

## REPORT\_TEAM4

### Comandi per creare una DWVA:

ovvero una damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

```
(kali@kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
604 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali@kali)-[~]
└─$ sudo service apache2 start

(kali@kali)-[~]
└─$ sudo service mysql start

(kali@kali)-[~]
└─$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-2 Debian n/a

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)]> CREATE USER 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'kali'@'127.0.0.1';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye

(kali@kali)-[~]
└─$ cd /var/www/html
```

```
(kali@kali)-[/var/www/html]
└─$ sudo git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 4503, done.
remote: Counting objects: 100% (53/53), done.
remote: Compressing objects: 100% (43/43), done.
remote: Total 4503 (delta 19), reused 35 (delta 9), pack-reused 4450
Receiving objects: 100% (4503/4503), 2.27 MiB | 5.56 MiB/s, done.
Resolving deltas: 100% (2130/2130), done.

(kali@kali)-[/var/www/html]
└─$ sudo chmod -R 777 /var/www/html/DVWA

(kali@kali)-[/var/www/html]
└─$ cd DVWA/config

(kali@kali)-[/var/www/html/DVWA/config]
└─$ sudo cp config.inc.php.dist config.inc.php

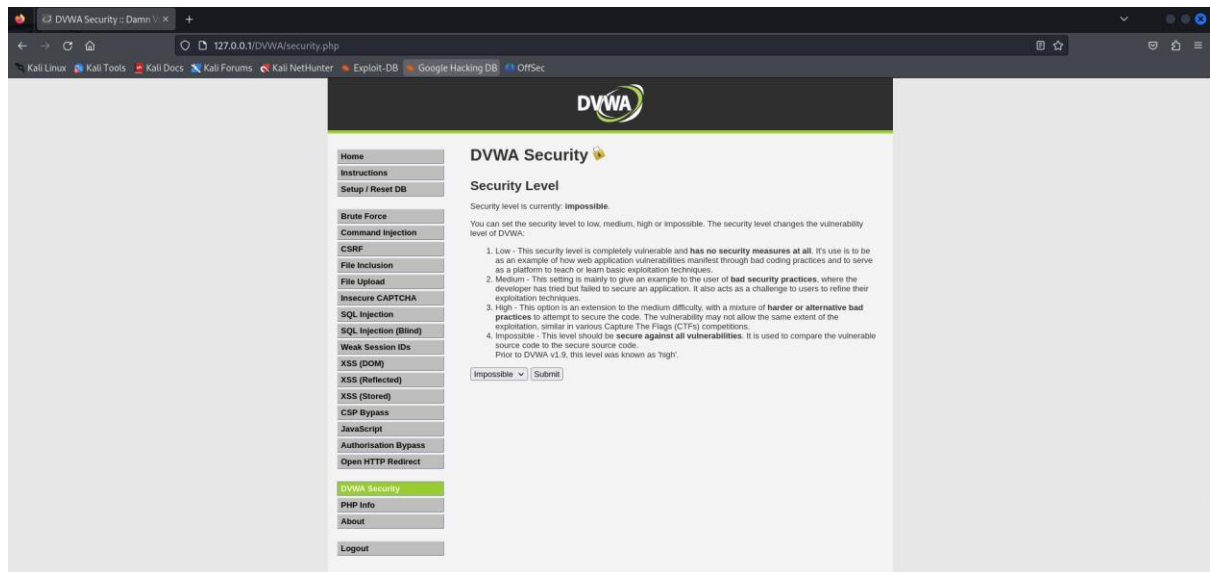
(kali@kali)-[/var/www/html/DVWA/config]
└─$ sudo nano config.inc.php

(kali@kali)-[/var/www/html/DVWA/config]
└─$ sudo nano /etc/php/8.2/apache2/php.ini

(kali@kali)-[/var/www/html/DVWA/config]
└─$ sudo service apache2 restart

(kali@kali)-[/var/www/html/DVWA/config]
└─$
```

## Risposta del codice



## Prova con burpsuite:

Cerchiamo di alterare i dati inseriti e procediamo con l'invio del form usando delle credenziali che sappiamo essere incorrette. Prima di procedere con la trasmissione, utilizziamo il tasto destro e scegliamo l'opzione "send to repeater". Dopo aver premuto il pulsante "send" per inviare i dati di accesso e aver seguito il reindirizzamento, otteniamo il risultato previsto: l'accesso non viene concesso con le credenziali sbagliate. Questo fallimento è confermato nel contenuto della risposta HTTP, dove troviamo il messaggio "Login failed".

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 4

Request cookies 2

Request headers 20

1 POST /DWA/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: "Chromium";v="121", "Not A(Brand";v="99"

6 sec-ch-ua-mobile: ?0

7 sec-ch-ua-platform: "Linux"

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/121.0.6167.85 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/DWA/login.php

18 Accept-Encoding: gzip, deflate, br

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

20 Cookie: security=impossible; PHPSESSID=3dbet6cia6vhash5pvc16tr2o

21 Connection: close

22

23 username=admin&password=Dani1o6&login=Login&user\_token=3cd93e1792a9ef4f871c201c95d1f951

Event log All issues

Memory: 131.8MB

Send Cancel < >

Target: http://127.0.0.1

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 18

Response headers 9

Request

1 GET /DWA/Login.php HTTP/1.1

2 Host: 127.0.0.1

3 Cache-Control: max-age=0

4 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"

5 sec-ch-ua-mobile: ?0

6 sec-ch-ua-platform: "Linux"

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/121.0.6167.85 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/DWA/login.php

16 Accept-Encoding: gzip, deflate, br

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

18 Cookie: security=impossible; PHPSESSID=714p511nld0pubv66rnjjog86

19 Connection: close

20

21

Response

44 <fieldset>

45 <label for="user">

46 Username

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

48 <br />

49 <label for="pass">

50 Password

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

52 <br />

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

54 </fieldset>

55

56

57 <input type="hidden" name="user\_token" value="0da87135536a3ec241422b9a2035d990">

58 </form>

59 <br />

60

61

62 <div class="message">

63 Login failed

64 </div>

65 <br />

66 <br />

67 <br />

68 <br />

69 <br />

70 <br />

71 <br />

72 <br />

Event log All issues

1,672 bytes | 6 millis

Memory: 131.8MB