DVWA E BURP SUITE W8D1

Configuro una DVWA (Damn Vulnerable Web Application) utile per vedere le tecniche per sfruttare le vulnerabilità nella fase di exploit:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 5165, done.
remote: Counting objects: 100% (118/118), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 5165 (delta 90), reused 82 (delta 76), pack-reused 5047 (from 4)
Receiving objects: 100% (5165/5165), 2.49 MiB | 6.65 MiB/s, done.
Resolving deltas: 100% (2525/2525), 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]
└─# cp config.inc.php.dist config.inc.php

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

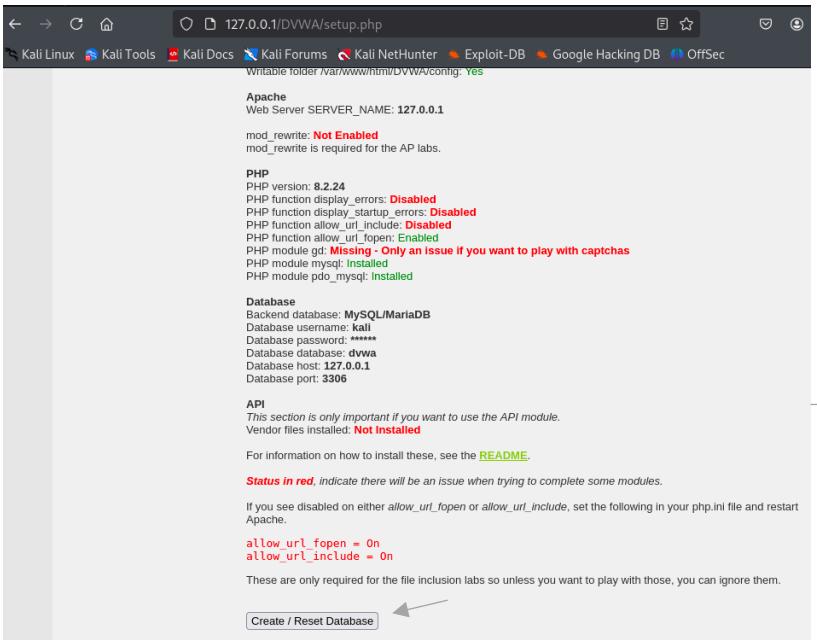
Modifico user e password

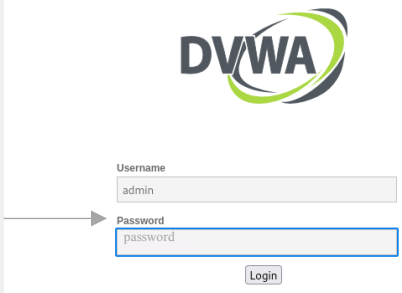
```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'kali';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'kali';
$_DVWA[ 'db_port']      = getenv('DB_PORT') ?: '3306';
```

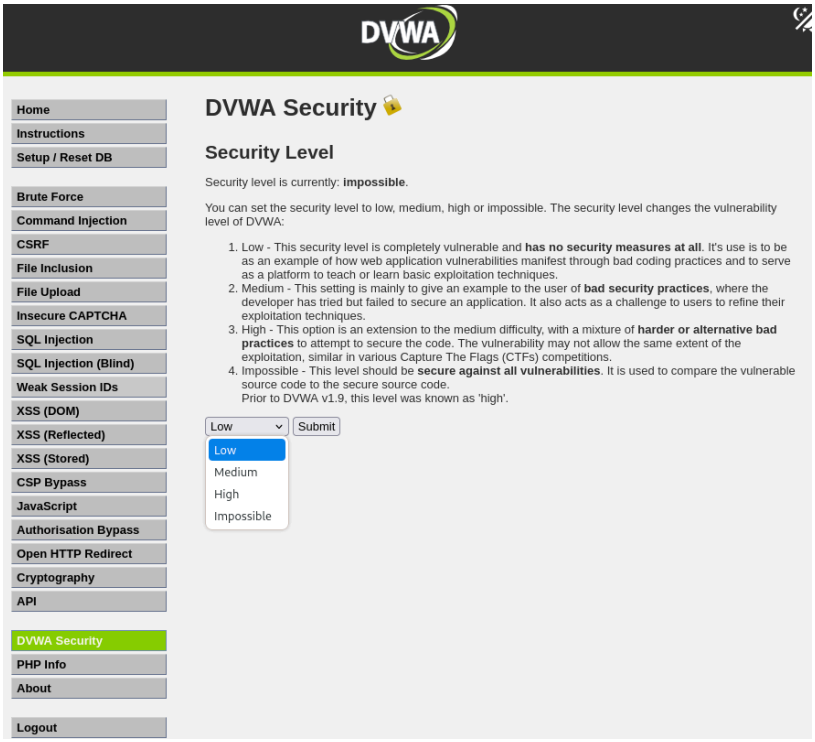
```
┌──(root㉿kali)-[/home/kali]
└─# service mysql start

┌──(root㉿kali)-[/home/kali]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 Debian n/a

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

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'kali'@'127.0.0.01' identified by 'kali' ;
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali'
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> exit
Bye

┌──(root㉿kali)-[/home/kali]
└─# service apache2 start

┌──(root㉿kali)-[/home/kali]
└─# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

┌──(root㉿kali)-[/home/kali]
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
8.2

┌──(root㉿kali)-[/etc/php]
└─# cd /etc/php/8.2/apache2

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# sudo nano php.ini

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# service apache2 start
```

```
; 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
```

Apro sul browser DVWA:







Apro BurpeSuite, creo un progetto temporaneo, apro un browser e cerco l'indirizzo "1270.0.1/DVWA"