJmYzlhYjQxZmQ3MTY4NTUxMDBlODhlYTE2NjRmY2I4YmFiMDE4NzI0NWZ
jMWI3OTIxYjQzYzRiYTU2MDAifQ%3D%3D;
laravel_session=eyJpdiI6InNTRU8zcWN5Sk52ZEd3WUhFYlZiMGc9PSIsInZhbHVlIjoiaG1iS0FtMUFZVlJu
M3Zzc1pwdUN6WUp2Q1p0TVwvM2FjbnY3YitNcmV1VFVOcm9hZUxFVFZrY24wUDRXMFBcL3l0YWpRbDQ3WWFmanF2
WjZVdStwTUE4QT09IiwibWFjIjoiOGEzY2Q0NDZjODA4MDZkZDAwZDAzNTMxNGVjNjAzMDVkMjI5YzM0MjMzZmQz
MzU3MmQ1NTU3NTdhNGM5NDMyZiJ9
Host: apps.career.undip.ac.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

User credentials are sent in clear text

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

Description

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

Impact

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

Recommendation

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

Affected items

/plugins/jquery-placeholder/tests

Details

Form name: <empty>
Form action: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/
Form method: GET

Form inputs:

- search [Text]
- name [Text]
- email [Text]
- url [Text]
- tel [Text]
- password [Password]
- message [TextArea]

Request headers

```
GET /plugins/jquery-placeholder/tests/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...R2SGd5RElpNW03RXBmSzR2NjlSekNScGQrNEhPSzhRZFhoUWVWTnR6NGdPa1U3OTFJQlZzYUlNNHRqYUV0OHp
2Q2F1UW5ldz09IiwibWFjIjoiMGU5MmM2ZTJmYWM3ZDVhODgyYTAwNjk0ZjE3ZjBjNDEzNTYxMzhkYzY0NTJhNTN
jMTA5MTg1MGRlYjM0NDk3ZSJ9;
laravel_session=eyJpdiI6IndWMFVPcnQ0VGxxamJJeUMyS0RcL3hRPT0iLCJ2YWx1ZSI6InV1M1dVOW9tY1wv
SzdHT3pLY3FXOEJVYXBKeHlFamxDSVYwXC9hVENtQURVTUl1aTRaWkdVdVpCMEoxQXA5RHRNWmdRT2JNbXZPcGpK
OTRNcHBObmFyUFE9PSIsIm1hYyI6ImJkYTE1ODUwMTE5YjU0NDYzZDRiMTE2YTUwNWI5MzNlMTYwZWI2MWY3MzIy
ZjM4YzBhNGYxMWQ3OWFmYmY0YTMifQ%3D%3D
Host: apps.career.undip.ac.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

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

Affected items

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
(line truncated)
...A2citLZEhcL0M3ZlltRlJHbndoZkhNY1FGcm11OEI2RW9uN0JhSnRhd0FWb3lZd3ZzUmp1NFF3Z2xxclVHZW9
RUU9kMkZBPT0iLCJtYWMiOiJkOTk3ZTE3MjViOGZkOGU3YTlhMmY4NzNkNzE4MjRkMWZmZmQ5NDEwZjdiYmUxZTh
hMjBlODJkYzg5OWJkNzcxIn0%3D;
laravel_session=eyJpdiI6IjZkTXZOQ2RLM21sM1g0aXViVFZsNlE9PSIsInZhbHVlIjoibUM2azgwTHRTSHly
eVRpXC9HUmY0MEJieUM5a05nWXdkYmlWRFZpTStqT3ptME16ZURWVlwvNENhZGtob1VSYXEwRk9DVWF0NTVQVUR1
TFwvTUZEQ1pcL1NBPT0iLCJtYWMiOiI3NmQ2NzcxMGNkZDMyNjZjNTg2MDY2OWUyNjA0YTAwNzkzMzVjZGM0Y2Q2
NzFhMWIzYjQyYWYzNTcwOTUyMTgzIn0%3D
Host: apps.career.undip.ac.id
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: */*
```

Documentation file

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Readme_Files.script)

Description

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Remove or restrict access to all documentation file acessible from internet.

Affected items

/plugins/pretty-photo/README

Details

File contents (first 250 characters):prettyPhoto v3.1.4
Â© Copyright, Stephane Caron
http://www.no-margin-for-errors.com

============================== Released under ==============================

Creative Commons 2.5
http://creativecommons.org/licenses/by/2.5/

OR

GPLV2 license
http ...

Request headers

```
GET /plugins/pretty-photo/README HTTP/1.1
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*
```

OPTIONS method is enabled

Severity	**Low**
Type	Validation
Reported by module	Scripting (Options_Server_Method.script)

Description

HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

Impact

The OPTIONS method may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

It's recommended to disable OPTIONS Method on the web server.

References

Testing for HTTP Methods and XST (OWASP-CM-008)

Affected items

Web Server

Details

Methods allowed: GET,HEAD

Request headers

```
OPTIONS / HTTP/1.1
(line truncated)
...I0cFZ1V3VIVHZkNStqR1pJWjYxSTV3TTV6XC9KMzNPbmlzbGU5WUNoQmQyTjhpV0NIaFJ0U0podDdieWNcLzl
rOTNmdzRXQ2kwWHNyUT09IiwibWFjIjoiNGU5M2NjMmRjYTFlZDJkN2Y3NzhiNGZmZDhlYThlMDUyMDUyNGU5YzY
1YjFhNjc3YjAxNmM3YzE4ZGNkYWY0MyJ9;
laravel_session=eyJpdiI6IjJSZkN0T3JPR2hNXC8zM0V5M0JMM0ZBPT0iLCJ2YWx1ZSI6IkRTcU4xcmJESzFD
enpUK0VBTnJcLzZDTHByUGFYakgyWTlJdXdDZHp1Y1RLeHY4RVZnK1JtMWw0S0NsUGtlY1N4OVM4U0k2ajhaaEZN
VklRTHRhZEhyZz09IiwibWFjIjoiNGE4NzQ0ZjYxNTE4MWI4OGNlMjViYTA5ZWU2ODU1YjkyYzdhMTk1NDM0YmQ3
ZTM5ZTVhMGE1MzE1ZTMwNzBjOSJ9
Host: apps.career.undip.ac.id
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: */*
```

Possible sensitive directories

Severity	**Low**
Type	Validation
Reported by module	Scripting (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

Affected items

/plugins/jquery-placeholder/tests

Details

No details are available.

Request headers

```
GET /plugins/jquery-placeholder/tests HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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
```

/uploads

Details

No details are available.

Request headers

```
GET /uploads HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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
```

Possible sensitive files

Severity	**Low**
Type	Validation
Reported by module	Scripting (Possible_Sensitive_Files.script)

Description

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

Impact

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

Recommendation

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

References

Web Server Security and Database Server Security

Affected items

/uploads/.gitignore

Details

No details are available.

Request headers

```
GET /uploads/.gitignore HTTP/1.1
Accept: acunetix/wvs
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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
```

/web.config

Details

No details are available.

Request headers

```
GET /web.config HTTP/1.1
Accept: acunetix/wvs
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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
```

Sensitive page could be cached

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

Description

This page contains possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent caching by adding "Cache Control: No-store" to the page headers.

Affected items

/plugins/jquery-placeholder/tests (cbd4237ed51ff081eb8f66f230b05f50)

Details

No details are available.

Request headers

```
GET
/plugins/jquery-placeholder/tests/?email=sample%40email.tst&message=20&name=psmmtkrg&pas
sword=g00dPa%24%24w0rD&search=&tel=555-666-0606&url=1 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...RKdmJ3RnlyYnAxYTR5c2lyTXdSaENrTmhwbDJvcWpPSnZnWXZEZStGZzBJZk40UzJINDc1WjlQb29ENGVNVEF
FRmJxRXc9PSIsIm1hYyI6IjQ0NzI2MzdmNWIwMmNiZjhlMzBmMmY3YjlkN2ZmZmQ0NDk2YmYxYzQ4MDc5N2Y2ZmU
yODhlNWU5MGJmOTRjMjYifQ%3D%3D;
laravel_session=eyJpdiI6ImNzNHRQd2JZRFZNS3Y0TlpBdlpGaFE9PSIsInZhbHVlIjoiK29NWU5QMjJJK3Bq
d3JQODB2WkJPR2dSZkNuMnRqZ0xmWDE4VGh5aWQxaU5ScEVUTGJra2xYSEdWQ2Q0WG9aUmxURU9VM09xaW1HeXNL
dmQwZTNia2c9PSIsIm1hYyI6Ijk3NmUwMzdiNTY4MTMwODM5NTI4ZDViOTE4MzQwMTQ1ODJiNDY3NjYzZDdlNjU0
YWQ1NDExYmNmOGQyMWJmNjUifQ%3D%3D
Host: apps.career.undip.ac.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Session Cookie without HttpOnly flag set

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

Description

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

Impact

None

Recommendation

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

Affected items

/

Details

Cookie name: "XSRF-TOKEN"
Cookie domain: "apps.career.undip.ac.id"

Request headers

```
GET / HTTP/1.1
(line truncated)
...A2citLZEhcL0M3ZlltRlJHbndoZkhNY1FGcm11OEI2RW9uN0JhSnRhd0FWb3lZd3ZzUmp1NFF3Z2xxclVHZW9
RUU9kMkZBPT0iLCJtYWMiOiJkOTk3ZTE3MjViOGZkOGU3YTlhMmY4NzNkNzE4MjRkMWZmZmQ5NDEwZjdiYmUxZTh
hMjBlODJkYzg5OWJkNzcxIn0%3D;
laravel_session=eyJpdiI6IjZkTXZOQ2RLM21sM1g0aXViVFZsNlE9PSIsInZhbHVlIjoibUM2azgwTHRTSHly
eVRpXC9HUmY0MEJieUM5a05nWXdkYmlWRFZpTStqT3ptME16ZURWVlwvNENhZGtob1VSYXEwRk9DVWF0NTVQVUR1
TFwvTUZEQ1pcL1NBPT0iLCJtYWMiOiI3NmQ2NzcxMGNkZDMyNjZjNTg2MDY2OWUyNjA0YTAwNzkzMzVjZGM0Y2Q2
NzFhMWIzYjQyYWYzNTcwOTUyMTgzIn0%3D
Host: apps.career.undip.ac.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Session Cookie without Secure flag set

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

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

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

Affected items

/

Details

Cookie name: "XSRF-TOKEN"
Cookie domain: "apps.career.undip.ac.id"

Request headers

```
GET / HTTP/1.1
(line truncated)
...A2citLZEhcL0M3ZlltRlJHbndoZkhNY1FGcm11OEI2RW9uN0JhSnRhd0FWb3lZd3ZzUmp1NFF3Z2xxclVHZW9
RUU9kMkZBPT0iLCJtYWMiOiJkOTk3ZTE3MjViOGZkOGU3YTlhMmY4NzNkNzE4MjRkMWZmZmQ5NDEwZjdiYmUxZTh
hMjBlODJkYzg5OWJkNzcxIn0%3D;
laravel_session=eyJpdiI6IjZkTXZOQ2RLM21sM1g0aXViVFZsNlE9PSIsInZhbHVlIjoibUM2azgwTHRTSHly
eVRpXC9HUmY0MEJieUM5a05nWXdkYmlWRFZpTStqT3ptME16ZURWVlwvNENhZGtob1VSYXEwRk9DVWF0NTVQVUR1
TFwvTUZEQ1pcL1NBPT0iLCJtYWMiOiI3NmQ2NzcxMGNkZDMyNjZjNTg2MDY2OWUyNjA0YTAwNzkzMzVjZGM0Y2Q2
NzFhMWIzYjQyYWYzNTcwOTUyMTgzIn0%3D
Host: apps.career.undip.ac.id
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: */*
```

/

Details

Cookie name: "laravel_session"
Cookie domain: "apps.career.undip.ac.id"

Request headers

```
GET / HTTP/1.1
(line truncated)
...A2citLZEhcL0M3ZlltRlJHbndoZkhNY1FGcm11OEI2RW9uN0JhSnRhd0FWb3lZd3ZzUmp1NFF3Z2xxclVHZW9
RUU9kMkZBPT0iLCJtYWMiOiJkOTk3ZTE3MjViOGZkOGU3YTlhMmY4NzNkNzE4MjRkMWZmZmQ5NDEwZjdiYmUxZTh
hMjBlODJkYzg5OWJkNzcxIn0%3D;
laravel_session=eyJpdiI6IjZkTXZOQ2RLM21sM1g0aXViVFZsNlE9PSIsInZhbHVlIjoibUM2azgwTHRTSHly
eVRpXC9HUmY0MEJieUM5a05nWXdkYmlWRFZpTStqT3ptME16ZURWVlwvNENhZGtob1VSYXEwRk9DVWF0NTVQVUR1
TFwvTUZEQ1pcL1NBPT0iLCJtYWMiOiI3NmQ2NzcxMGNkZDMyNjZjNTg2MDY2OWUyNjA0YTAwNzkzMzVjZGM0Y2Q2
NzFhMWIzYjQyYWYzNTcwOTUyMTgzIn0%3D
Host: apps.career.undip.ac.id
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: */*
```

Content type is not specified

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

Description

This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

Impact

None

Recommendation

Set a Content-Type header value for this page.

Affected items

/plugins/bootstrap/fonts/glyphicons-halflings-regular.woff2

Details

```
HTTP/1.1 200 OK
Date: Fri, 15 Sep 2017 07:04:24 GMT
Server: Apache
Last-Modified: Mon, 25 Jul 2016 05:43:02 GMT
ETag: "466c-5386f41eb0580"
Accept-Ranges: bytes
Content-Length: 18028
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

Request headers

```
GET /plugins/bootstrap/fonts/glyphicons-halflings-regular.woff2 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/plugins/bootstrap/css/bootstrap.min.css
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...dcLzY0ZWlDWk94YlwvUktxNUZZU01vcnpxZ0xOMldhVHZWc3RNeGh6OUpuOWhYMFgyc25yYUtNUjlaTmxYSjR
ybkdXQ2N2a2c9PSIsIm1hYyI6IjQ5MDlhMzg1M2FjNGViZTc1MDhlNmIyYmI1ZGFhYjJiNTg3NTgzMDU0ZDY2Zjg
wMmY4MjY0ZmU3MzRiNDYzNzEifQ%3D%3D;
laravel_session=eyJpdiI6ImtHM2VjYXNzUENZdldUbitVZ3gzdVE9PSIsInZhbHVlIjoiXC9rUmo0KzZhdE9w
SVJXcDNaOXU0bmZ5YWJVRlpEVStKTTd1Yk1ZY0FyQmRcL0NlWTZaZ3VTdFlWYVVRd2V3eXpDUGFZUHFMVUdvK2F2
dnFKV013NDJEZz09IiwibWFjIjoiNWJiMWJlZTViM2I3YzhhZjgxZDI1Y2E4OGMyYTI3ZDEwZDgwMTYzYTA0ZTUx
NjEwY2I0NzgwYThlNWY2YzQ1MCJ9
Host: apps.career.undip.ac.id
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: */*
```

/plugins/font-awesome/fonts/fontawesome-webfont.woff2

Details

```
HTTP/1.1 200 OK
Date: Fri, 15 Sep 2017 07:04:23 GMT
Server: Apache
Last-Modified: Tue, 23 May 2017 08:43:52 GMT
ETag: "12d68-5502cfcb42200"
Accept-Ranges: bytes
Content-Length: 77160
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

Request headers

```
GET /plugins/font-awesome/fonts/fontawesome-webfont.woff2 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/plugins/font-awesome/css/font-awesome.css
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...dcLzY0ZWlDWk94YlwvUktxNUZZU01vcnpxZ0xOMldhVHZWc3RNeGh6OUpuOWhYMFgyc25yYUtNUjlaTmxYSjR
ybkdXQ2N2a2c9PSIsIm1hYyI6IjQ5MDlhMzg1M2FjNGViZTc1MDhlNmIyYmI1ZGFhYjJiNTg3NTgzMDU0ZDY2Zjg
wMmY4MjY0ZmU3MzRiNDYzNzEifQ%3D%3D;
laravel_session=eyJpdiI6ImtHM2VjYXNzUENZdldUbitVZ3gzdVE9PSIsInZhbHVlIjoiXC9rUmo0KzZhdE9w
SVJXcDNaOXU0bmZ5YWJVRlpEVStKTTd1Yk1ZY0FyQmRcL0NlWTZaZ3VTdFlWYVVRd2V3eXpDUGFZUHFMVUdvK2F2
dnFKV013NDJEZz09IiwibWFjIjoiNWJiMWJlZTViM2I3YzhhZjgxZDI1Y2E4OGMyYTI3ZDEwZDgwMTYzYTA0ZTUx
NjEwY2I0NzgwYThlNWY2YzQ1MCJ9
Host: apps.career.undip.ac.id
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: */*
```

/plugins/font-awesome/fonts/fontawesome-webfont.woff2 (5862d25f39771f43cac31b2a71d2973f)

Details

```
HTTP/1.1 200 OK
Date: Fri, 15 Sep 2017 07:04:23 GMT
Server: Apache
Last-Modified: Tue, 23 May 2017 08:43:52 GMT
ETag: "12d68-5502cfcb42200"
Accept-Ranges: bytes
Content-Length: 77160
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

Request headers

```
GET /plugins/font-awesome/fonts/fontawesome-webfont.woff2?v=4.7.0 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/plugins/font-awesome/css/font-awesome.css
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...dcLzY0ZWlDWk94YlwvUktxNUZZU01vcnpxZ0xOMldhVHZWc3RNeGh6OUpuOWhYMFgyc25yYUtNUjlaTmxYSjR
ybkdXQ2N2a2c9PSIsIm1hYyI6IjQ5MDlhMzg1M2FjNGViZTc1MDhlNmIyYmI1ZGFhYjJiNTg3NTgzMDU0ZDY2Zjg
wMmY4MjY0ZmU3MzRiNDYzNzEifQ%3D%3D;
laravel_session=eyJpdiI6ImtHM2VjYXNzUENZdldUbitVZ3gzdVE9PSIsInZhbHVlIjoiXC9rUmo0KzZhdE9w
SVJXcDNaOXU0bmZ5YWJVRlpEVStKTTd1Yk1ZY0FyQmRcL0NlWTZaZ3VTdFlWYVVRd2V3eXpDUGFZUHFMVUdvK2F2
dnFKV013NDJEZz09IiwibWFjIjoiNWJiMWJlZTViM2I3YzhhZjgxZDI1Y2E4OGMyYTI3ZDEwZDgwMTYzYTA0ZTUx
NjEwY2I0NzgwYThlNWY2YzQ1MCJ9
Host: apps.career.undip.ac.id
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: */*
```

/plugins/pretty-photo/README

Details

HTTP/1.1 200 OK
Date: Fri, 15 Sep 2017 07:28:55 GMT
Server: Apache
Last-Modified: Fri, 18 Jan 2013 14:52:42 GMT
ETag: "374-4d39143706280"
Accept-Ranges: bytes
Content-Length: 884
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

Request headers

```
GET /plugins/pretty-photo/README HTTP/1.1
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*
```

/uploads/.gitignore

Details

HTTP/1.1 200 OK
Date: Fri, 15 Sep 2017 07:53:12 GMT
Server: Apache
Last-Modified: Tue, 04 Jul 2017 01:08:30 GMT
ETag: "17-5537385853f80"
Accept-Ranges: bytes
Content-Length: 23
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

Request headers

```
GET /uploads/.gitignore HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/uploads/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*
```

/web.config

Details

HTTP/1.1 200 OK
Date: Fri, 15 Sep 2017 07:53:12 GMT
Server: Apache
Last-Modified: Tue, 04 Jul 2017 01:08:29 GMT
ETag: "392-553738575fd40"
Accept-Ranges: bytes
Content-Length: 914
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

Request headers

```
GET /web.config HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*
```

Email address found

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_Dir.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

Email Address Disclosed on Website Can be Used for Spam

Affected items

/plugins/jquery-placeholder/tests

Details

Pattern found: address@example.ext

Request headers

```
GET /plugins/jquery-placeholder/tests/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...R2SGd5RElpNW03RXBmSzR2NjlSekNScGQrNEhPSzhRZFhoUWVWTnR6NGdPa1U3OTFJQlZzYUlNNHRqYUV0OHp
2Q2F1UW5ldz09IiwibWFjIjoiMGU5MmM2ZTJmYWM3ZDVhODgyYTAwNjk0ZjE3ZjBjNDEzNTYxMzhkYzY0NTJhNTN
jMTA5MTg1MGRlYjM0NDk3ZSJ9;
laravel_session=eyJpdiI6IndWMFVPcnQ0VGxxamJJeUMyS0RcL3hRPT0iLCJ2YWx1ZSI6InV1M1dVOW9tY1wv
SzdHT3pLY3FXOEJVYXBKeHlFamxDSVYwXC9hVENtQURVTUl1aTRaWkdVdVpCMEoxQXA5RHRNWmdRT2JNbXZPcGpK
OTRNcHBObmFyUFE9PSIsIm1hYyI6ImJkYTE1ODUwMTE5YjU0NDYzZDRiMTE2YTUwNWI5MzNlMTYwZWI2MWY3MzIy
ZjM4YzBhNGYxMWQ3OWFmYmY0YTMifQ%3D%3D
Host: apps.career.undip.ac.id
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

/plugins/jquery-placeholder/tests

Details

Password type input named password from unnamed form with action tests has autocomplete enabled.

Request headers

```
GET /plugins/jquery-placeholder/tests/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...R2SGd5RElpNW03RXBmSzR2NjlSekNScGQrNEhPSzhRZFhoUWVWTnR6NGdPa1U3OTFJQlZzYUlNNHRqYUV0OHp
2Q2F1UW5ldz09IiwibWFjIjoiMGU5MmM2ZTJmYWM3ZDVhODgyYTAwNjk0ZjE3ZjBjNDEzNTYxMzhkYzY0NTJhNTN
jMTA5MTg1MGRlYjM0NDk3ZSJ9;
laravel_session=eyJpdiI6IndWMFVPcnQ0VGxxamJJeUMyS0RcL3hRPT0iLCJ2YWx1ZSI6InV1M1dVOW9tY1wv
SzdHT3pLY3FXOEJVYXBKeHlFamxDSVYwXC9hVENtQURVTUl1aTRaWkdVdVpCMEoxQXA5RHRNWmdRT2JNbXZPcGpK
OTRNcHBObmFyUFE9PSIsIm1hYyI6ImJkYTE1ODUwMTE5YjU0NDYzZDRiMTE2YTUwNWI5MzNlMTYwZWI2MWY3MzIy
ZjM4YzBhNGYxMWQ3OWFmYmY0YTMifQ%3D%3D
Host: apps.career.undip.ac.id
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: */*
```

Possible internal IP address disclosure

Severity	**Informational**
Type	Informational
Reported by module	Scripting (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

/index.php/news/

Details

Tested on URI: /index.php/news/hYBhR0JvQ2.jsp

Pattern found in response: 127.187.201.352

Request headers

```
GET /index.php/news/hYBhR0JvQ2.jsp HTTP/1.1
(line truncated)
...YTFhWGtlWDZuTjNXT2p3Zk5USXhwQmNielwvdytscTNSYTFhdlk4U09WakJTU040XC9lcFZkZThDb2tXN2NsW
VhlTEcyRWVXUndCUT09IiwibWFjIjoiMzU2NDg3ZjEwNjkzOTcwZjQ2MmI2ZGVjMmRkMjA5ZmYxZTYwZjU3YTFhZ
jVjZTBkMzEwZjY4YWYzNTNkZWRhZCJ9;
laravel_session=eyJpdiI6Img4NFl1bHFcL0pyb1NtNEtaSE84czRRPT0iLCJ2YWx1ZSI6ImpyUElON2FZSVJ1
elhSKzV4TU83UDV1NkVXTVlwMm9pTlMyMERRdm9VZVhrUXpSMVVYNGFmZURJRnhrdndlTDUwT2V3RCthT2l3SlB0
NTVueUw4Z3lnPT0iLCJtYWMiOiIyZDc0NjhlZjAxZWMzYjVkOThkZjgzZDgyNjc1YzJjNDZhODlhNTdjZjZiZDI3
NDA5NTY3NzZhYjQ2YzUwMTg2In0%3D
Host: apps.career.undip.ac.id
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: */*
```

/index.php/news/%20kategori-a

Details

Pattern found: 127.187.201.352

Request headers

```
GET /index.php/news/%20kategori-a HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...RKdmJ3RnlyYnAxYTR5c2lyTXdSaENrTmhwbDJvcWpPSnZnWXZEZStGZzBJZk40UzJINDc1WjlQb29ENGVNVEF
FRmJxRXc9PSIsIm1hYyI6IjQ0NzI2MzdmNWIwMmNiZjhlMzBmMmY3YjlkN2ZmZmQ0NDk2YmYxYzQ4MDc5N2Y2ZmU
yODhlNWU5MGJmOTRjMjYifQ%3D%3D;
laravel_session=eyJpdiI6ImNzNHRQd2JZRFZNS3Y0TlpBdlpGaFE9PSIsInZhbHVlIjoiK29NWU5QMjJJK3Bq
d3JQODB2WkJPR2dSZkNuMnRqZ0xmWDE4VGh5aWQxaU5ScEVUTGJra2xYSEdWQ2Q0WG9aUmxURU9VM09xaW1HeXNL
dmQwZTNia2c9PSIsIm1hYyI6Ijk3NmUwMzdiNTY4MTMwODM5NTI4ZDViOTE4MzQwMTQ1ODJiNDY3NjYzZDdlNjU
```

```
0YWQ1NDExYmNmOGQyMWJmNjUifQ%3D%3D
Host: apps.career.undip.ac.id
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: */*
```

/index.php/news/%20kategori-a/

Details

Tested on URI: /index.php/news/%20kategori-a/27F8yUYciI.jsp

Pattern found in response: 127.187.201.352

Request headers

```
GET /index.php/news/%20kategori-a/27F8yUYciI.jsp HTTP/1.1
(line truncated)
...YTFhWGtlWDZuTjNXT2p3Zk5USXhwQmNielwvdytscTNSYTFhdlk4U09WakJTU040XC9lcFZkZThDb2tXN2NsW
VhlTEcyRWVXUndCUT09IiwibWFjIjoiMzU2NDg3ZjEwNjkzOTcwZjQ2MmI2ZGVjMmRkMjA5ZmYxZTYwZjU3YTFhZ
jVjZTBkMzEwZjY4YWYzNTNkZWRhZCJ9;
laravel_session=eyJpdiI6Img4NFl1bHFcL0pyb1NtNEtaSE84czRRPT0iLCJ2YWx1ZSI6ImpyUElON2FZSVJ1
elhSKzV4TU83UDV1NkVXTVlwMm9pTlMyMERRdm9VZVhrUXpSMVVYNGFmZURJRnhrdndlTDUwT2V3RCthT2l3SlB0
NTVueUw4Z3lnPT0iLCJtYWMiOiIyZDc0NjhlZjAxZWMzYjVkOThkZjgzZDgyNjc1YzJjNDZhODlhNTdjZjZiZDI3
NDA5NTY3NzZhYjQ2YzUwMTg2In0%3D
Host: apps.career.undip.ac.id
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: */*
```

/index.php/news/kategori-a/

Details

Tested on URI: /index.php/news/kategori-a/UbEyqPzeif.jsp

Pattern found in response: 127.187.201.352

Request headers

```
GET /index.php/news/kategori-a/UbEyqPzeif.jsp HTTP/1.1
(line truncated)
...YTFhWGtlWDZuTjNXT2p3Zk5USXhwQmNielwvdytscTNSYTFhdlk4U09WakJTU040XC9lcFZkZThDb2tXN2NsW
VhlTEcyRWVXUndCUT09IiwibWFjIjoiMzU2NDg3ZjEwNjkzOTcwZjQ2MmI2ZGVjMmRkMjA5ZmYxZTYwZjU3YTFhZ
jVjZTBkMzEwZjY4YWYzNTNkZWRhZCJ9;
laravel_session=eyJpdiI6Img4NFl1bHFcL0pyb1NtNEtaSE84czRRPT0iLCJ2YWx1ZSI6ImpyUElON2FZSVJ1
elhSKzV4TU83UDV1NkVXTVlwMm9pTlMyMERRdm9VZVhrUXpSMVVYNGFmZURJRnhrdndlTDUwT2V3RCthT2l3SlB0
NTVueUw4Z3lnPT0iLCJtYWMiOiIyZDc0NjhlZjAxZWMzYjVkOThkZjgzZDgyNjc1YzJjNDZhODlhNTdjZjZiZDI3
NDA5NTY3NzZhYjQ2YzUwMTg2In0%3D
Host: apps.career.undip.ac.id
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: */*
```

/news/

Details

Tested on URI: /news/6MUaebRIzh.jsp

Pattern found in response: 127.187.201.352

Request headers

```
GET /news/6MUaebRIzh.jsp HTTP/1.1
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE
```

```
4elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzB
hZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*
```

/news/%20kategori-a

Details

Pattern found: 127.187.201.352

Request headers

```
GET /news/%20kategori-a HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...dcLzY0ZWlDWk94YlwvUktxNUZZU01vcnpxZ0xOMldhVHZWc3RNeGh6OUpuOWhYMFgyc25yYUtNUjlaTmxYSjR
ybkdXQ2N2a2c9PSIsIm1hYyI6IjQ5MDlhMzg1M2FjNGViZTc1MDhlNmIyYmI1ZGFhYjJiNTg3NTgzMDU0ZDY2Zjg
wMmY4MjY0ZmU3MzRiNDYzNzEifQ%3D%3D;
laravel_session=eyJpdiI6ImtHM2VjYXNzUENZdldUbitVZ3gzdVE9PSIsInZhbHVlIjoiXC9rUmo0KzZhdE9w
SVJXcDNaOXU0bmZ5YWJVRlpEVStKTTd1Yk1ZY0FyQmRcL0NlWTZaZ3VTdFlWYVVRd2V3eXpDUGFZUHFMVUdvK2F2
dnFKV013NDJEZz09IiwibWFjIjoiNWJiMWJlZTViM2I3YzhhZjgxZDI1Y2E4OGMyYTI3ZDEwZDgwMTYzYTA0ZTUx
NjEwY2I0NzgwYThlNWY2YzQ1MCJ9
Host: apps.career.undip.ac.id
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: */*
```

/news/%20kategori-a/

Details

Tested on URI: /news/%20kategori-a/YKiA1J33Iu.jsp

Pattern found in response: 127.187.201.352

Request headers

```
GET /news/%20kategori-a/YKiA1J33Iu.jsp HTTP/1.1
(line truncated)
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*
```

/news/kategori-a/

Details

Tested on URI: /news/kategori-a/FKQKE5t0dr.jsp

Pattern found in response: 127.187.201.352

Request headers

```
GET /news/kategori-a/FKQKE5t0dr.jsp HTTP/1.1
(line truncated)
```

```
...9mdmU1dmJ3N09ENnd5ZDhESnhkbGpwTFk0Nkp4aTZJUzhycjdJWWx5dkZ5UGhVNmdEUUxPalwvM25CSDBIMkF
vNElOK0sweWc9PSIsIm1hYyI6ImVjNWQyN2Y4ZTg2OGNmM2VhYmYxYzAxNTlkMGFiODgzZWQ2M2I4YmQ1Y2FmOGV
lZTZiMTE2NmNkYzg1MDk5YzEifQ%3D%3D;
laravel_session=eyJpdiI6Ikl5a2ZPNWtwdDN5UFUwVFhwXC9HOEhnPT0iLCJ2YWx1ZSI6ImpUTWhTYlBiOVMy
c3NIc1NMSlRPTmhYeUJ0V1wveXFSc1A5c0hvQUtTMkpVbDM2UExTVDE2UndtRnJTV2tOeUl1TDFKa3d4OEpXTVE4
elgzMGpkYmw5QT09IiwibWFjIjoiNTZmZGRjNGRhZWJkZWYzZWRmNDhlZGMxMDE5NzJjZjU3YzZlMDAzNDhlYzBh
ZWRjMTUzM2EyZTAyZDA4NTgxMiJ9
Host: apps.career.undip.ac.id
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: */*
```

Possible username or password disclosure

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

Description

A username and/or password was found in this file. This information could be sensitive.

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

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

/plugins/font-awesome/css/font-awesome.css

Details

Pattern found: pass:before

Request headers

```
GET /plugins/font-awesome/css/font-awesome.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://apps.career.undip.ac.id/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
(line truncated)
...R3VDSk02VW1JWDY0ZFdzOUJVWVF2TWk5OWtsdFZMdlZoZndWVDJpekFiazg1MmtEN21ldFErMEMyd05yUTdVd
jdPNGE0eWc9PSIsIm1hYyI6Ijg1N2YxNzBiMTJlNzFjYWM2NjFmOTc1YTE1OGJhZWU0YmVkYThlYjMxN2Y5MjA4M
GExYmFlMDAzZWNkNmRkNzkifQ%3D%3D;
laravel_session=eyJpdiI6IlFaR01GcHN6YXd3d1dWZ0lGSkRLVnc9PSIsInZhbHVlIjoiS0lZblZWcWwyOE1S
TTlrWkVvSU05NUxZYW40RDB6dE5kRWVrVEZBdnByUlRLY0RTT29JaWhubk5PenRXUWVzdFBMbTBLRFRBM3hGU1V0
THlndUNcL3l3PT0iLCJtYWMiOiJjOGNjMTIxM2Q4NmE1ZjJjZWI5NmIyZDZlOWNmN2YyYTU2ZWE0MTAxNGU1YjVl
Njc4ZjIxNjZkZWI1ZTIzMTljIn0%3D
Host: apps.career.undip.ac.id
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 105 URLs. Found 21 vulnerable.

URL: http://apps.career.undip.ac.id/

Vulnerabilities has been identified for this URL

7 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
/	Path Fragment

Input scheme 2	
Input name	Input type
/	Path Fragment
/	Path Fragment

Input scheme 3	
Input name	Input type
/	Path Fragment
/	Path Fragment
/	Path Fragment

Input scheme 4	
Input name	Input type
/plugins/pretty-photo/	Path Fragment (suffix .html)

URL: http://apps.career.undip.ac.id/search

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
q	URL encoded GET

URL: http://apps.career.undip.ac.id/uploads/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/uploads/2017-08/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/uploads/2017-07/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/uploads/2017-09/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/uploads/.gitignore

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/news

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/news/kategori-a
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/news/kategori-a/my-own-post
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/news/%20kategori-a
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/news/%20kategori-a/my-own-post
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/about
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/events
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/events/all
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/events/uploads
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/events/uploads/2017-07
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/events/Respond.js
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/gallery
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/contact
Vulnerabilities has been identified for this URL
5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_token	URL encoded POST
email	URL encoded POST
message	URL encoded POST
name	URL encoded POST
phone	URL encoded POST

URL: http://apps.career.undip.ac.id/responses
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://apps.career.undip.ac.id/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/css/styles.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/css/custom-style.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/images/misc/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/flexslider/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/flexslider/flexslider.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/flexslider/jquery.flexslider-min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/flexslider/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/font-awesome/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/font-awesome/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/font-awesome/css/icomoon.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/font-awesome/css/font-awesome.css

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/icomoon.ttf

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/icomoon.svg

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/icomoon.eot

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/icomoon.woff

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/fontawesome-webfont.svg

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
v	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/fontawesome-webfont.ttf

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
v	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/fontawesome-webfont.eot

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type

v	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/fontawesome-webfont.woff

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
v	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/font-awesome/fonts/fontawesome-webfont.woff2

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
v	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/bootstrap/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/bootstrap/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/bootstrap/css/bootstrap.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/bootstrap/js/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/bootstrap/js/bootstrap.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/bootstrap/fonts/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/bootstrap/fonts/glyphicons-halflings-regular.woff2

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/css/prettyPhoto.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/js/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/js/jquery.prettyPhoto.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/prettyPhoto/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/prettyPhoto/default/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/prettyPhoto/facebook/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/prettyPhoto/dark_square/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/prettyPhoto/light_square/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/prettyPhoto/dark_rounded/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/prettyPhoto/light_rounded/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/fullscreen/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/images/thumbnails/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/pretty-photo/xhr_response.html

No vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
ajax	URL encoded GET
height	URL encoded GET
width	URL encoded GET

URL: http://apps.career.undip.ac.id:80/plugins/pretty-photo/README

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/jquery-1.12.3.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/bootstrap-hover-dropdown.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/back-to-top.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/jquery-placeholder/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/jquery-placeholder/jquery.placeholder.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/

Vulnerabilities has been identified for this URL

10 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
email	URL encoded GET
message	URL encoded GET
name	URL encoded GET
password	URL encoded GET
search	URL encoded GET
tel	URL encoded GET
url	URL encoded GET

Input scheme 2	
Input name	Input type
testNumber	URL encoded GET

Input scheme 3	
Input name	Input type
noglobals	URL encoded GET

Input scheme 4	
Input name	Input type
notrycatch	URL encoded GET

URL: http://apps.career.undip.ac.id/plugins/jquery-placeholder/tests/tests.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/jflickrfeed/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/plugins/jflickrfeed/jflickrfeed.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/js/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/js/main.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/robots.txt

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/missing

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/web.config

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/search

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
q	URL encoded GET

URL: http://apps.career.undip.ac.id/index.php/news

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/news/kategori-a

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/news/kategori-a/my-own-post

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/news/%20kategori-a

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/news/%20kategori-a/my-own-post

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/about

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/events

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/events/all

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/events/uploads

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/events/uploads/2017-07

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/events/Respond.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/contact

Vulnerabilities has been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_token	URL encoded POST
email	URL encoded POST
message	URL encoded POST
name	URL encoded POST
phone	URL encoded POST

URL: http://apps.career.undip.ac.id/index.php/gallery

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/responses

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/uploads

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/uploads/2017-08

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/uploads/2017-09

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/uploads/2017-07

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/missing

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://apps.career.undip.ac.id/index.php/Respond.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL