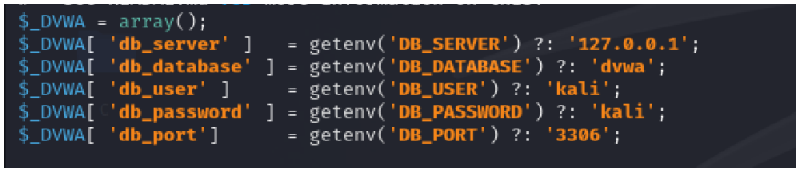
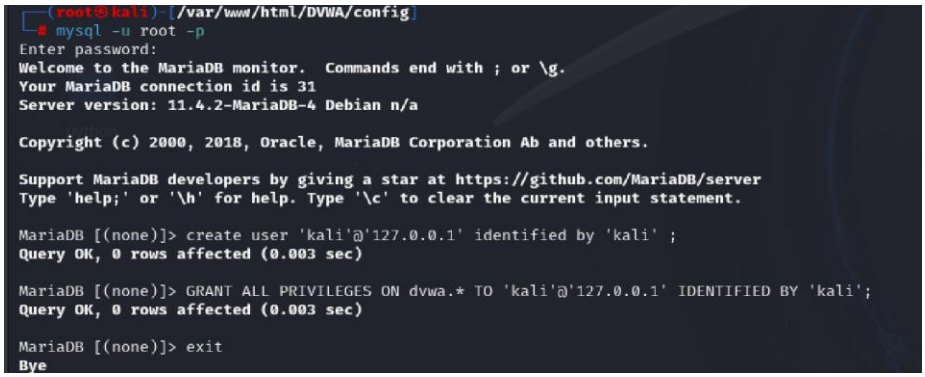
REPORT S3/L3

Traccia: Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

Andiamo ad editare i file config.inc.php, inserendo “kali” “kali” come “user” e “password”.



Sempre con utenza di root su Kali, facciamo partire il servizio mysql con il comando: ***service mysql start*** poi connettiamoci al db con utenza di root con il comando seguente (ricordatevi che la password standard per utente di root è «kali»): ***mysql –u root –p***



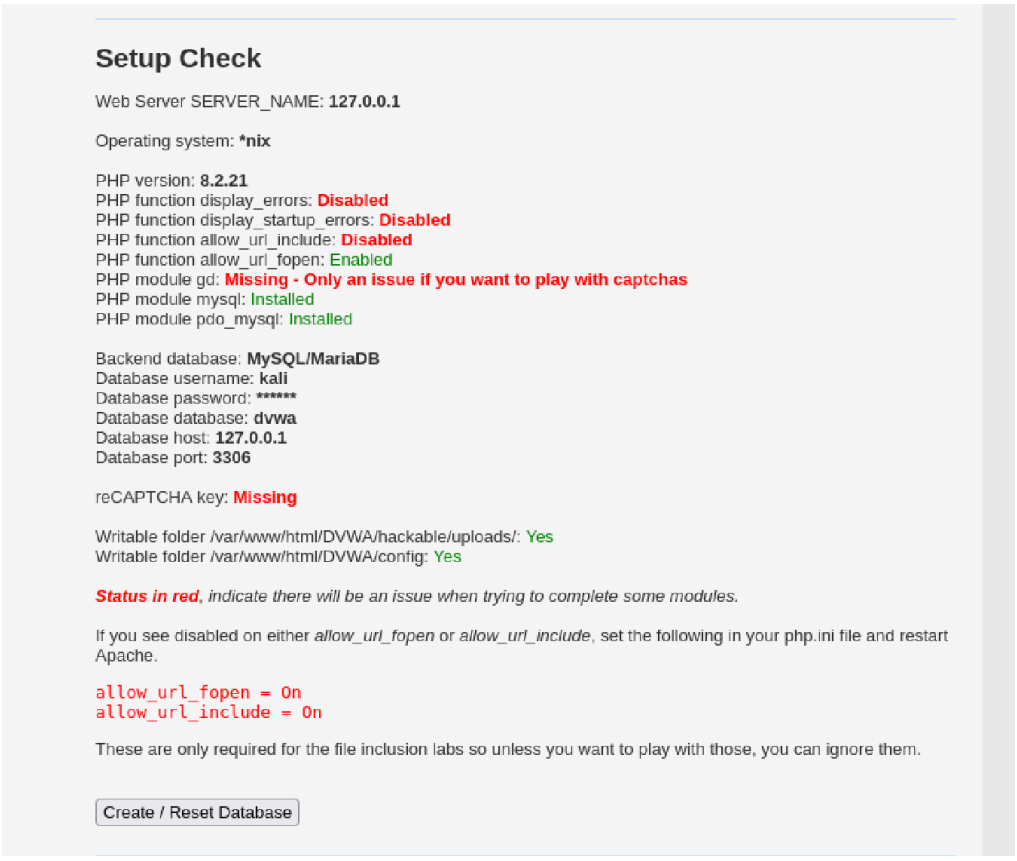
Creiamo un’utenza sul db con il comando: ***create user 'kali'@'127.0.0.1' identified by 'kali' ;*** successivamente assegniamo i privilegi all’utente kali con il seguente comando: ***grant all***

privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ; ed usciamo utilizzando “***exit***”.

```
┌──(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: 11.4.2-MariaDB-4 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)]>
```

Avviamo il servizio apache con il comando “***service apache2 start***” e editiamo il file php.ini.

Infine dopo aver eseguito i vari passaggi inserire nel browser l’ indirizzo 127.0.0.1/DVWA



Setup Check

Web Server SERVER_NAME: **127.0.0.1**

Operating system: ***nix**

PHP version: **8.2.21**
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

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

reCAPTCHA key: **Missing**

Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
Writable folder /var/www/html/DVWA/config: Yes

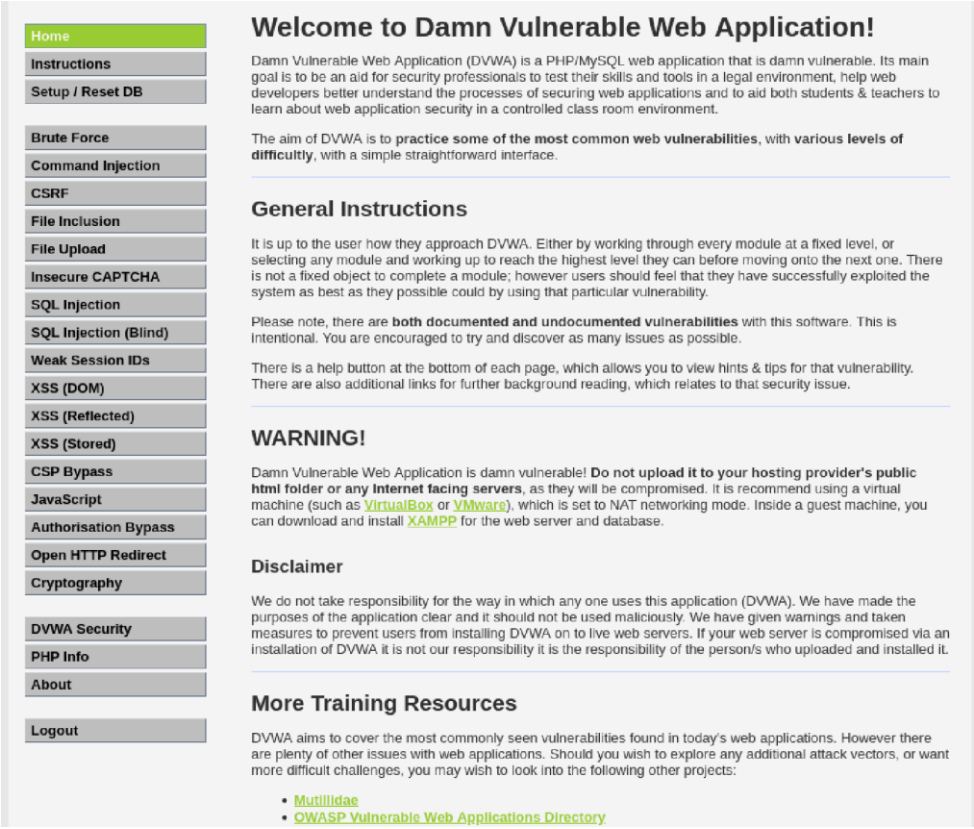
Status in red, *indicate there will be an issue when trying to complete some modules.*

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.

Create / Reset Database



Avviare ora ***BURPSUITE*** andando a intercettare la richiesta di login facendo poi varie prove. Andando a modificare i dati in rosso si possono notare i differenti esiti.