

ESERCIZIO - W8D2

- Effettuo l'installazione di MySql Database e Web Server Apache tramite terminale da Kali.

```
(root@kali)-[~]
# apt install mysql -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package mysql

(root@kali)-[~]
# service mysql start

(root@kali)-[~]
# service mysql status
```

```
● mariadb.service - MariaDB 10.5.12 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; >
   Active: active (running) since Fri 2022-07-22 05:51:5>
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 1421 ExecStartPre=/usr/bin/install -m 755 -o >
   Process: 1422 ExecStartPre=/bin/sh -c systemctl unset->
   Process: 1424 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/>
   Process: 1487 ExecStartPost=/bin/sh -c systemctl unset>
   Process: 1489 ExecStartPost=/etc/mysql/debian-start (c>
  Main PID: 1471 (mariabdb)
    Status: "Taking your SQL requests now ... "
   Tasks: 15 (limit: 5154)
  Memory: 112.5M
     CPU: 558ms
   CGroup: /system.slice/mariadb.service
           └─1471 /usr/sbin/mariabdb
```

```
sudo apt install apache2
```

```
sudo service apache2 start
sudo service apache2 status
```

- Questi sono i primi passaggi per soddisfare i requirements dell'esercizio.

- Inseriamo i vari comandi dati dall'esercizio in ordine e cambiamo l'user e la password in kali, kali come quelle del nostro sistema operativo.

```
- cd /var/www/html
- git clone https://github.com/digininja/DVWA
- chmod -R 777 DVWA/
- cd DVWA/config
- cp config.inc.php.dist config.inc.php
- nano config.inc.php
```

```
DVWA[ 'db_database' ] = 'dvwa';
DVWA[ 'db_user' ]    = 'kali';
DVWA[ 'db_password' ] = 'kali';
DVWA[ 'db_port' ]    = '3306';
```

- Utilizziamo poi i comandi **mysql start** e successivamente **mysql -u root -p** ricordandoci che l'utente e password sono state cambiate .

```
File Actions Edit View Help

(root@kali)-[~]
# service mysql start

(root@kali)-[~]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with
Your MariaDB connection id is 44
Server version: 10.5.12-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporat

Type 'help;' or '\h' for help. Type '\c' to clear

MariaDB [(none)]> 
```

```
File Actions Edit View Help
root@kali
(root@kali)~#
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with \n.
Your MariaDB connection id is 45
Server version: 10.5.12-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab
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 (0.005 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> exit
Bye
(root@kali)~#
```

- Creiamo un user con il comando :
create user 'kali'@'127.0.0.1' identified by 'kali';
successivamente assegnamo i privilegi all'utente kali con il seguente comando:
grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali'; e usciamo con il comando exit.

```
; 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
```

- Avviamo Apache con il comando **service apache2 start** e ci spostiamo nella cartella /etc/php/8.2/apache2 con il comando :
cd /etc/php.8.2/apache2
- Successivamente cambiamo le impostazioni come sopra e rimandiamo il comando **service apache2 start** .

- Attraverso il browser andiamo all'indirizzo 127.0.0.1/DVWA/setup.php dal quale possiamo creare/resettare il database.

Setup Check

Web Server SERVER_NAME: 127.0.0.1

Operating system: *nix

PHP version: 8.1.2
PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
Database username: kali
Database password: *****
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306

reCAPTCHA key: Missing

[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
[User: root] Writable file /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes


[User: root] Writable folder /var/www/html/DVWA/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On  
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database



Username

Password

Login

- Inseriamo quindi Username e password che avevamo in precedenza e dovremmo ottenere la seguente schermata del nostro sito DVWA.



Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

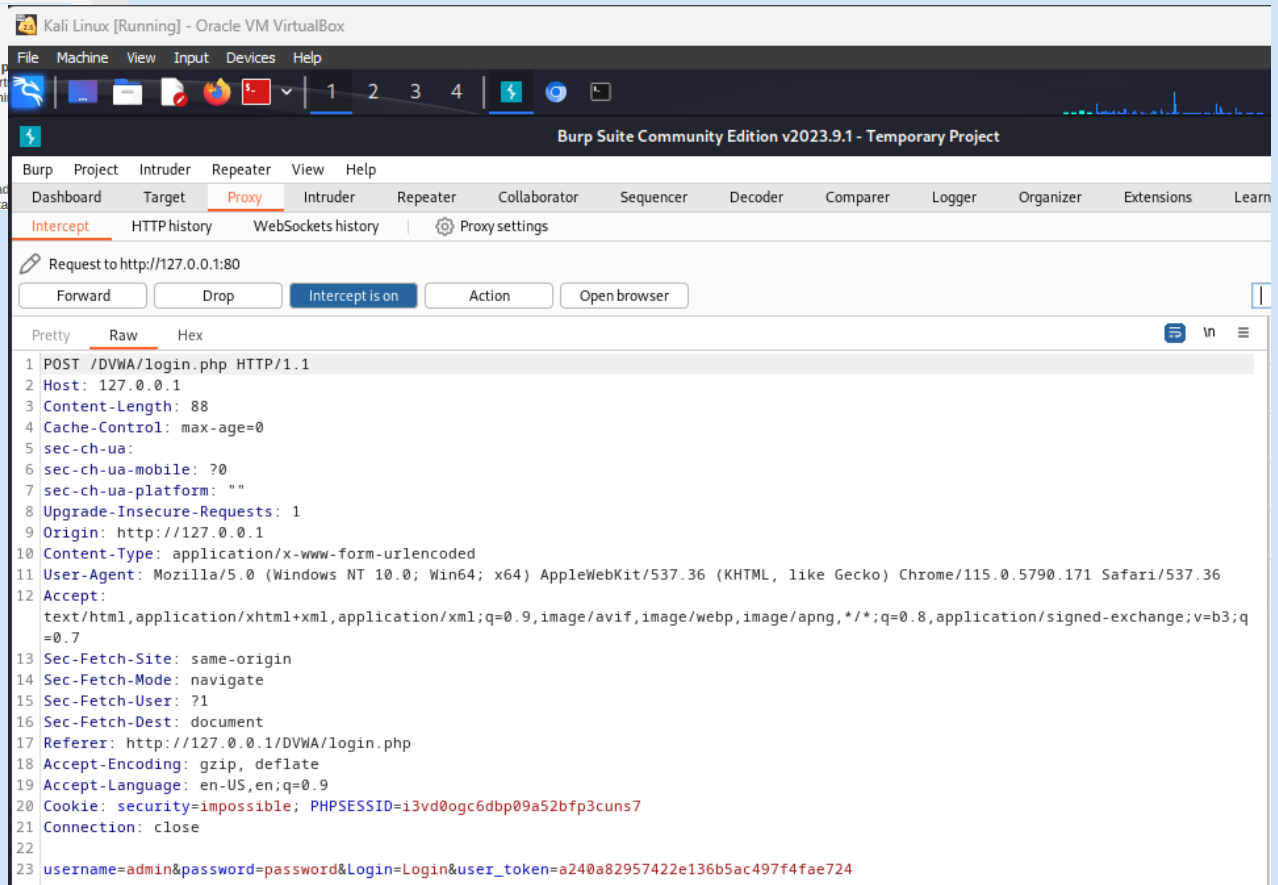
WARNING!

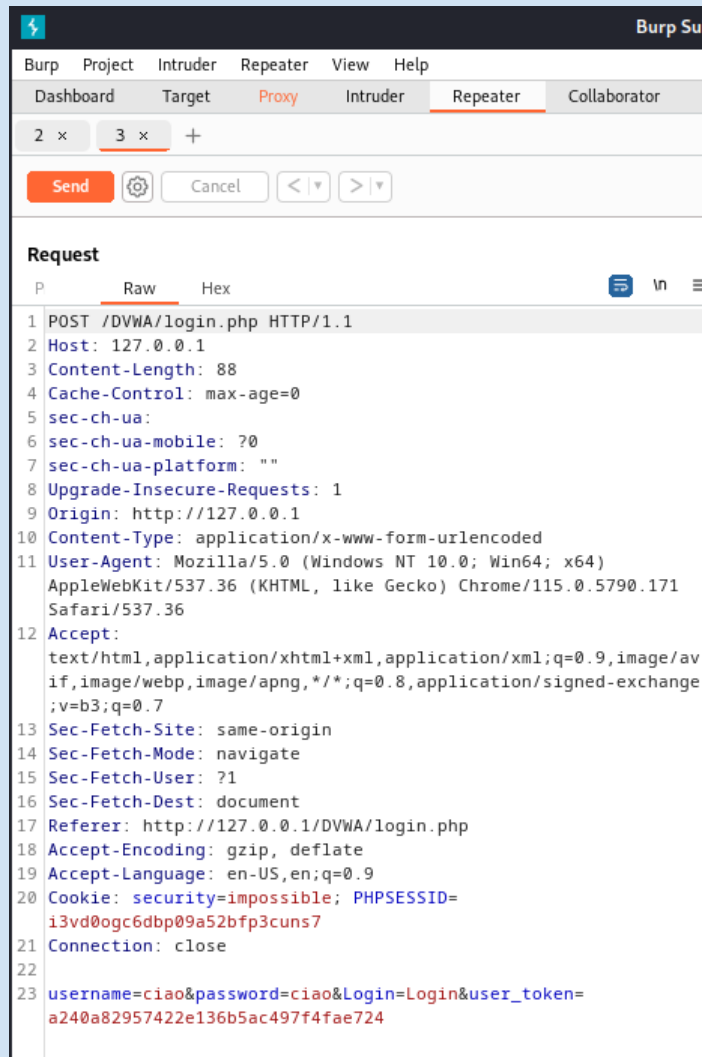
Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine you can download and install [XAMPP](#) for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and ta

• Questo è il risultato che andremmo a ottenere e quindi procediamo con l' intercettazione tramite proxy su Burp Suite.





• Dopo aver effettuato l'intercettazione tramite proxy cambiamo l'username e la password ed effettuiamo il trasferimento verso il Repeater tramite il quale faremo "Send" e successivamente "Follow Redirection".

