

Esercizio Web Application – preparazione ambiente

```
(kali@kali)-[/home]
$ sudo su
(root@kali)-[/home]
# cd /var/www/html

(root@kali)-[/var/www/html]
# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4314, done.
remote: Counting objects: 100% (92/92), done.
remote: Compressing objects: 100% (74/74), done.
remote: Total 4314 (delta 29), reused 58 (delta 15), pack-reused 4222
Receiving objects: 100% (4314/4314), 2.10 MiB | 3.25 MiB/s, done.
Resolving deltas: 100% (2044/2044), done.

(root@kali)-[/var/www/html]
# chmod -R 777 DVWA/

(root@kali)-[/var/www/html]
# cd DVWA/config

(root@kali)-[/var/www/html/DVWA/config]
# |
```

```
GNU nano 7.2 config.inc.php *
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$dbms = 'MySQL';
#$dbms = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
$_DVWA[ 'db_port' ] = '3306';
```

```
(kali㉿kali)-[/home]
└─$ sudo su
(kali㉿kali)-[/home]
└─# cd /var/www/html

(kali㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4314, done.
remote: Counting objects: 100% (92/92), done.
remote: Compressing objects: 100% (74/74), done.
remote: Total 4314 (delta 29), reused 58 (delta 15), pack-reused 4222
Receiving objects: 100% (4314/4314), 2.10 MiB | 3.25 MiB/s, done.
Resolving deltas: 100% (2044/2044), done.
```

```
(kali㉿kali)-[/var/www/html]
└─# chmod -R 777 DVWA/
```

```
(kali㉿kali)-[/var/www/html]
└─# cd DVWA/config
```

```
(kali㉿kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist config.inc.php
```

```
(kali㉿kali)-[/var/www/html/DVWA/config]
└─# nano config.inc.php
```

```
(kali㉿kali)-[/var/www/html/DVWA/config]
└─# service mysql start
```

```
(kali㉿kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.4-MariaDB-1 Debian 12
```

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> |

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
```

```
; https://php.net/allow-url-fopen
```

```
allow_url_fopen = On
```

```
; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
```

```
; https://php.net/allow-url-include
```

```
allow_url_include = On|
```

```
(kali㉿kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
```

```
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.11.4-MariaDB-1 Debian 12
```

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SELECT host, user FROM mysql.user;

Host	User
127.0.0.1	kali
localhost	mariadb.sys
localhost	mysql
localhost	root

4 rows in set (0.001 sec)


MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.019 sec)

MariaDB [(none)]> |

Prova Burpsuite – intercettazione richiesta POST http

Login :: Damn Vulnerable

127.0.0.1/DVWA/login.php



Username

Password

Login

Damn Vulnerable Web Application (DVWA)

Burp Suite Community Edition v2023.5.4 - Temporary Project

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerSettings

OrganizerExtensionsLearn

Site mapIssue definitionsScope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

http://127.0.0.1

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://127.0.0.1	GET	/DVWA/login.php		200	1686	HTML	Login :: Damn Vulnera...
http://127.0.0.1	GET	/DVWA/		301	527	HTML	301 Moved Permanently
http://127.0.0.1	GET	/DVWA/dvwa/images/...		302	485		

Request

RawPretty

1 GET /DVWA HTTP/1.1

2 Host: 127.0.0.1

3 sec-ch-ua:

4 sec-ch-ua-mobile: ?0

5 sec-ch-ua-platform: ""

6 Upgrade-Insecure-Requests: 1

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36

8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

9 Sec-Fetch-Site: none

10 Sec-Fetch-Mode: navigate

11 Sec-Fetch-User: ?1

12 Sec-Fetch-Dest: document

13 Accept-Encoding: gzip, deflate

14 Accept-Language: en-US,en;q=0.9

Response

RawPretty

1 HTTP/1.1 301 Moved Permanently

2 Date: Wed, 12 Jul 2023 08:55:59 GMT

3 Server: Apache/2.4.57 (Debian)

4 Location: http://127.0.0.1/DVWA/

5 Content-Length: 385

6 Connection: close

7 Content-Type: text/html; charset=iso-8859-1

8

9 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

10 <html>

11 <head>

12 <title>301 Moved Permanently</title>

13 </head>

14 <body>

15 <h1>Moved Permanently</h1>

16 <p>

17 The document has moved

18 here

Inspector

Request attributes2

Request headers14

Response headers6

Burp Suite Community Edition v2023.5.4 - Temporary Project

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://127.0.0.1	GET	/DVWA/			302	351	HTML	php	Login :: Damn Vulnera...			127.0.0.1	security=impossi...	17:05:44 12 J...	8080
2	http://127.0.0.1	GET	/DVWA/login.php			200	1686	HTML					127.0.0.1		17:06:03 12 J...	8080
3	http://127.0.0.1	GET	/favicon.ico			404	451	HTML	ico	404 Not Found			127.0.0.1		17:06:06 12 J...	8080
4	http://127.0.0.1	POST	/DVWA/login.php		✓			HTML	php				127.0.0.1		17:07:08 12 J...	8080

Request

RawHex

1 POST /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Content-Length: 88

4 Cache-Control: max-age=0

5 sec-ch-ua:

6 sec-ch-ua-mobile: ?0

7 sec-ch-ua-platform: ""

8 Upgrade-Insecure-Requests: 1

9 Origin: http://127.0.0.1

10 Content-Type: application/x-www-form-urlencoded

11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36

12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-User: ?1

16 Sec-Fetch-Dest: document

17 Referer: http://127.0.0.1/DVWA/login.php

18 Accept-Encoding: gzip, deflate

19 Accept-Language: en-US,en;q=0.9

20 Connection: close

21

22 username=admin&password=password&Login=Login&user_token=93189be757ddbfaacc10d4974550a9da0

Modifica parametri POST

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Request to http://127.0.0.1:80

ForwardDropIntercept is onActionOpen browser

PrettyRawHex

1 POST /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Content-Length: 88

4 Cache-Control: max-age=0

5 sec-ch-ua:

6 sec-ch-ua-mobile: ?0

7 sec-ch-ua-platform: ""

8 Upgrade-Insecure-Requests: 1

9 Origin: http://127.0.0.1

10 Content-Type: application/x-www-form-urlencoded

11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36

12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-User: ?1

16 Sec-Fetch-Dest: document

17 Referer: http://127.0.0.1/DVWA/login.php

18 Accept-Encoding: gzip, deflate

19 Accept-Language: en-US,en;q=0.9

20 Connection: close

21

22 username=tizio&password=caio&Login=Login&user_token=93189be757ddbfaacc10d4974550a9da0

Burp Suite Community Edition v2023.5.4 - Temporary Project

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

4 x +

SendCancel<>>Follow redirection

Request

PrettyRawHex

1 POST /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Content-Length: 84

4 Cache-Control: max-age=0

5 sec-ch-ua:

6 sec-ch-ua-mobile: ?0

7 sec-ch-ua-platform: ""

8 Upgrade-Insecure-Requests: 1

9 Origin: http://127.0.0.1

10 Content-Type: application/x-www-form-urlencoded

11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36

12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-User: ?1

16 Sec-Fetch-Dest: document

17 Referer: http://127.0.0.1/DVWA/login.php

18 Accept-Encoding: gzip, deflate

19 Accept-Language: en-US,en;q=0.9

20 Connection: close

21

22 username=tizio&password=caio&Login=Login&user_token=93189be757ddbfaacc10d4974550a9da0

Response

PrettyRawHexRender

1 HTTP/1.1 302 Found

2 Date: Wed, 12 Jul 2023 21:13:19 GMT

3 Server: Apache/2.4.57 (Debian)

4 Set-Cookie: security=impossible; path=/; HttpOnly

5 Set-Cookie: PHPSESSID=wdjp3jarvoajgg8g9cno9gh16; expires=Thu, 13 Jul 2023 21:13:19 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=1

6 Expires: Thu, 19 Nov 1981 08:52:00 GMT

7 Cache-Control: no-store, no-cache, must-revalidate

8 Pragma: no-cache

9 Location: login.php

10 Content-Length: 0

11 Connection: close

12 Content-Type: text/html; charset=UTF-8

13

14

Search...0 matches

Search...0 matches

1 x +

SendCancel< * > *

Request

PrettyRawHex

1 GET /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Cache-Control: max-age=0

4 sec-ch-ua:

5 sec-ch-ua-mobile: ?0

6 sec-ch-ua-platform: ""

7 Upgrade-Insecure-Requests: 1

8 Origin: http://127.0.0.1

9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36

10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

11 Sec-Fetch-Site: same-origin

12 Sec-Fetch-Mode: navigate

13 Sec-Fetch-User: ?1

14 Sec-Fetch-Dest: document

15 Referer: http://127.0.0.1/DVWA/login.php

16 Accept-Encoding: gzip, deflate

17 Accept-Language: en-US,en;q=0.9

18 Cookie: PHPSESSID=mmh5lksa7lg59gf5tp375ih385; security=impossible

19 Connection: close

20

21

Response

PrettyRawHexRender

44 <fieldset>

45

46 <label for="user">

Username

</label>

<input type="text" class="loginInput" size="20" name="username">

47

48 <label for="pass">

Password

</label>

<input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password">

50

51

52

53 <p class="submit">

<input type="submit" value="Login" name="Login">

</p>

54

55 </fieldset>

56

57 <input type="hidden" name="user_token" value="e564083c3b26a6fdb43b4b478153418" />

58

59 </form>

60

61

62

63 <div class="message">

Login failed

</div>

<div class="message">

Login failed

</div>

64

65

66

67

68

69

70

71

72

>>

0 matches

0 matches