

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:
(kali@kali)~[/home/kali/Desktop]
# cd /var/www/html

(kali@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.

(kali@kali)~[/var/www/html]
# chmod -R 777 DVWA/

(kali@kali)~[/var/www/html]
# cd DVWA/config
(kali@kali)~[/var/www/html/DVWA/config]
# cp config.inc.php.dist config.inc.php

(kali@kali)~[/var/www/html/DVWA/config]
# sudo nano config.inc.php

(kali@kali)~[/home/kali]
# service mysql start

(kali@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'@'127.0.0.1' 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

(kali@kali)~[/home/kali]
# service apache2 start

(kali@kali)~[/home/kali]
# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

(kali@kali)~[/home/kali]
# cd /etc/php

(kali@kali)~[/etc/php]
# ls
8.2

(kali@kali)~[/etc/php]
# cd /etc/php/8.2/apache2

(kali@kali)~[/etc/php/8.2/apache2]
# sudo nano php.ini

(kali@kali)~[/etc/php/8.2/apache2]
# service apache2 start
```

Modifico user e password

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

```
; 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:

Writable folder /var/www/html/DVWA/config: yes

Apache
Web Server SERVER_NAME: 127.0.0.1
mod_rewrite: **Not Enabled**
mod_rewrite is required for the AP labs.

PHP
PHP version: 8.2.24
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**

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

API
This section is only important if you want to use the API module.
Vendor files installed: **Not Installed**

For information on how to install these, see the [README](#).

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
admin

Password
password

Login

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

API

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

Low

Medium

High

Impossible

Apro BurpeSuite, creo un progetto temporaneo, apro un browser e cerco l’indirizzo “1270.0.1/DVWA”

Burp Suite Community Edition v2024.9.4 - Temporary Project

Burp Project Intruder Repeater View Help

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

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
1	http://127.0.0.1	GET	/DVWA/login.php			200	1860	HTML	php	Login:: Damn Vuln...			127.0.0.1	security=impossi...	13:07:59;
2	http://127.0.0.1	GET	/favicon.ico			404	487	HTML	ico	404 Not Found			127.0.0.1		13:08:05;
3	http://127.0.0.1	POST	/DVWA/login.php		✓	302	476	HTML	php				127.0.0.1	PHPSESSID=fhch...	13:08:15;
4	http://127.0.0.1	GET	/DVWA/index.php			200	6824	HTML	php	Welcome:: Damn Vul...			127.0.0.1		13:08:15;

Request

Raw

Hex

```
HTTP/1.1 302 Found
Date: Wed, 23 Apr 2025 17:08:15 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=fhchsGkF8evb3v4p8Vpemu489s; expires=Thu, 24 Apr 2025 17:08:15 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Inspector

Raw

Hex

Render

Request attributes

2

Request body parameters

4

Request cookies

2

Request headers

20

Response headers

11

Event log (1)

All issues

Memory: 117.7MB