

Per prima cosa andiamo ad installare la macchina DVWA su Kali (seguiamo le istruzioni del tutorial).

```
└─(root㉿kali)-[~/www/html/DVWA/config]
  └─# cp config.inc.php.dist config.inc.php
  └─# nano config.inc.php

└─(root㉿kali)-[~/www/html/DVWA/config]
  └─# service mysql start

└─(root㉿kali)-[~/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: 10.11.4-MariaDB-1 Debian 12

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 (0.011 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

└─(root㉿kali)-[~/www/html/DVWA/config]
  └─# service apache2 start

└─(root㉿kali)-[~/www/html/DVWA/config]
  └─# cd /etc/php

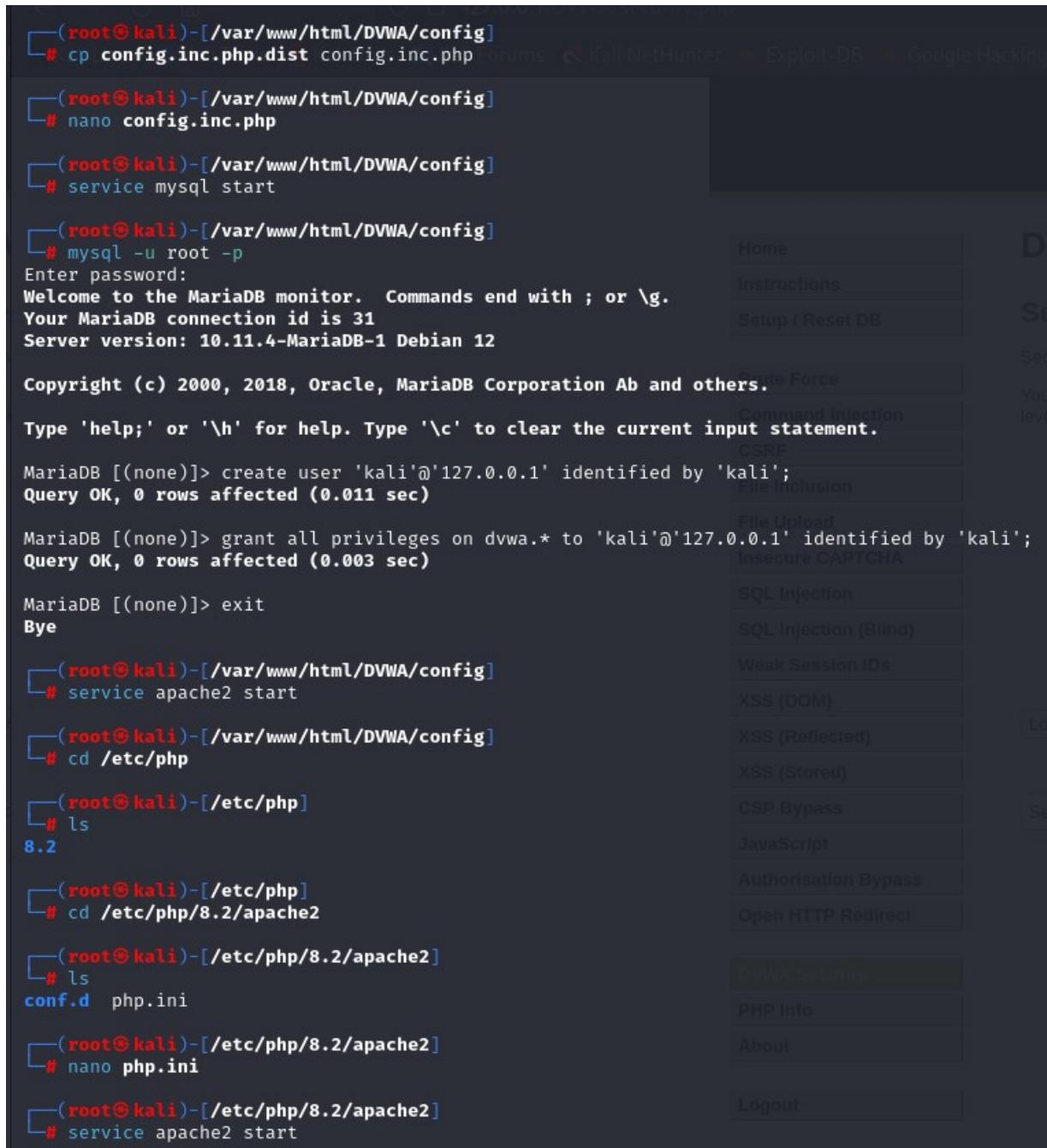
└─(root㉿kali)-[/etc/php]
  └─# ls
  8.2

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

└─(root㉿kali)-[/etc/php/8.2/apache2]
  └─# ls
  conf.d  php.ini

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

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



Una volta installata, settiamo il livello di sicurezza al minimo.

The screenshot shows the DVWA Security interface. On the left is a sidebar with various exploit categories: 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, and Open HTTP Redirect. The 'Security Level' section on the right displays the message "Security level is currently: **low**". Below this, a note states: "You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:". A numbered list explains the four levels: 1. Low - completely vulnerable with no security measures at all. 2. Medium - example of bad security practices where developer failed to secure. 3. High - extension of medium difficulty with harder bad practices. 4. Impossible - secure against all vulnerabilities. A note below says "Prior to DVWA v1.9, this level was known as 'high'". There is a dropdown menu set to "Low" with a "Submit" button. A red oval highlights a message box containing "Security level set to low".

Ora usiamo BurpSuite per intercettare i dati sensibili al login in DVWA (user name e soprattutto password).

The screenshot shows the BurpSuite interface with the 'Proxy' tab selected. The 'Intercept' button is highlighted in blue. The 'Raw' tab is selected in the message list. A captured POST request for 'http://127.0.0.1:80/DVWA/login.php' is shown. The raw data is as follows:

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="117", "Not ;A=Brand";v="8"
6 sec-ch-ua-mobile: ?
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)
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
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/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=apbsfsomunv6lkj09ragblqd32; security=impossible
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=509ce109739f7eb8166f3f781c76bc93
```

A red oval highlights the 'username' and 'password' parameters in the request body.

Dopo aver cambiato user name e password nella schermata sopra, tentiamo di entrare in DVWA con le credenziali false; riceviamo un errore (login failed).

Response

Pretty Raw Hex Render

```
35
36      <br />
37
38  </div>
39  <!--<div id="header">-->
40
41  <div id="content">
42
43    <form action="login.php" method="post">
44
45      <fieldset>
46
47        <label for="user">
48          Username
49        </label>
50        <input type="text" class="loginInput" size="20" name="username">
51        <br />
52
53        <label for="pass">
54          Password
55        </label>
56        <input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password">
57        <br />
58
59        <br />
60
61        <p class="submit">
62          <input type="submit" value="Login" name="Login">
63        </p>
64
65      </fieldset>
66
67      <input type='hidden' name='user_token' value='2a6dd8124493c0b2eddc0569fd58cb1f' />
68
69    </form>
70
71    <br />
72
73    <div class="message">
74      Login failed
75    </div>
76
77    <br />
78    <br />
79    <br />
```