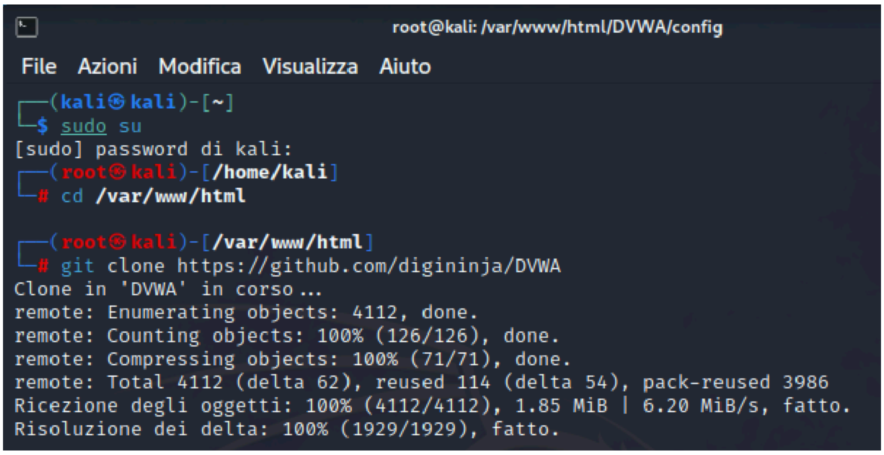
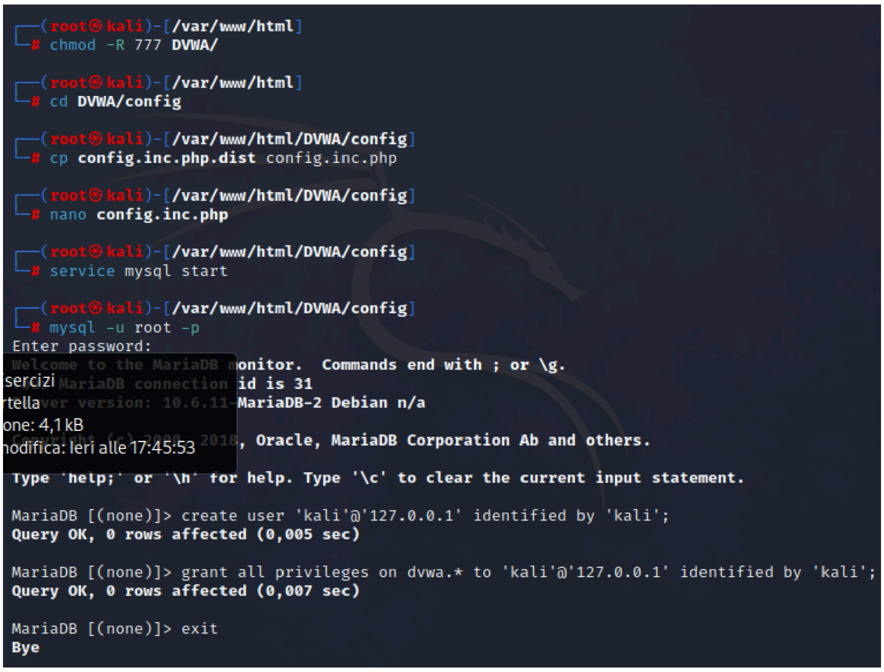
3. Pre-requisiti: Programmazione per Hacker con Python pt. 2

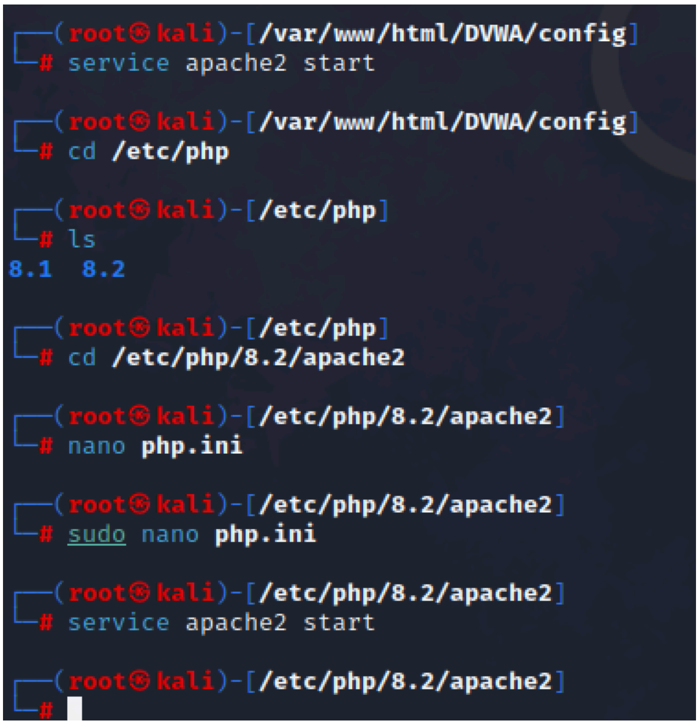


root@kali: /var/www/html/DVWA/config
File Azioni Modifica Visualizza Aiuto

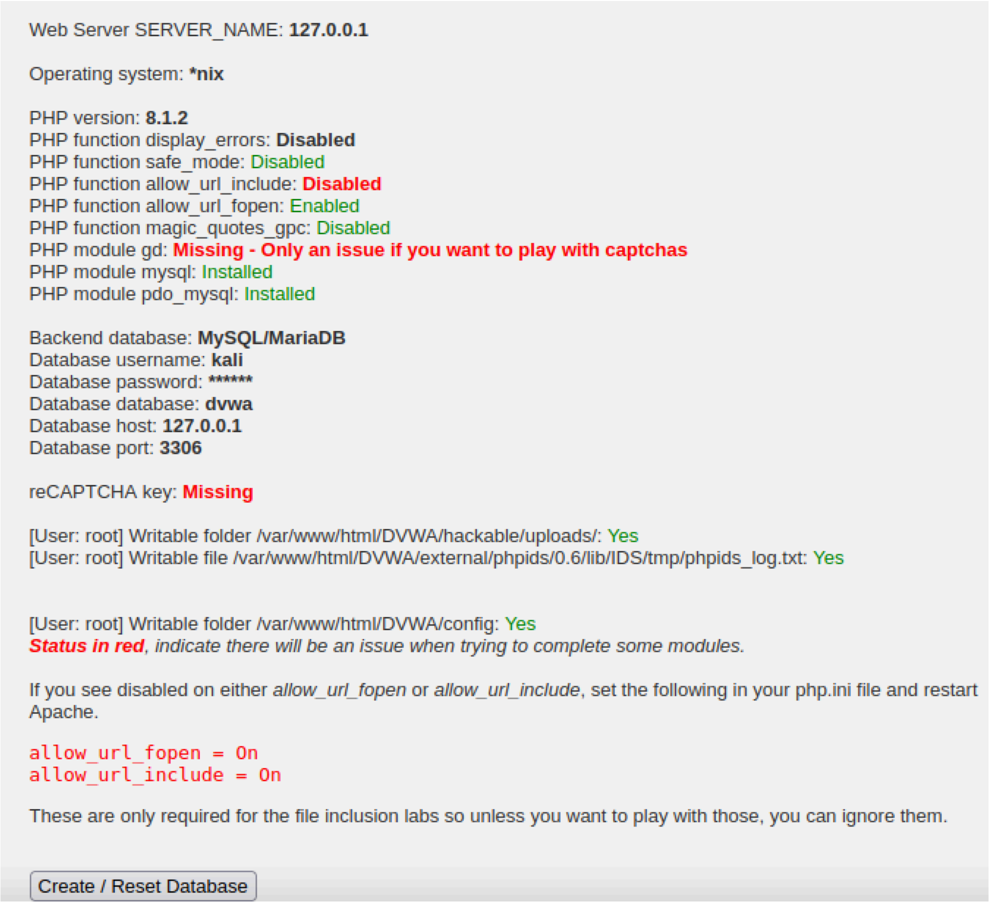
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password di kali:
┌──(root㉿kali)-[/home/kali]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Clone in 'DVWA' in corso...
remote: Enumerating objects: 4112, done.
remote: Counting objects: 100% (126/126), done.
remote: Compressing objects: 100% (71/71), done.
remote: Total 4112 (delta 62), reused 114 (delta 54), pack-reused 3986
Ricezione degli oggetti: 100% (4112/4112), 1.85 MiB | 6.20 MiB/s, fatto.
Risoluzione dei delta: 100% (1929/1929), fatto.
```



```
┌──(root㉿kali)-[/var/www/html]
└─# chmod -R 777 DVWA/

┌──(root㉿kali)-[/var/www/html]
└─# cd DVWA/config

┌──(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: 10.6.11-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';
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 (0,007 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
8.1  8.2

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

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

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

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

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



Web Server SERVER_NAME: **127.0.0.1**

Operating system: ***nix**

PHP version: **8.1.2**
PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
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**

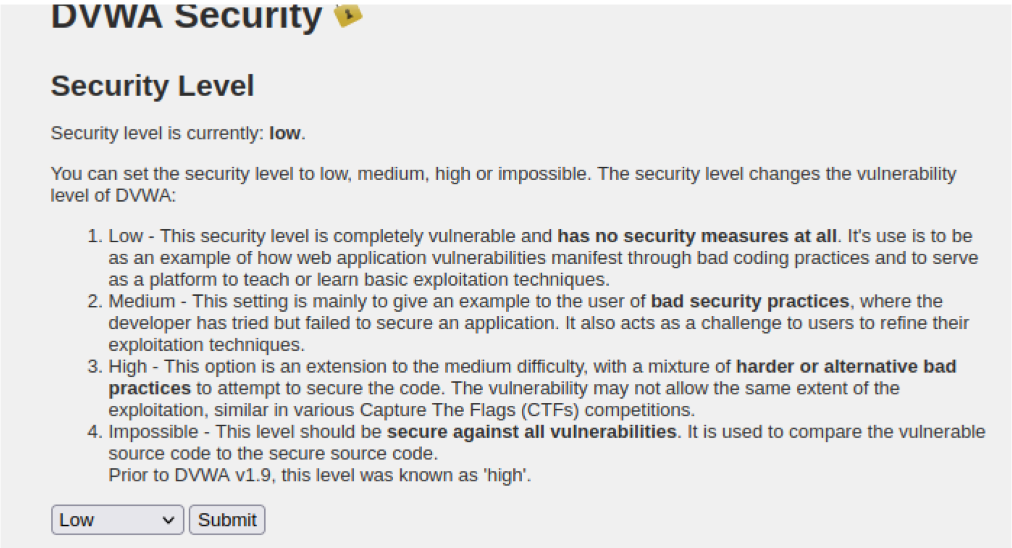
[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
[User: root] Writable file /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

[User: root] 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.



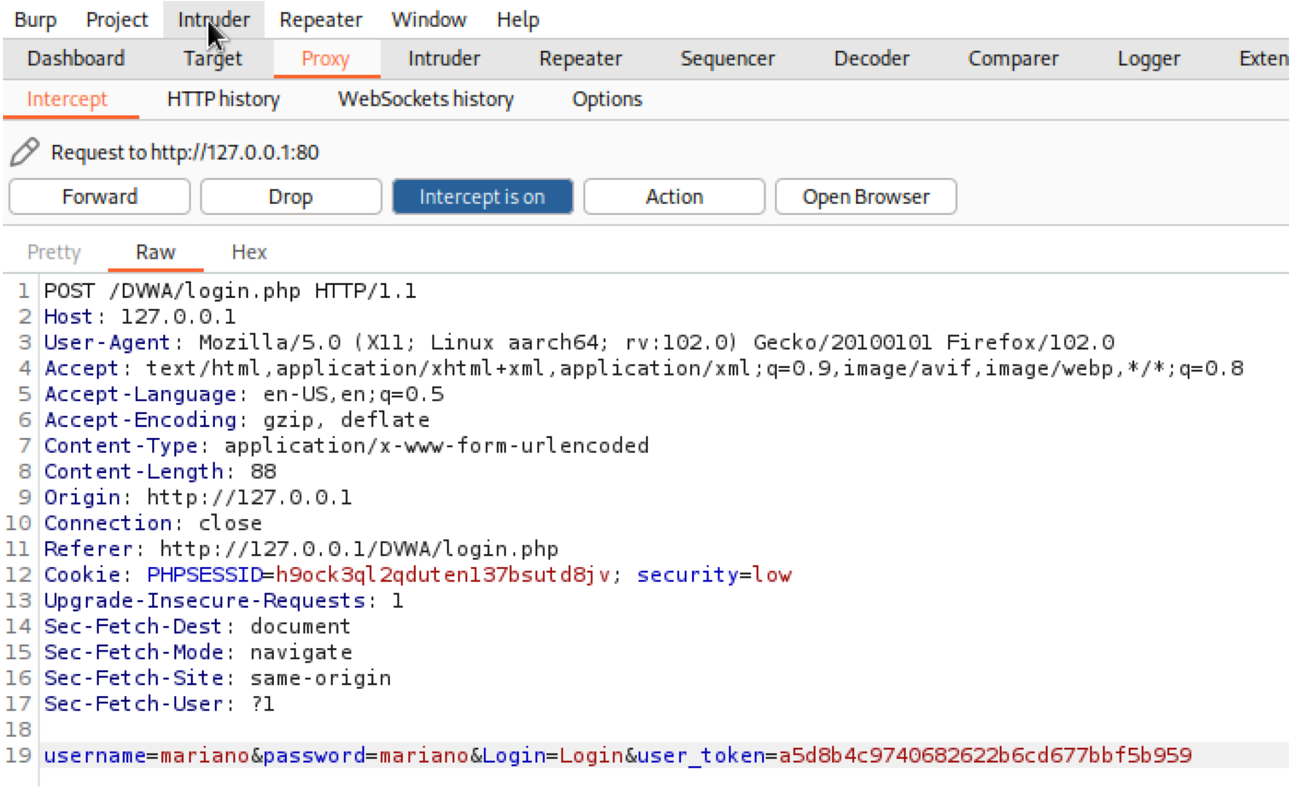
DVWA Security

Security Level

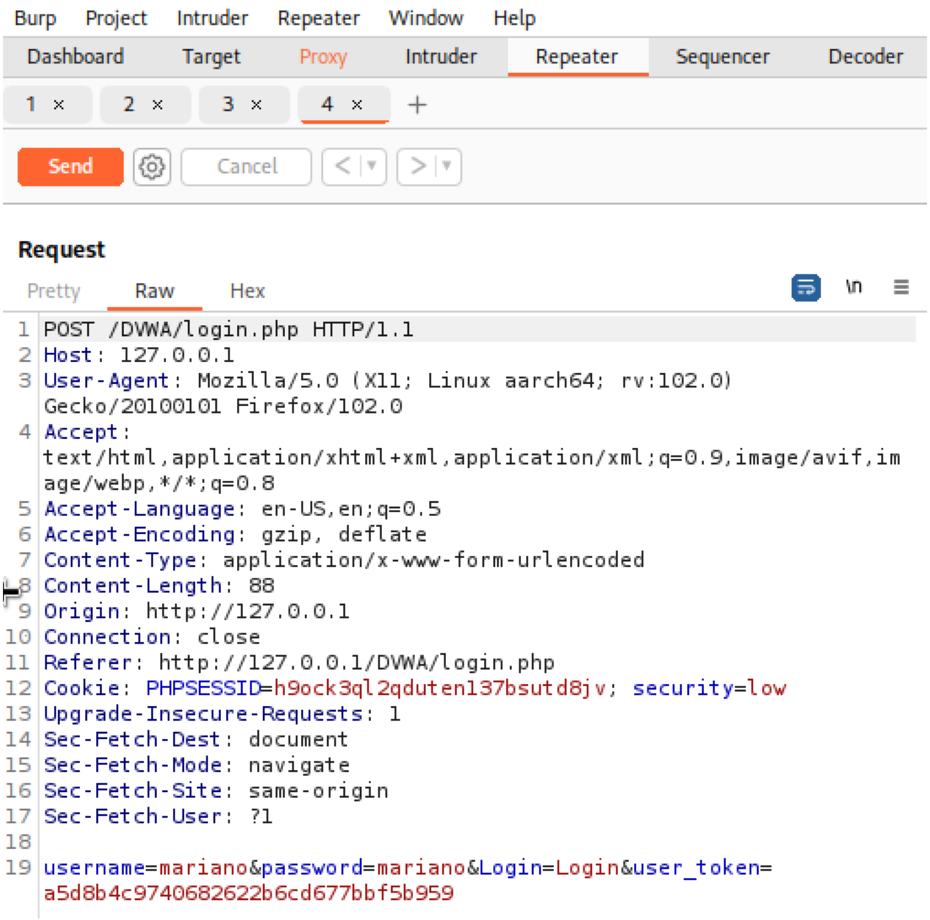
Security level is currently: **low**.

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'.



```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/DVWA/login.php
Cookie: PHPSESSID=h9ock3ql2qduten137bsutd8jv; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

username=mariano&password=mariano&Login=Login&user_token=a5d8b4c9740682622b6cd677bbf5b959
```



```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/DVWA/login.php
Cookie: PHPSESSID=h9ock3ql2qduten137bsutd8jv; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

username=mariano&password=mariano&Login=Login&user_token=
a5d8b4c9740682622b6cd677bbf5b959
```