

## Configurazione del server DVWA

```
sudo su  
cd /var/www/html  
sudo git clone https://github.com/digininja/DVWA  
cd DVWA/config  
cp config.inc.php.dist config.inc.php  
nano config.inc.php
```

## Cambiare la password

```
$_DVWA[ 'db_server' ] = getenv( 'DB_SERVER' ) ? : '127.0.0.1';  
$_DVWA[ 'db_database' ] = getenv( 'DB_DATABASE' ) ? : 'dvwa';  
$_DVWA[ 'db_user' ] = getenv( 'DB_USER' ) ? : 'dvwa';  
$_DVWA[ 'db_password' ] = getenv( 'DB_PASSWORD' ) ? : 'p@ssw0rd';  
$_DVWA[ 'db_port' ] = getenv( 'DB_PORT' ) ? : '3306';
```

## Configurazione di MySQL

Avviare il database

```
service mysql start
```

```
mysql -u root -p
```

E qui ci porterà alla configurazione del database

I comandi che dobbiamo entrare saranno:

```
create user 'kali'@'127.0.0.1' identified by 'kali' ;  
grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'kali';  
exit
```

Dopo dobbiamo abilitare questi parametri utilizzando nano

```
cd /etc/php/8.2/apache2
```

```
nano php.ini
```

```
;;;;;;;;;;;;;
; 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

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
;from="john@doe.com"
```

E dopo si deve avviare il server apache2

```
service apache2 start
```

Sucessivamente andare su **127.0.0.1/DVWA/setup.php** su firefox e dopo essere entrati con l'indirizzo ip di kali si deve cliccare su create / reset database

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: 8.2.18  
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

Dopo aver creato il database si bisogna impostare il livello di sicurezza piu basso

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

Cryptography

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'.

Low

Submit