

Traccia:

Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

Installazione tramite github del web server DVWA

```
(tiger@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 4494, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (35/35), done.
remote: Total 4494 (delta 15), reused 33 (delta 8), pack-reused 4450
Receiving objects: 100% (4494/4494), 2.29 MiB | 5.12 MiB/s, done.
Resolving deltas: 100% (2110/2110), done.
```

Avvio MySQL

```
(tiger@kali)-[/]
$ service mysql start
```

Accesso con permessi root a MySQL

```
(tiger@kali)-[/]
$ sudo mysql -u root -p
[sudo] password for tiger:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 37
Server version: 10.11.6-MariaDB-1 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.
```

Creazione utenza su DB

```
MariaDB [(none)]> create user 'kali'@'127.0.0.0' identified by 'kali';
Query OK, 0 rows affected (0.001 sec)
```

Assegnazione privilegi utente

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.001 sec)
```

Avvio Apache2

```
(tiger@kali)-[/]
$ service apache2 start
```

Modifica configurazione php.ini

```
(tiger@kali)-[/etc/php/8.2/apache2]
$ sudo nano php.ini
```

Login su server DVWA



Username

Password

Login

CSRF token is incorrect

Intercettazione pacchetto Login tramite Burp Suite

Burp Suite Community Edition v2023.11.13 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
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: "Not_A Brand";v="8", "Chromium";v="120"
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/120.0.6099.71 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, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=rqt25uci4h93uqv7uacfs9ei5v
21 Connection: close
22
23 username=admisss&password=password&Login=Login&user_token=02993ecc400693bbdeeb94217bae2db8
```

