

Commix Scan Report

Target URL: <http://testphp.vulnweb.com/login.php>

Scope: 1

```

      _
    _ _ _ _ _ ^ \ _ _
  / _ \ / _ \ ' _ ' _ \ ' _ ' _ \ \ \ \ \ v4.1-dev#11
^ \ _ / ^ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ > < /
 \ \ _ \ \ \ _ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ https://commixproject.com
  \ _ _ \ / \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ (@commixproject)

```

 $+-$

Automated All-in-One OS Command Injection Exploitation Tool

Copyright © 2014-2025 Anastasios Stasinopoulos (@ancst)

 $+-$

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

Do you want to check target for the existence of site's sitemap(.xml)? [y/N] > N

```
[23:57:16] [info] Starting crawler for target URL 'http://testphp.vulnweb.com/login.php'.
```

[23:57:18] [info] Searching for usable links with depth 1.

[23:57:19] [info] 1/11 links visited.

[23:57:20] [info] 2/11 links visited.

[23:57:21] [info] 3/11 links visited.

[23:57:22] [info] 4/11 links visited.

[23:57:24] [info] 5/11 links visited.

Got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] > Y

```
[23:57:27] [info] Following redirection to 'http://testphp.vulnweb.com/login.php'.
```

[23:57:27] [info] 6/11 links visited.

[23:57:28] [info] 7/11 links visited.

[23:57:29] [info] 8/11 links visited.

It is not recommended to continue in this kind of cases. Do you want to ignore the response

HTTP error code '404' and continue the tests? [Y/n] > Y

[23:57:31] [info] 9/11 links visited.

[23:57:32] [info] 10/11 links visited.

[23:57:33] [info] 11/11 links visited.

Do you want to normalize crawling results? [Y/n] > Y

Do you want to store crawling results to a temporary file (for eventual further processing with other tools)? [y/N] > N

```
[23:57:33] [info] Found a total of 4 targets.
```

```
[1/4] URL - GET http://testphp.vulnweb.com/listproducts.php?cat=1
```

Do you want to use URL #1 to perform tests? [Y/n] > Y

```
[23:57:33] [info] Testing URL 'http://testphp.vulnweb.com/listproducts.php?cat=1'.
```

```
[23:57:33] [info] Testing connection to the target URL.
```

[23:57:34] [info] Checking if the target is protected by some kind of WAF/IPS.

[23:57:36] [info] Performing identification (passive) tests to the target URL.

```
[23:57:36] [info] Setting GET parameter 'cat' for tests.
```

[23:57:36] [info] Performing heuristic (basic) tests to the GET parameter 'cat'.

[23:58:02] [warning] Heuristic (basic) tests shows that GET parameter 'cat' might not be injectable.

[23:58:03] [info] Testing the (results-based) classic command injection technique... (11.1%)

[23:58:05] [info] Testing the (results-based) classic command injection technique... (22.2%)

[23:58:06] [info] Testing the (results-based) classic command injection technique... (33.3%)

[23:58:07] [info] Testing the (results-based) classic command injection technique... (44.4%)

[23:58:08] [info] Testing the (results-based) classic command injection technique... (55.6%)

[23:58:09] [info] Testing the (results-based) classic command injection technique... (66.7%)

[23:58:11] [info] Testing the (results-based) classic command injection technique... (77.8%)

[23:58:12] [info] Testing the (results-based) classic command injection technique... (88.9%)

[23:58:13] [info] Testing the (results-based) classic command injection technique.

[23:58:14] [info] Testing the (results-based) dynamic code evaluation technique... (8.3%)

[23:58:15] [info] Testing the (results-based) dynamic code evaluation technique... (16.7%)

[23:58:17] [info] Testing the (results-based) dynamic code evaluation technique... (25.0%)

[23:58:18] [info] Testing the (results-based) dynamic code evaluation technique... (33.3%)

[23:58:19] [info] Testing the (results-based) dynamic code evaluation technique... (41.7%)

[23:58:20] [info] Testing the (results-based) dynamic code evaluation technique... (50.0%)

[23:58:21] [info] Testing the (results-based) dynamic code evaluation technique... (58.3%)

[23:58:23] [info] Testing the (results-based) dynamic code evaluation technique... (66.7%)

[23:58:24] [info] Testing the (results-based) dynamic code evaluation technique... (75.0%)

[23:58:25] [info] Testing the (results-based) dynamic code evaluation technique... (83.3%)

[23:58:26] [info] Testing the (results-based) dynamic code evaluation technique... (91.7%)

[23:58:27] [info] Testing the (results-based) dynamic code evaluation technique.

[23:58:27] [warning] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions.

[23:58:29] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:29] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:30] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:30] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:31] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:31] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:32] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:32] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:33] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:33] [info] Testing the (blind) time-based command injection technique... (22.2%)

Unexpected time delays that may lead to false-positive results, have been identified. How do you want to proceed? [(C)ontinue/(s)kip] > C

[23:58:34] [info] Testing the (blind) time-based command injection technique... (22.2%)

[23:58:36] [info] Checking if the injection point on GET parameter 'cat' is a false positive.

[23:58:36] [warning] Time-based comparison requires reset of statistical model, please wait...

...

[23:58:39] [warning] False positive or unexploitable injection point has been detected.

[23:58:40] [info] Testing the (blind) time-based command injection technique... (66.7%)

[23:58:41] [info] Testing the (blind) time-based command injection technique... (66.7%)

[23:58:42] [info] Testing the (blind) time-based command injection technique... (66.7%)

[23:58:44] [info] Testing the (blind) time-based command injection technique... (66.7%)

[23:58:45] [info] Testing the (blind) time-based command injection technique... (66.7%)

[23:58:46] [info] Testing the (blind) time-based command injection technique... (66.7%)

[23:58:47] [info] Testing the (blind) time-based command injection technique... (66.7%)

[23:58:48] [info] Testing the (blind) time-based command injection technique... (66.7%)

[23:58:50] [info] Testing the (blind) time-based command injection technique... (66.7%)
[23:58:51] [info] Testing the (blind) time-based command injection technique... (77.8%)
[23:58:52] [info] Testing the (blind) time-based command injection technique... (77.8%)
[23:58:53] [info] Testing the (blind) time-based command injection technique... (77.8%)
[23:58:54] [info] Testing the (blind) time-based command injection technique... (77.8%)
[23:58:55] [info] Testing the (blind) time-based command injection technique... (77.8%)
[23:58:57] [info] Testing the (blind) time-based command injection technique... (77.8%)
[23:58:58] [info] Testing the (blind) time-based command injection technique... (77.8%)
[23:58:59] [info] Testing the (blind) time-based command injection technique... (77.8%)
[23:59:00] [info] Testing the (blind) time-based command injection technique... (77.8%)
[23:59:01] [info] Testing the (blind) time-based command injection technique... (88.9%)
[23:59:02] [info] Testing the (blind) time-based command injection technique... (88.9%)
[23:59:04] [info] Testing the (blind) time-based command injection technique... (88.9%)
[23:59:05] [info] Testing the (blind) time-based command injection technique... (88.9%)
[23:59:06] [info] Testing the (blind) time-based command injection technique... (88.9%)
[23:59:07] [info] Testing the (blind) time-based command injection technique... (88.9%)
[23:59:08] [info] Testing the (blind) time-based command injection technique... (88.9%)
[23:59:10] [info] Testing the (blind) time-based command injection technique... (88.9%)
[23:59:11] [info] Testing the (blind) time-based command injection technique... (88.9%)
[23:59:11] [info] Testing the (blind) time-based command injection technique.
Enter what you want to use for writable directory (e.g. '/var/www/testphp.vulnweb.com/public_html/') > /var/www/testphp.vulnweb.com/public_html/
[23:59:11] [info] Trying to create a file in directory '/var/www/testphp.vulnweb.com/public_html/' for command execution output.
Do you want to use URL 'http://testphp.vulnweb.com/FXSSMA.txt' for command execution output? [Y/n] > Y
[23:59:13] [info] Testing the (semi-blind) file-based command injection technique... (11.1%)
[23:59:16] [info] Testing the (semi-blind) file-based command injection technique... (22.2%)
[23:59:19] [info] Testing the (semi-blind) file-based command injection technique... (33.3%)
[23:59:22] [info] Testing the (semi-blind) file-based command injection technique... (44.4%)
[23:59:25] [info] Testing the (semi-blind) file-based command injection technique... (55.6%)
[23:59:27] [info] Testing the (semi-blind) file-based command injection technique... (66.7%)
[23:59:30] [info] Testing the (semi-blind) file-based command injection technique... (77.8%)
It seems that you don't have permissions to read and/or write files in directory '/var/www/testphp.vulnweb.com/public_html/'.
Do you want to use the temporary directory ('/tmp/')? [Y/n] > Y
[23:59:33] [info] Trying to create a file in directory '/tmp/' for command execution output.
[23:59:33] [warning] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions.
[23:59:34] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[23:59:34] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[23:59:35] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[23:59:35] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[23:59:37] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[23:59:37] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[23:59:38] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[23:59:38] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[23:59:39] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[23:59:39] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
Unexpected time delays that may lead to false-positive results, have been identified. How do

you want to proceed? [(C)ontinue/(s)kip] > C

[23:59:40] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)

[23:59:42] [info] Checking if the injection point on GET parameter 'cat' is a false positive.

[23:59:42] [warning] Time-based comparison requires reset of statistical model, please wait...

...

[23:59:45] [warning] False positive or unexploitable injection point has been detected.

[23:59:46] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[23:59:47] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[23:59:48] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[23:59:49] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[23:59:50] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[23:59:52] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[23:59:53] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[23:59:54] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[23:59:55] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[23:59:56] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)

[23:59:58] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)

[23:59:59] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)

[00:00:00] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)

[00:00:01] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)

[00:00:02] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)

[00:00:04] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)

[00:00:05] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)

[00:00:06] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)

[00:00:07] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)

[00:00:08] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)

[00:00:10] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)

[00:00:11] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)

[00:00:12] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)

[00:00:13] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)

[00:00:14] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)

[00:00:16] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)

[00:00:17] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)

[00:00:17] [info] Testing the (semi-blind) tempfile-based injection technique.

[00:00:20] [info] Testing the (semi-blind) file-based command injection technique.

[00:00:20] [warning] The tested GET parameter 'cat' does not seem to be injectable.

[00:00:20] [critical] All tested parameters do not appear to be injectable. Try to increase value for '--level' option if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved, maybe you could try to use option '--tamper' and/or switch '--random-agent'.

[2/4] URL - GET <http://testphp.vulnweb.com/artists.php?artist=1>

Do you want to use URL #2 to perform tests? [Y/n] > Y

[00:00:20] [info] Testing URL '<http://testphp.vulnweb.com/artists.php?artist=1>'.

[00:00:20] [info] Testing connection to the target URL.

[00:00:21] [info] Checking if the target is protected by some kind of WAF/IPS.

[00:00:22] [info] Performing identification (passive) tests to the target URL.

[00:00:22] [info] Setting GET parameter 'artist' for tests.

[00:00:22] [info] Performing heuristic (basic) tests to the GET parameter 'artist'.

[00:00:49] [warning] Heuristic (basic) tests shows that GET parameter 'artist' might not be injectable.

[00:00:50] [info] Testing the (results-based) classic command injection technique... (11.1%)
[00:00:51] [info] Testing the (results-based) classic command injection technique... (22.2%)
[00:00:52] [info] Testing the (results-based) classic command injection technique... (33.3%)
[00:00:54] [info] Testing the (results-based) classic command injection technique... (44.4%)
[00:00:55] [info] Testing the (results-based) classic command injection technique... (55.6%)
[00:00:56] [info] Testing the (results-based) classic command injection technique... (66.7%)
[00:00:57] [info] Testing the (results-based) classic command injection technique... (77.8%)
[00:00:58] [info] Testing the (results-based) classic command injection technique... (88.9%)
[00:01:00] [info] Testing the (results-based) classic command injection technique.
[00:01:01] [info] Testing the (results-based) dynamic code evaluation technique... (8.3%)
[00:01:02] [info] Testing the (results-based) dynamic code evaluation technique... (16.7%)
[00:01:03] [info] Testing the (results-based) dynamic code evaluation technique... (25.0%)
[00:01:04] [info] Testing the (results-based) dynamic code evaluation technique... (33.3%)
[00:01:06] [info] Testing the (results-based) dynamic code evaluation technique... (41.7%)
[00:01:07] [info] Testing the (results-based) dynamic code evaluation technique... (50.0%)
[00:01:08] [info] Testing the (results-based) dynamic code evaluation technique... (58.3%)
[00:01:09] [info] Testing the (results-based) dynamic code evaluation technique... (66.7%)
[00:01:10] [info] Testing the (results-based) dynamic code evaluation technique... (75.0%)
[00:01:12] [info] Testing the (results-based) dynamic code evaluation technique... (83.3%)
[00:01:13] [info] Testing the (results-based) dynamic code evaluation technique... (91.7%)
[00:01:14] [info] Testing the (results-based) dynamic code evaluation technique.
[00:01:14] [warning] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions.
[00:01:15] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:15] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:16] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:16] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:18] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:18] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:19] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:19] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:20] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:20] [info] Testing the (blind) time-based command injection technique... (22.2%)
Unexpected time delays that may lead to false-positive results, have been identified. How do you want to proceed? [(C)ontinue/(s)kip] > C
[00:01:21] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:01:23] [info] Checking if the injection point on GET parameter 'artist' is a false positive.
[00:01:23] [warning] Time-based comparison requires reset of statistical model, please wait...
...
[00:01:26] [warning] False positive or unexploitable injection point has been detected.
[00:01:27] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:01:28] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:01:29] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:01:30] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:01:32] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:01:33] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:01:34] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:01:35] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:01:36] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:01:38] [info] Testing the (blind) time-based command injection technique... (77.8%)

[00:01:39] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:01:40] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:01:41] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:01:43] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:01:44] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:01:45] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:01:46] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:01:47] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:01:48] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:01:50] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:01:51] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:01:52] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:01:53] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:01:54] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:01:56] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:01:57] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:01:58] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:01:58] [info] Testing the (blind) time-based command injection technique.
[00:02:01] [info] Testing the (semi-blind) file-based command injection technique... (11.1%)
[00:02:04] [info] Testing the (semi-blind) file-based command injection technique... (22.2%)
[00:02:06] [info] Testing the (semi-blind) file-based command injection technique... (33.3%)
[00:02:09] [info] Testing the (semi-blind) file-based command injection technique... (44.4%)
[00:02:12] [info] Testing the (semi-blind) file-based command injection technique... (55.6%)
[00:02:15] [info] Testing the (semi-blind) file-based command injection technique... (66.7%)
[00:02:17] [info] Testing the (semi-blind) file-based command injection technique... (77.8%)
It seems that you don't have permissions to read and/or write files in directory '/var/www/test
php.vulnweb.com/public_html/'.
Do you want to use the temporary directory ('/tmp/')? [Y/n] > Y
[00:02:20] [info] Trying to create a file in directory '/tmp/' for command execution output.
[00:02:20] [warning] It is very important to not stress the network connection during usage of
time-based payloads to prevent potential disruptions.
[00:02:21] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:21] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:23] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:23] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:24] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:24] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:25] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:25] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:26] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:26] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
Unexpected time delays that may lead to false-positive results, have been identified. How do
you want to proceed? [(C)ontinue/(s)kip] > C
[00:02:27] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:02:29] [info] Checking if the injection point on GET parameter 'artist' is a false positive.
[00:02:29] [warning] Time-based comparison requires reset of statistical model, please wait...
...
[00:02:32] [warning] False positive or unexploitable injection point has been detected.
[00:02:33] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:02:34] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[00:02:35] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:02:37] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:02:38] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:02:39] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:02:40] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:02:42] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:02:43] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:02:44] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:02:45] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:02:46] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:02:48] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:02:49] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:02:50] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:02:51] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:02:52] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:02:54] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:02:55] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:02:56] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:02:57] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:02:58] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:03:00] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:03:01] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:03:02] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:03:03] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:03:04] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:03:04] [info] Testing the (semi-blind) tempfile-based injection technique.
[00:03:07] [info] Testing the (semi-blind) file-based command injection technique.
[00:03:07] [warning] The tested GET parameter 'artist' does not seem to be injectable.
[00:03:07] [critical] All tested parameters do not appear to be injectable. Try to increase value for '--level' option if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved, maybe you could try to use option '--tamper' and/or switch '--random-agent'.
[3/4] URL - GET http://testphp.vulnweb.com/comment.php?aid=1
Do you want to use URL #3 to perform tests? [Y/n] > Y
[00:03:07] [info] Testing URL 'http://testphp.vulnweb.com/comment.php?aid=1'.
[00:03:07] [info] Testing connection to the target URL.
[00:03:09] [warning] The web server responded with an HTTP error code '404' which could interfere with the results of the tests.
[00:03:09] [info] Checking if the target is protected by some kind of WAF/IPS.
[00:03:10] [info] Performing identification (passive) tests to the target URL.
[00:03:11] [critical] Unable to connect to the target URL (HTTP Error 404: Not Found).
[00:03:11] [info] Setting GET parameter 'aid' for tests.
[00:03:11] [info] Performing heuristic (basic) tests to the GET parameter 'aid'.
[00:03:46] [warning] Heuristic (basic) tests shows that GET parameter 'aid' might not be injectable.
[00:03:47] [info] Testing the (results-based) classic command injection technique... (11.1%)
[00:03:49] [info] Testing the (results-based) classic command injection technique... (22.2%)
[00:03:51] [info] Testing the (results-based) classic command injection technique... (33.3%)
[00:03:52] [info] Testing the (results-based) classic command injection technique... (44.4%)
[00:03:54] [info] Testing the (results-based) classic command injection technique... (55.6%)

[00:03:55] [info] Testing the (results-based) classic command injection technique... (66.7%)
[00:03:57] [info] Testing the (results-based) classic command injection technique... (77.8%)
[00:03:59] [info] Testing the (results-based) classic command injection technique... (88.9%)
[00:04:00] [info] Testing the (results-based) classic command injection technique.
[00:04:02] [info] Testing the (results-based) dynamic code evaluation technique... (8.3%)
[00:04:03] [info] Testing the (results-based) dynamic code evaluation technique... (16.7%)
[00:04:05] [info] Testing the (results-based) dynamic code evaluation technique... (25.0%)
[00:04:06] [info] Testing the (results-based) dynamic code evaluation technique... (33.3%)
[00:04:08] [info] Testing the (results-based) dynamic code evaluation technique... (41.7%)
[00:04:10] [info] Testing the (results-based) dynamic code evaluation technique... (50.0%)
[00:04:11] [info] Testing the (results-based) dynamic code evaluation technique... (58.3%)
[00:04:13] [info] Testing the (results-based) dynamic code evaluation technique... (66.7%)
[00:04:14] [info] Testing the (results-based) dynamic code evaluation technique... (75.0%)
[00:04:16] [info] Testing the (results-based) dynamic code evaluation technique... (83.3%)
[00:04:17] [info] Testing the (results-based) dynamic code evaluation technique... (91.7%)
[00:04:19] [info] Testing the (results-based) dynamic code evaluation technique.
[00:04:19] [warning] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions.
[00:04:21] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:21] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:22] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:22] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:24] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:24] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:25] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:25] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:27] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:27] [info] Testing the (blind) time-based command injection technique... (22.2%)
Unexpected time delays that may lead to false-positive results, have been identified. How do you want to proceed? [(C)ontinue/(s)kip] > C
[00:04:29] [info] Testing the (blind) time-based command injection technique... (22.2%)
[00:04:31] [info] Checking if the injection point on GET parameter 'aid' is a false positive.
[00:04:31] [warning] Time-based comparison requires reset of statistical model, please wait...
...
[00:04:34] [warning] False positive or unexploitable injection point has been detected.
[00:04:35] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:04:37] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:04:38] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:04:40] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:04:42] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:04:43] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:04:45] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:04:46] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:04:48] [info] Testing the (blind) time-based command injection technique... (66.7%)
[00:04:50] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:04:51] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:04:53] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:04:54] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:04:56] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:04:58] [info] Testing the (blind) time-based command injection technique... (77.8%)

[00:04:59] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:05:01] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:05:02] [info] Testing the (blind) time-based command injection technique... (77.8%)
[00:05:04] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:05:06] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:05:07] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:05:09] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:05:10] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:05:12] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:05:14] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:05:15] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:05:17] [info] Testing the (blind) time-based command injection technique... (88.9%)
[00:05:17] [info] Testing the (blind) time-based command injection technique.
[00:05:20] [info] Testing the (semi-blind) file-based command injection technique... (11.1%)
[00:05:23] [info] Testing the (semi-blind) file-based command injection technique... (22.2%)
[00:05:26] [info] Testing the (semi-blind) file-based command injection technique... (33.3%)
[00:05:29] [info] Testing the (semi-blind) file-based command injection technique... (44.4%)
[00:05:32] [info] Testing the (semi-blind) file-based command injection technique... (55.6%)
[00:05:36] [info] Testing the (semi-blind) file-based command injection technique... (66.7%)
[00:05:39] [info] Testing the (semi-blind) file-based command injection technique... (77.8%)
It seems that you don't have permissions to read and/or write files in directory '/var/www/test.php.vulnweb.com/public_html/'.
Do you want to use the temporary directory ('/tmp/')} [Y/n] > Y
[00:05:42] [info] Trying to create a file in directory '/tmp/' for command execution output.
[00:05:42] [warning] It is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions.
[00:05:43] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:43] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:45] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:45] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:47] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:47] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:48] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:48] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:50] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:50] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
Unexpected time delays that may lead to false-positive results, have been identified. How do you want to proceed? [(C)ontinue/(s)kip] > C
[00:05:51] [info] Testing the (semi-blind) tempfile-based injection technique... (22.2%)
[00:05:53] [info] Checking if the injection point on GET parameter 'aid' is a false positive.
[00:05:53] [warning] Time-based comparison requires reset of statistical model, please wait...
...
[00:05:57] [warning] False positive or unexploitable injection point has been detected.
[00:05:58] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:06:00] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:06:01] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:06:03] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:06:05] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:06:06] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:06:08] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)

[00:06:09] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:06:11] [info] Testing the (semi-blind) tempfile-based injection technique... (66.7%)
[00:06:13] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:06:14] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:06:16] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:06:17] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:06:19] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:06:21] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:06:22] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:06:24] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:06:25] [info] Testing the (semi-blind) tempfile-based injection technique... (77.8%)
[00:06:27] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:06:29] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:06:30] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:06:32] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:06:33] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:06:35] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:06:36] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:06:38] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:06:40] [info] Testing the (semi-blind) tempfile-based injection technique... (88.9%)
[00:06:40] [info] Testing the (semi-blind) tempfile-based injection technique.
[00:06:43] [info] Testing the (semi-blind) file-based command injection technique.
[00:06:43] [warning] The tested GET parameter 'aid' does not seem to be injectable.
[00:06:43] [critical] All tested parameters do not appear to be injectable. Try to increase value for '--level' option if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved, maybe you could try to use option '--tamper' and/or switch '--random-agent'.
[4/4] URL - GET http://testphp.vulnweb.com/showimage.php?file=
Do you want to use URL #4 to perform tests? [Y/n] > Y
[00:06:43] [info] Testing URL 'http://testphp.vulnweb.com/showimage.php?file='.
[00:06:43] [info] Testing connection to the target URL.
[00:06:44] [info] Checking if the target is protected by some kind of WAF/IPS.
[00:06:45] [info] Performing identification (passive) tests to the target URL.
[00:06:45] [warning] The provided value for GET parameter 'file' is empty. You are advised to use only valid values, so commix could be able to run properly.
[00:06:46] [info] Setting GET parameter 'file' for tests.
[00:06:46] [info] Performing heuristic (basic) tests to the GET parameter 'file'.
[00:06:47] [critical] <urlopen error unknown url type: ;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))a;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))1;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))a;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))c;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))1;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))o;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))0;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))b;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))x;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|

[illegible]

2b%206143))|echo%20\$((3492%20%2b%206143))1;echo%20\$((3492%20%2b%206143))%
26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))o;echo%20\$((3
492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b
%206143))0;echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|
echo%20\$((3492%20%2b%206143))b;echo%20\$((3492%20%2b%206143))%26echo%20\$(
(3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))x;echo%20\$((3492%20%2b
%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((3492%20%2b%206143))0;
echo%20\$((3492%20%2b%206143))%26echo%20\$((3492%20%2b%206143))|echo%20\$((
3492%20%2b%206143))>