

#### 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 sia durante la build week 1 che durante lo sviluppo del modulo 2, dove vedremo da vicino le tecniche per sfruttare le vulnerabilità nella fase di exploit.

## 1. Configurazione DVWA :

avendo l'utenza root sul terminale di kali linux, ci spostiamo nella directory html, successivamente cloniamo la pagina e modifichiamo i permessi nella sezione DVWA, successivamente entriamo nella cartella DVWA-config e copiamo il file config.inc.php.dist nella directory corrente e lo rinominiamo in config.inc.php, successivamente apriamo il file rinominato e cambiamo utente e password di default inserendo, user:kali, password:kali . Di seguito elencati i comandi per configurare correttamente il DVWA:

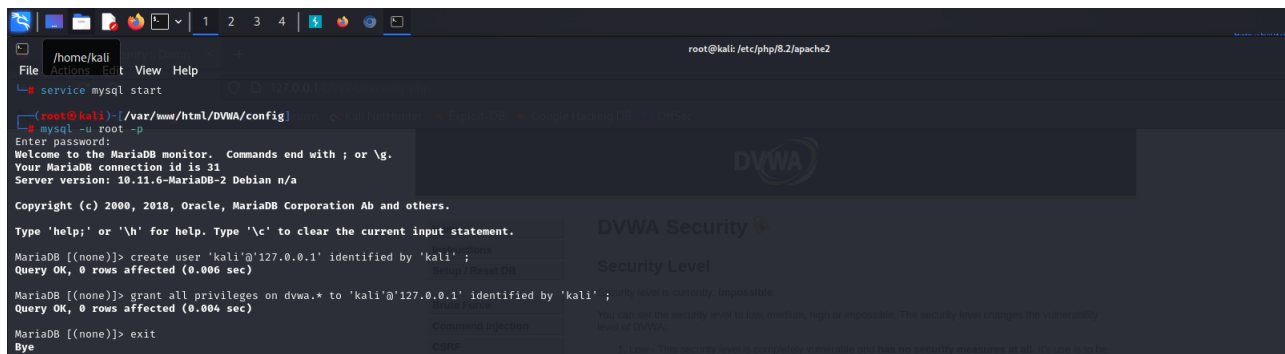
- `cd /var/www/html`
- `git clone https://github.com/digininja/DVWA`
- `chmod -R 777 DVWA/`
- `cd DVWA/config`
- `cp config.inc.php.dist config.inc.php`
- `nano config.inc.php`

```
# WARNING: The database specified under db_database
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root
# 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';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
```

## 2. Servizio mysql :

- Per avviare il servizio mysql basta e connetterci al db con utenza root , eseguiamo questi comandi:
  - `service mysql start`
  - `mysql -u root -p`
- **Creazione utenza db**
  - creiamo un'utenza sul db con il seguente comando `create user 'kali'@'127.0.0.1' identified by 'kali'` ;
  - successivamente assegniamo i privilegi all'utente kali con il seguente comando: `grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;`
  - ed usciamo utilizzando `"exit"`



```
root@kali: /etc/php/8.2/apache2
File Actions Edit View Help
service mysql start

(root@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: 10.11.6-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 (0.006 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
```

### 3. Avviare servizio apache2

Passiamo al servizio apache (il web server). Facciamo partire il servizio con il comando:

- Service apache2 start

Ci spostiamo nella cartella /etc/php/8.2/apache2 con il comando:

- cd /etc/php/8.2/apache2
- Utilizziamo l'editor di testo **nano** per modificare il file php.ini all'interno della cartella apache2.
- Modificate le voci allow\_url\_fopen e allow\_url\_include e settarla su ON

```
; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;;;;;;;

; 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
```

### 4. Verifichiamo che l'indirizzo 127.0.0.1/DVWA/setup.php sia raggiungibile dal browser

Setup DVWA

Instructions

About

## Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.  
If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset**.  
You can also use this to reset the administrator credentials ("admin // password") at any stage.

---

### Setup Check

Web Server SERVER\_NAME: **127.0.0.1**

Operating system: **\*nix**

PHP version: **8.2.12**  
 PHP function display\_errors: **Disabled**  
 PHP function display\_startup\_errors: **Disabled**  
 PHP function allow\_url\_include: **Disabled**  
 PHP function allow\_url\_fopen: **Enabled**  
 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**

Writable folder `/var/www/html/DVWA/hackable/uploads/`: **Yes**  
 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

## 5. Accedere al database inserendo le credenziali di default

- andare nella sezione DVWA Security

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

PHP Info

About

Logout

DVWA Security

### Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

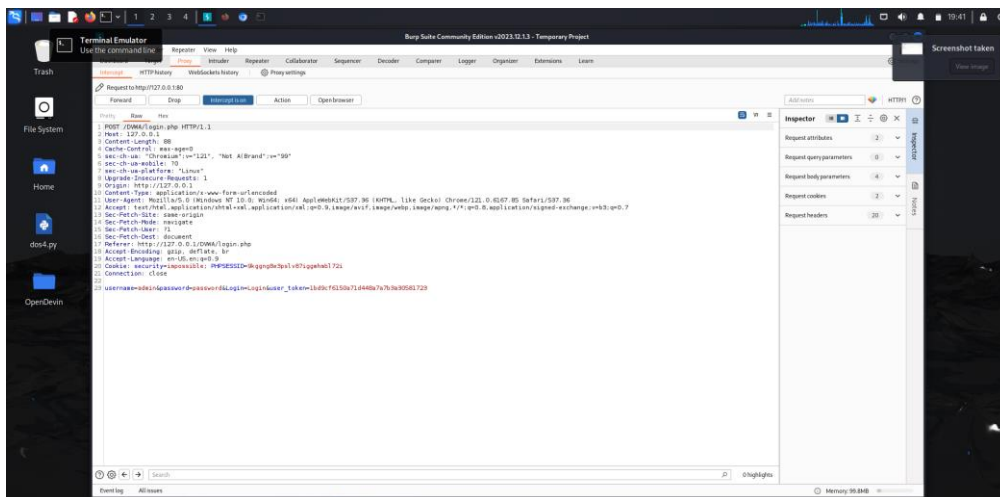
1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.  
Prior to DVWA v1.9, this level was known as 'high'.

Impossible

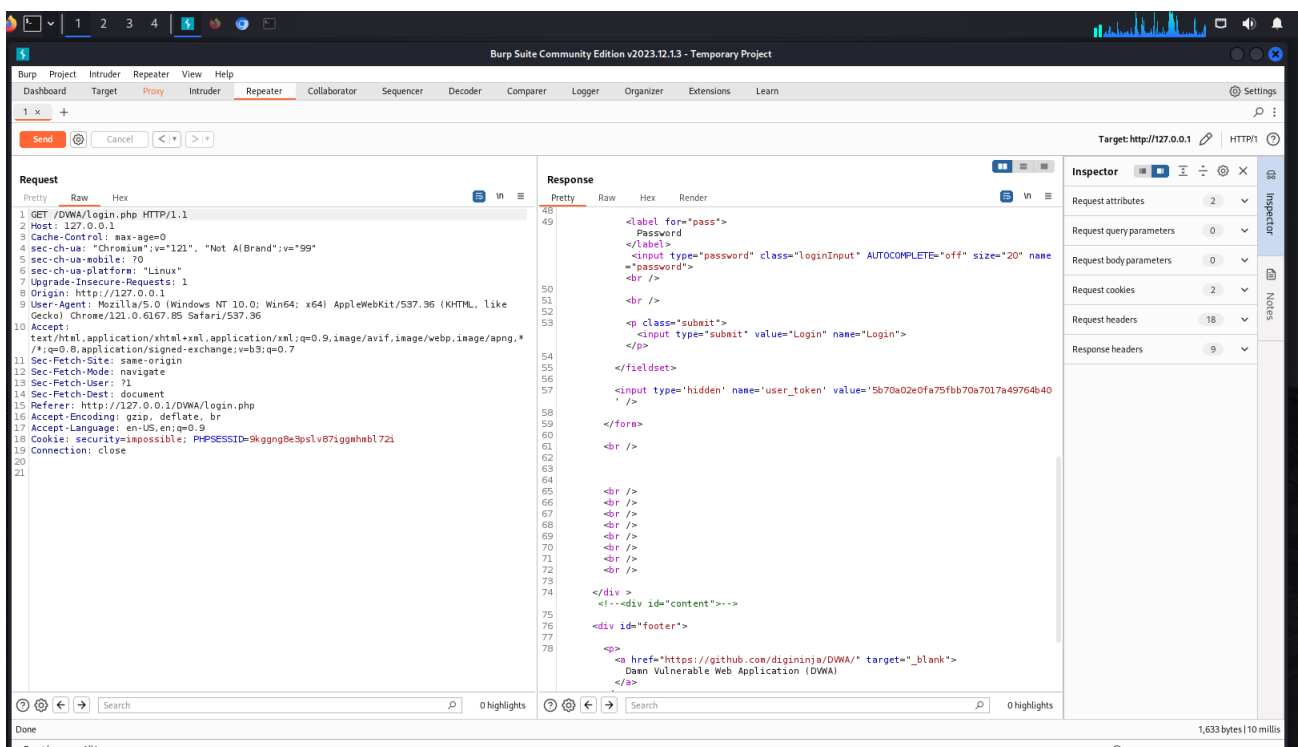
Submit

## 6. Burpsuite

- scegliamo un progetto temporaneo ed apriamo un browser, inserendo l'indirizzo della nostra DVWA: `1270.0.1/DVWA` e inseriamo nei campi login e password i valori «admin» e «password» . Intercettiamo poi la richiesta con burp e vediamo come possiamo modificarla:



- Proviamo a modificare i campi, ed inviare la richiesta inserendo delle credenziali errate. Prima di inviare la richiesta, clicchiamo con il tasto destro e selezioniamo «send to repeater» Clicchiamo su send per inviare la richiesta di login ed e poi su follow redirection:



- Possiamo notare che il login failed non spunta nella risposta ma sappiamo che le credenziali sono sbagliate e il login è sbagliato.
- Il motivo per cui non si vede il login failed forse è dovuto alla versione gratuita del software che può limitarne il funzionamento.