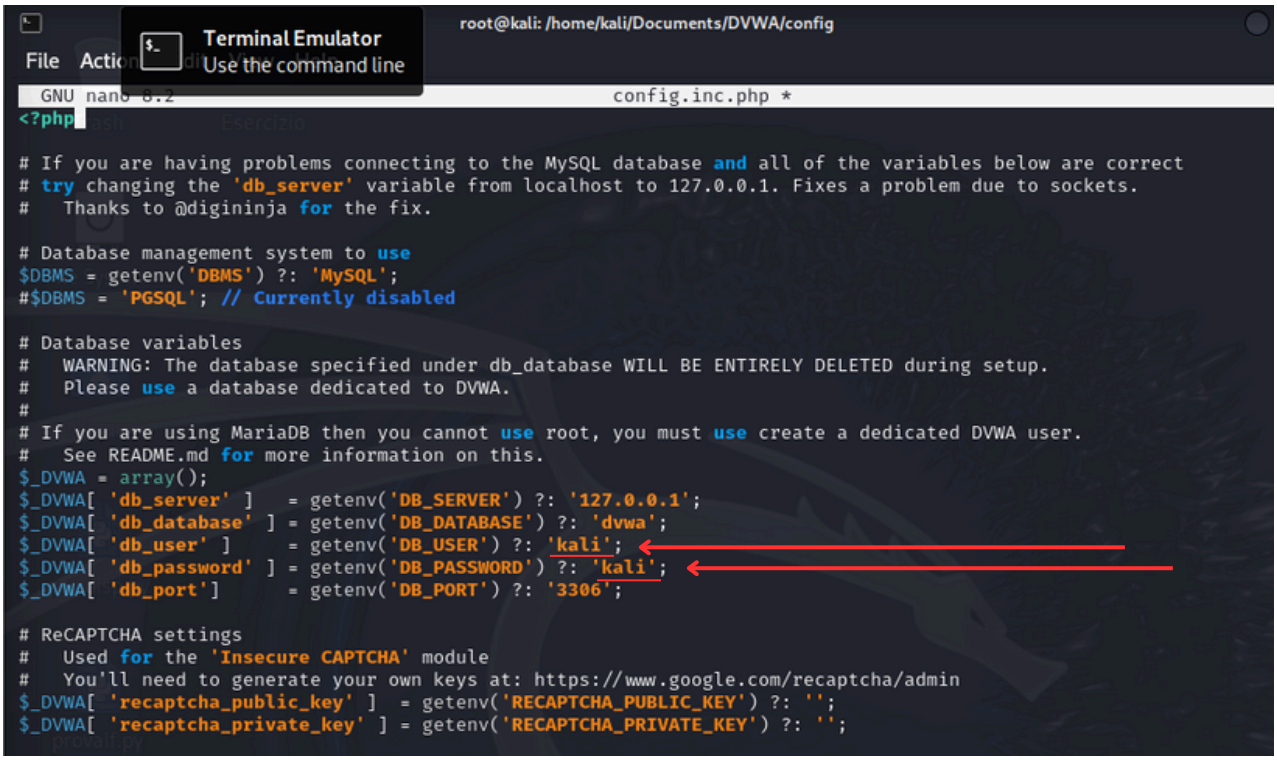
Esercizio S3/L3

L'esercizio di oggi richiedeva la configurazione di una DVWA, ovvero di una Damn Vulnerable Web Application, su Kali Linux. Per iniziare bisogna eseguire i comandi con utenza di root (sudo su), precedentemente proposti nelle slide, ovvero:

- cd /var/www/html
- git clone https://github.com/digininja/DVWA
- chmod –R 777 DVWA/
- cd DVWA/config
- cp config.inc.php.dist config.inc.php
- nano config.inc.php

Una volta eseguiti bisogna modificare il file "config.inc.php" e, sulle voci db_user e db_password inserire "kali"



Successivamente bisogna far partire il servizio mysql con il comando mysql start e connettersi al database con utenza di root attraverso il comando mysql -u root -p.

```
┌──(root㉿kali)-[/home/kali/Documents/DVWA/config]
└─# service mysql start

┌──(root㉿kali)-[/home/kali/Documents/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)]>
```

Ora bisogna creare un utenza sul database e assegnare i prilvilegi, rispettivamente con i comandi:

- create user 'kali'@'127.0.0.1' identified by 'kali' ;
- grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;

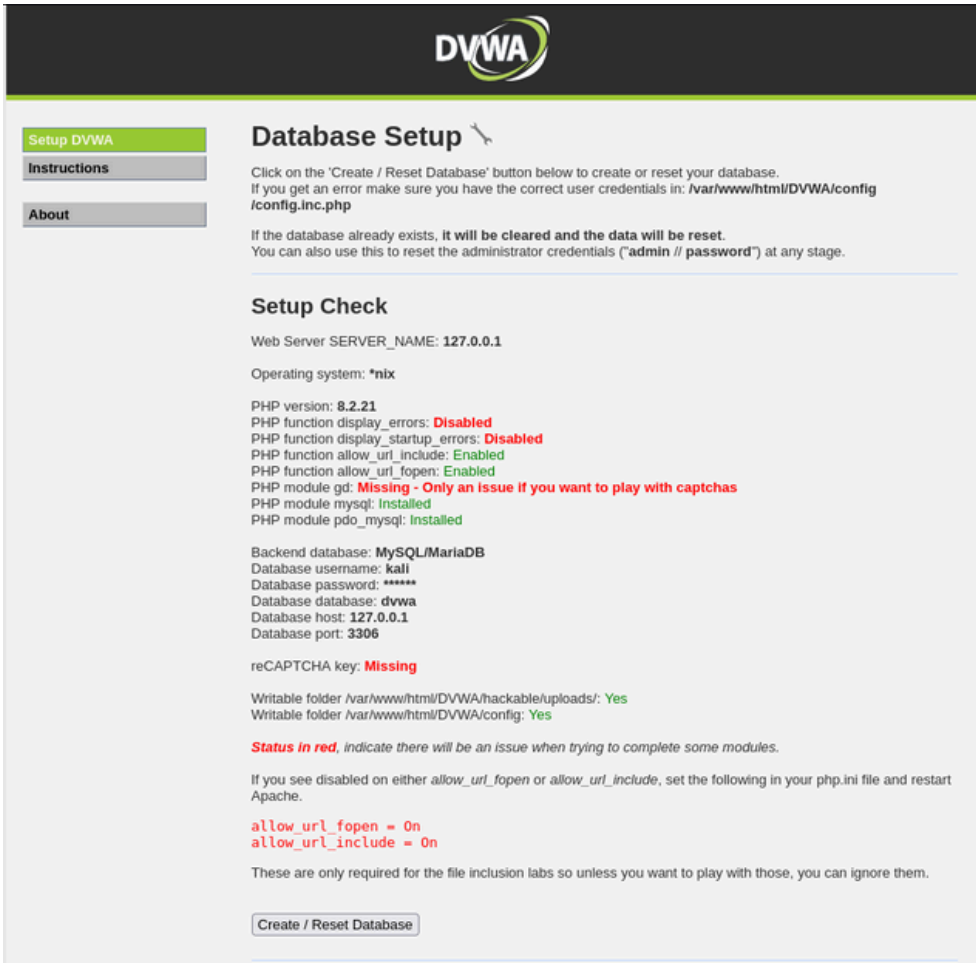
E infine uscire.

```
┌──(root㉿kali)-[/home/kali/Documents/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)]> create user 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> exit
Bye

┌──(root㉿kali)-[/home/kali/Documents/DVWA/config]
└─#
```

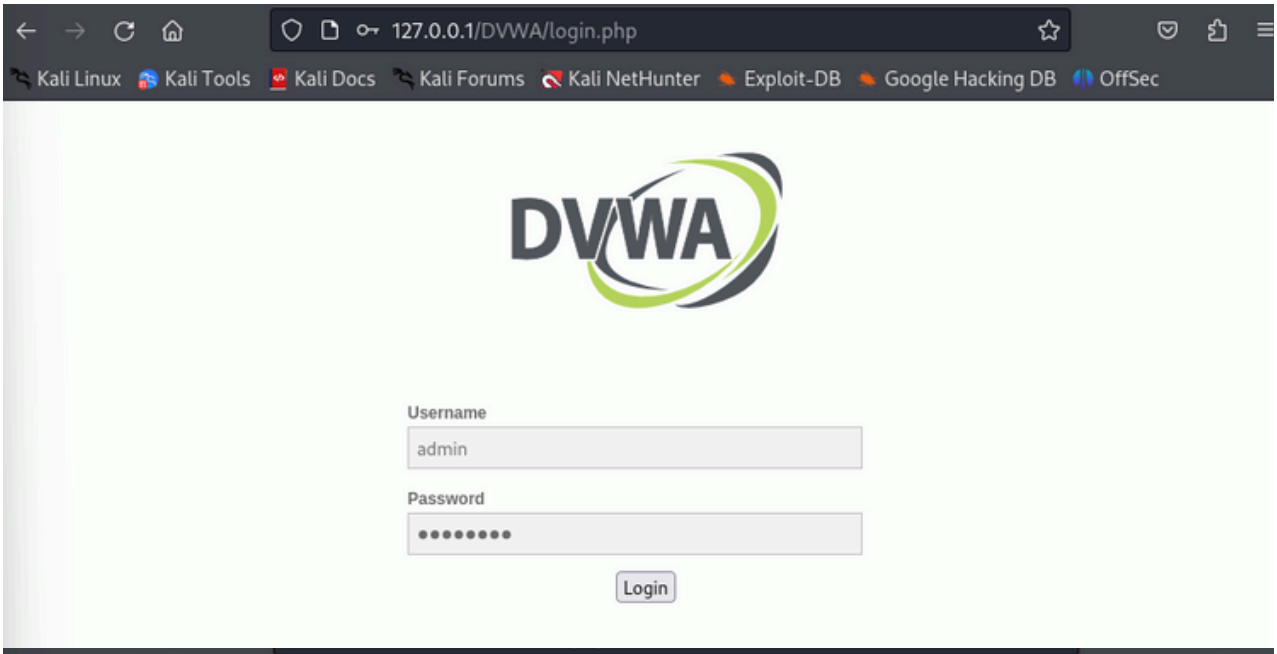
A questo punto bisogna attivare il servizio di web server apache con il comando apache2 start, e con il successivo comando apache2 status si può verificare se è attivo.

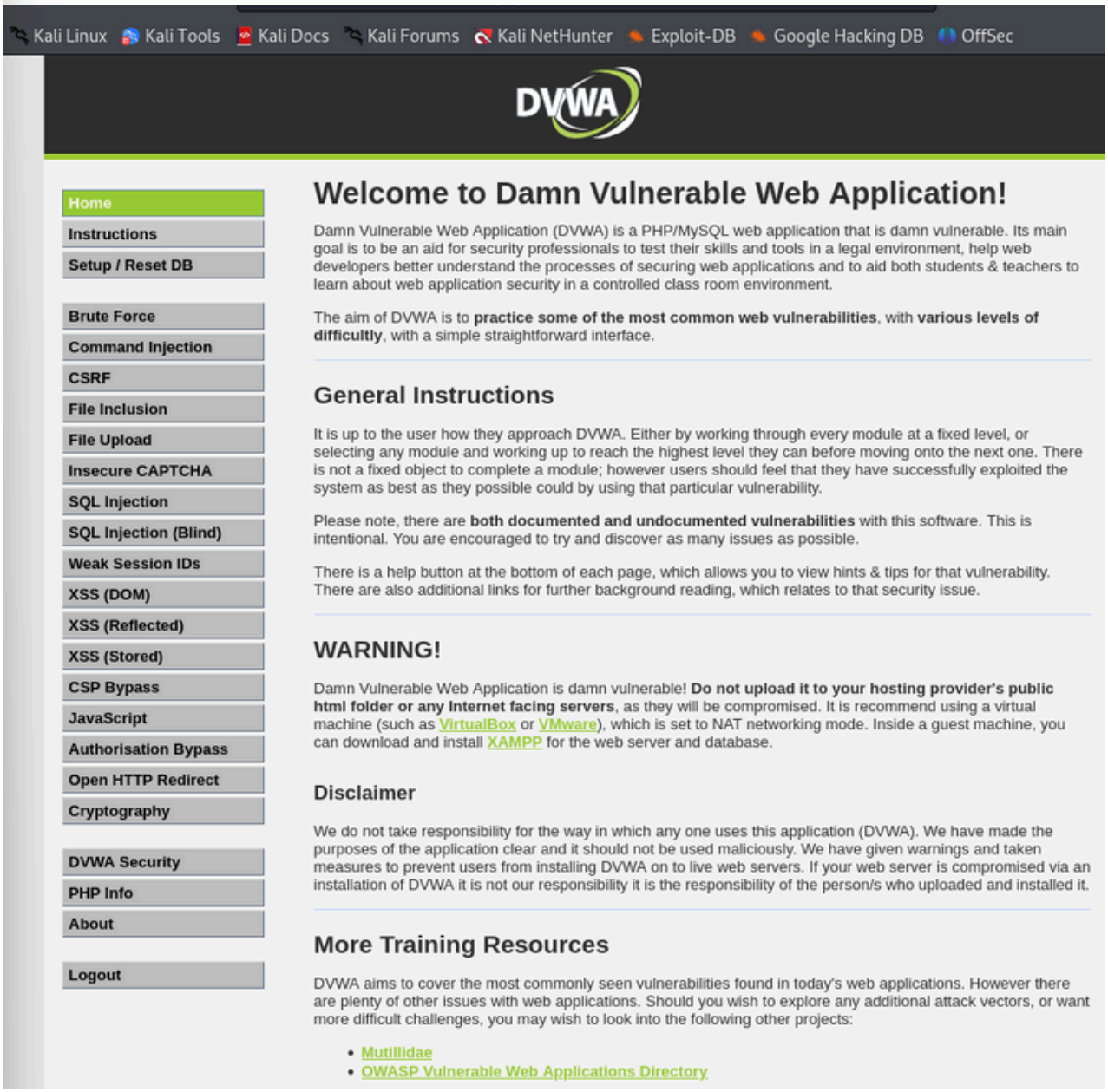
```
┌──(kali㉿kali)-[~]
└─$ service apache2 start

┌──(kali㉿kali)-[~]
└─$ service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Wed 2024-12-11 09:22:04 EST; 1h 9min ago
 Invocation: 0df9d3b82f91442abe587826e11c2978
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 8100 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 8116 (apache2)
      Tasks: 11 (limit: 2269)
     Memory: 19.5M (peak: 27.8M swap: 10.4M swap peak: 15.1M)
        CPU: 639ms
     CGroup: /system.slice/apache2.service
             ├─8116 /usr/sbin/apache2 -k start
             ├─8119 /usr/sbin/apache2 -k start
             ├─8120 /usr/sbin/apache2 -k start
             ├─8121 /usr/sbin/apache2 -k start
             ├─8122 /usr/sbin/apache2 -k start
             ├─8123 /usr/sbin/apache2 -k start
             ├─9835 /usr/sbin/apache2 -k start
             ├─9844 /usr/sbin/apache2 -k start
             ├─9845 /usr/sbin/apache2 -k start
             ├─9846 /usr/sbin/apache2 -k start
             └─9847 /usr/sbin/apache2 -k start

Dec 11 09:22:03 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Dec 11 09:22:04 kali apachectl[8115]: AH00558: apache2: Could not reliably determine the server's ful
Dec 11 09:22:04 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Provando poi a inserire nell'URL di ricerca del browser Firefox 127.0.0.1/DVWA/setup.php ecco come apparirà. Clicchiamo poi sul pulsante "Create/reset Database



Potremo accedere con utenza “admin” e “password”. Dopodichè si aprirà la Web Application





Aprendo adesso Burpsuite potremo intercettare la richiesta al sito e, facendo il login, potremo osservare username e password completamente in chiaro.

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: "Not/A)Brand";v="8", "Chromium";v="126"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Linux"
8  Accept-Language: en-US
9  Upgrade-Insecure-Requests: 1
10 Origin: http://127.0.0.1
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
13 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=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security=impossible; PHPSESSID=miggtvsrvngbrabpe5ctdj5lqq
21 Connection: keep-alive
22
23 username=admin&password=password&Login=Login&user_token=7dcc8a4a8d2f96f814685e194af9159f
```

Proviamo ora a fare la richiesta inversa alla Web Application ma inserendo un username e una password diversa.

Burp | Project | Intruder | Repeater | View | Help

Dashboard | Target | Proxy | Intruder | Repeater | Collaborator | Sequencer | Decoder | Comparer | Logger | Organizer | Extension

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: "Not/A)Brand";v="8", "Chromium";v="126"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Linux"
8  Accept-Language: en-US
9  Upgrade-Insecure-Requests: 1
10 Origin: http://127.0.0.1
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security=impossible; PHPSESSID=miggtvsrvngbrabpe5ctdj5lqq
21 Connection: keep-alive
22
23 username=Salve&password=Salvino&Login=Login&user_token=7dcc8a4a8d2f96f814685e194af9159f
```

Ecco come vedremo la richiesta dal programma.