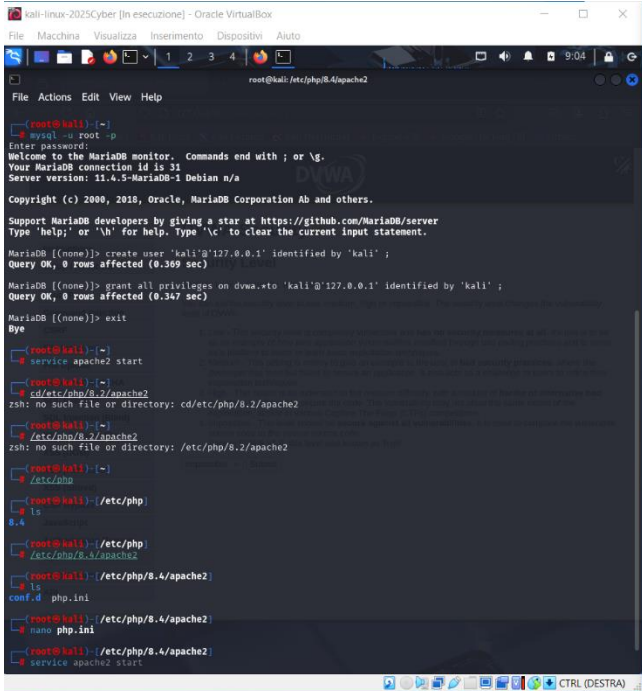


Esercizio S3/L3

Esecuzione dei comandi dal terminale come amministratore.



```
root@kali: /etc/php/8.4/apache2
root@kali:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.5-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation AB and others.

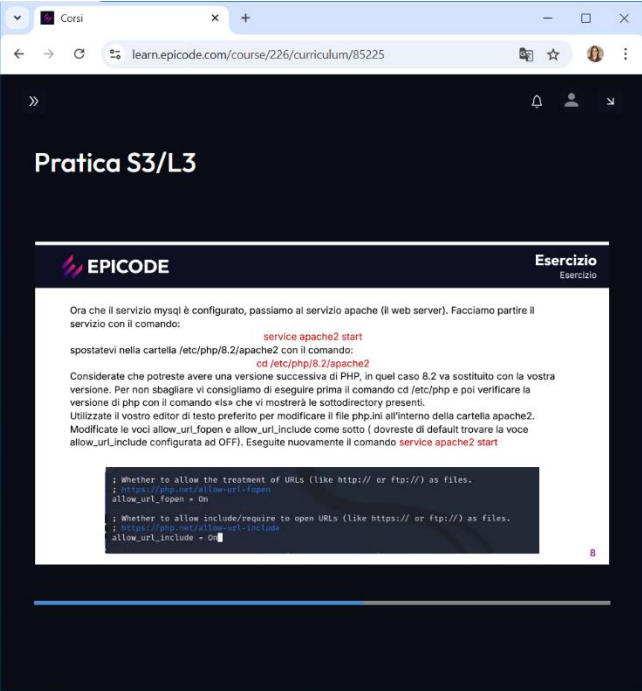
Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.369 sec)

MariaDB [(none)]> grant all privileges on dwva.*to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.347 sec)

MariaDB [(none)]> exit
Bye

root@kali:~# service apache2 start
root@kali:~# cd /etc/php/8.2/apache2
root@kali:~# /etc/php/8.2/apache2
zsh: no such file or directory: cd/etc/php/8.2/apache2
root@kali:~# /etc/php
root@kali:~# /etc/php
root@kali:~# /etc/php/8.4/apache2
root@kali:~# nano php.ini
root@kali:~# service apache2 start
```



Pratica S3/L3

EPICODE

Esercizio

Ora che il servizio mysql è configurato, passiamo al servizio apache (il web server). Facciamo partire il servizio con il comando:

```
service apache2 start
```

spostatevi nella cartella /etc/php/8.2/apache2 con il comando:

```
cd /etc/php/8.2/apache2
```

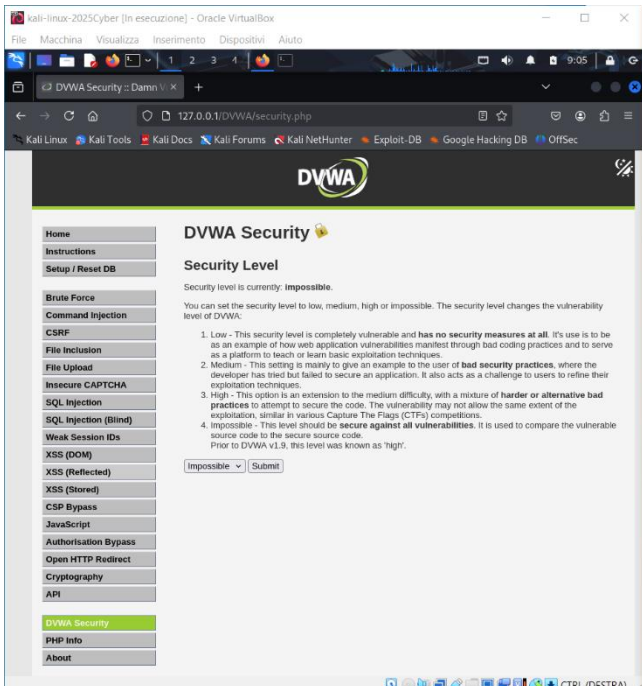
Considerate che potreste avere una versione successiva di PHP, in quel caso 8.2 va sostituito con la vostra versione. Per non sbagliare vi consigliamo di eseguire prima il comando `cd /etc/php` e poi verificare la versione di php con il comando «ls» che vi mostrerà le sottodirectory presenti.

Utilizzate il vostro editor di testo preferito per modificare il file `php.ini` all'interno della cartella `apache2`. Modificate le voci `allow_url_fopen` e `allow_url_include` come sotto (i dovreste di default trovare la voce `allow_url_include` configurata ad OFF). Eseguite nuovamente il comando `service apache2 start`

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = Off
```

Accesso effettuato su DVWA



```
127.0.0.1/DVWA/security.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
```

DVWA Security

Security Level

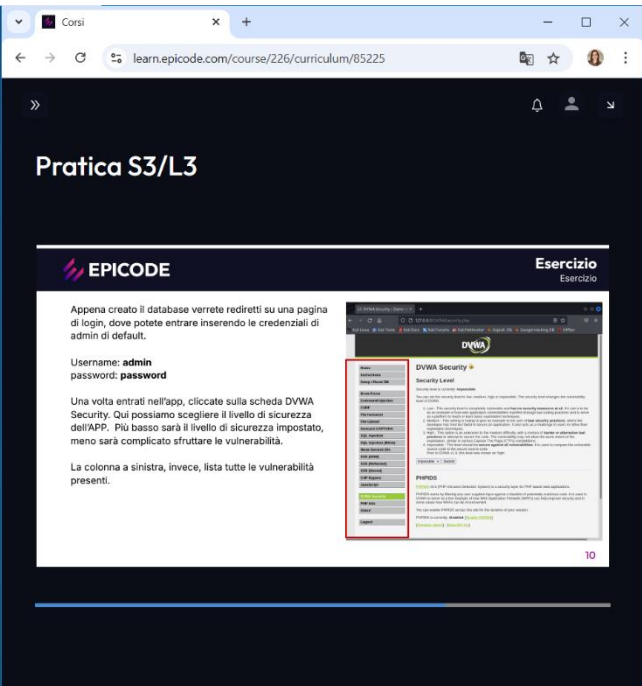
Security level is currently: **Impossible**.

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

- 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.
- 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.
- 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 to various Capture The Flags (CTFs) competitions.
- 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'.

Impossible Submit



Pratica S3/L3

EPICODE

Esercizio

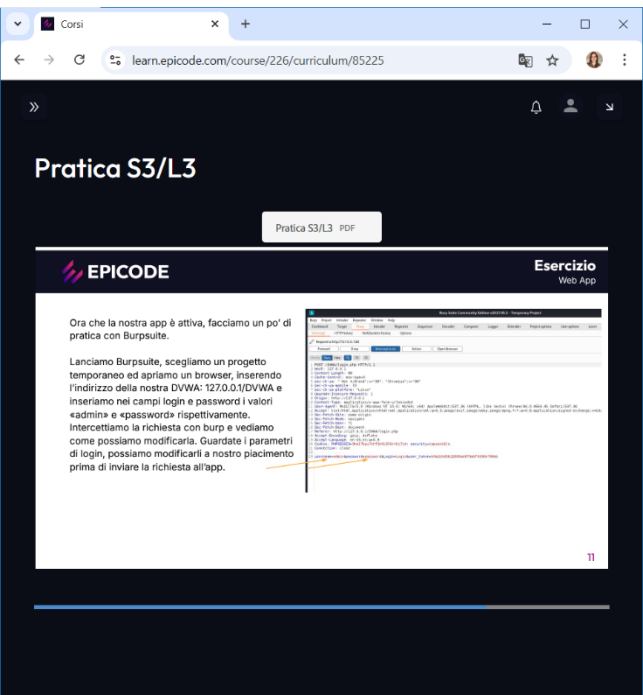
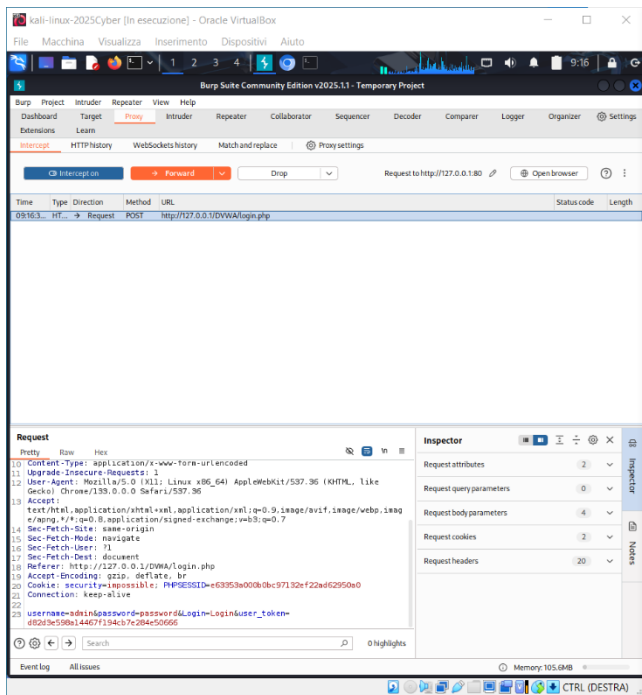
Appena creato il database verrete rediretti su una pagina di login, dove potete entrare inserendo le credenziali di admin di default.

Username: **admin**
password: **password**

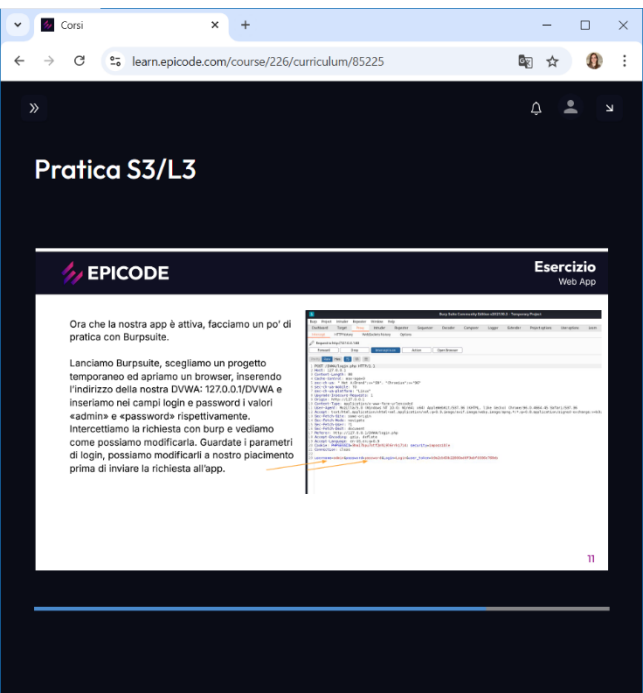
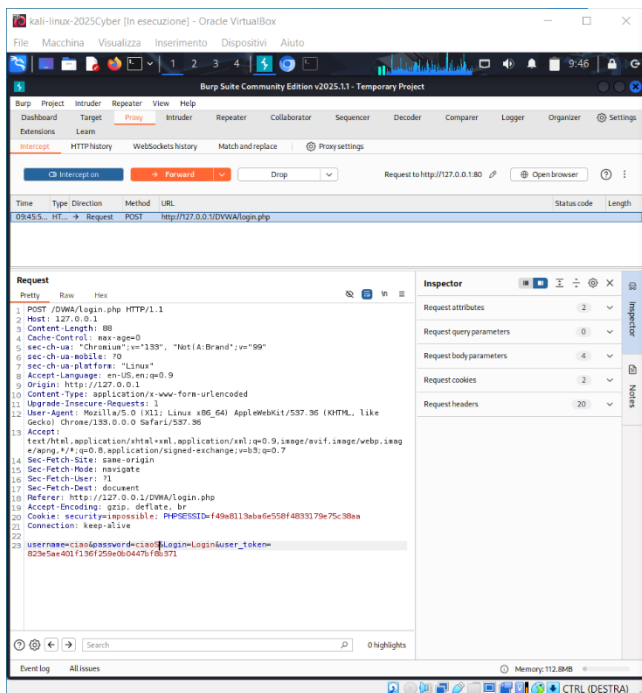
Una volta entrati nell'app, cliccate sulla scheda DVWA Security. Qui possiamo scegliere il livello di sicurezza dell'APP. Più basso sarà il livello di sicurezza impostato, meno sarà complicato sfruttare le vulnerabilità.

La colonna a sinistra, invece, lista tutte le vulnerabilità presenti.

Catturo il traffico con BurpSuite



Modifica dei campi.



Modificando le credenziali l'app non permette di entrare.

