

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

```
(root@kali)-[/var/www/html/DVWA/config]
# cp config.inc.php.dist config.inc.php

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

(root@kali)-[/var/www/html/DVWA/config]
# 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: 10.11.4-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)-[/var/www/html/DVWA/config]
# service apache2 start

(root@kali)-[/var/www/html/DVWA/config]
# cd /etc/php

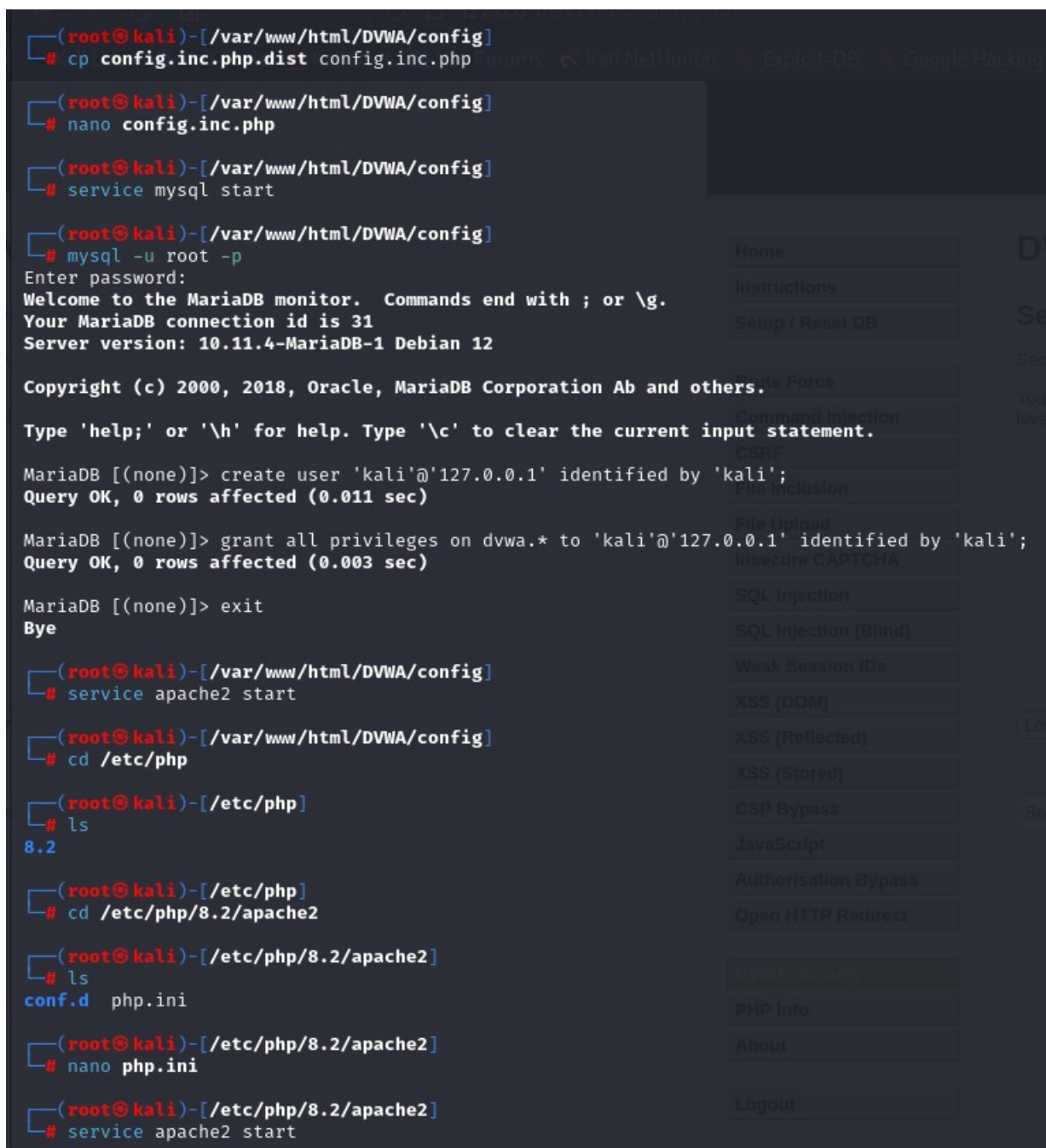
(root@kali)-[/etc/php]
# ls
8.2

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

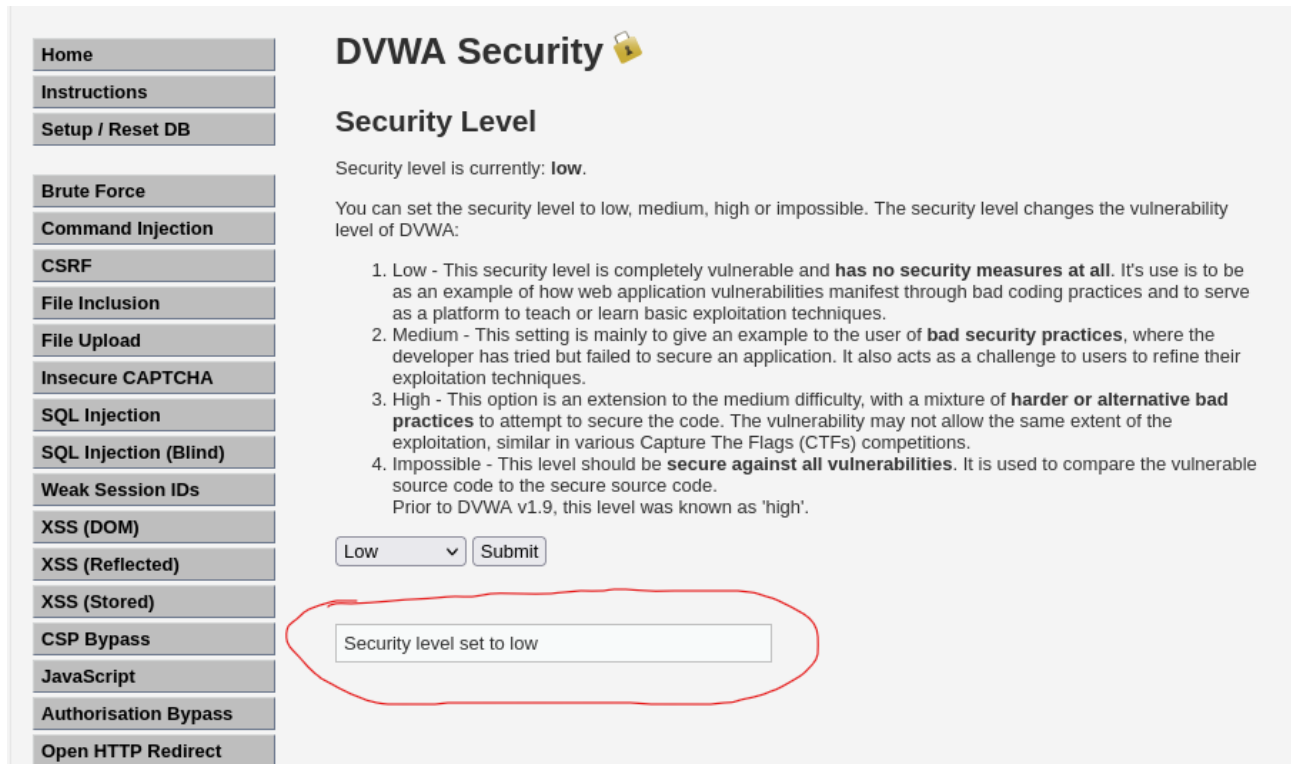
(root@kali)-[/etc/php/8.2/apache2]
# ls
conf.d  php.ini


(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.



**DVWA Security** 

### Security Level

Security level is currently: **low**.

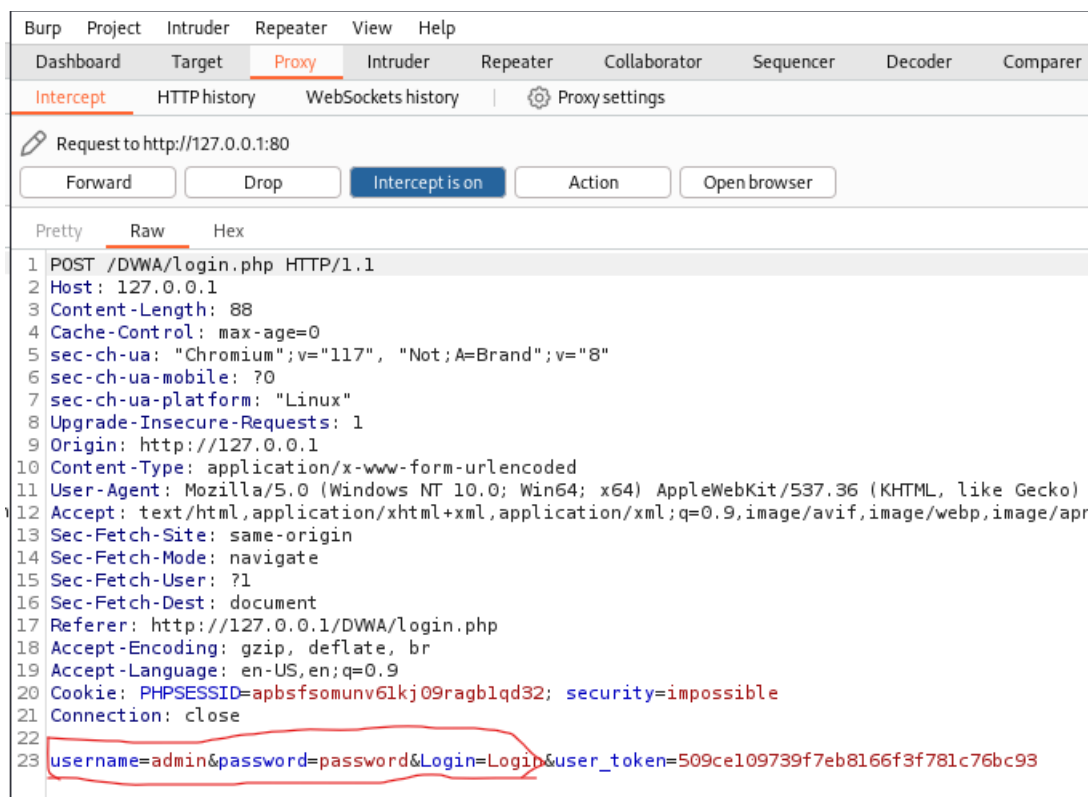
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

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

Security level set to low

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



Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer

Intercept HTTP history WebSockets history Proxy settings

Request to http://127.0.0.1:80

Forward Drop **Intercept is on** Action Open browser

Pretty **Raw** Hex

```
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: ?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)
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apr
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
```

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