

Settimana 3 Esercizio 3

Esercizio Web Application

Le WEB APPLICATION sono vere e proprie applicazioni che operano a livello di Web Server e, nella maggior parte dei casi girano per mezzo di web browser.

Nell'esercizio andremo ad installare la web application DVWA tramite terminale con utenza 'root' su kali andando ad inserire i comandi in figura per poter andare a modificare username e password così da renderlo più semplice (tramite comando 'nano config.inc.php'.

```
root@Andrea: /var/www/html/DVWA/config
File Actions Edit View Help
cd: no such file or directory: var/www/html

(root@Andrea) ~
# cd /var/www/html

(root@Andrea) ~ (/var/www/html)
# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 4414, done.
remote: Counting objects: 100% (189/189), done.
remote: Compressing objects: 100% (135/135), done.
remote: Total 4414 (delta 86), reused 122 (delta 51), pack-reused 4225
Receiving objects: 100% (4414/4414), 2.16 MiB | 3.88 MiB/s, done.
Resolving deltas: 100% (2097/2097), done.

(root@Andrea) ~ (/var/www/html)
# chmod -R 777 DVWA/

(root@Andrea) ~ (/var/www/html)
# cd DVWA/config

(root@Andrea) ~ (/var/www/html/DVWA/config)
# cp config.inc.php.dist config.inc.php

(root@Andrea) ~ (/var/www/html/DVWA/config)
# nano config.inc.php

(root@Andrea) ~ (/var/www/html/DVWA/config)
# service mysql start
```

A questo punto andiamo ad eseguire il servizio MYSQL per la gestione dei database tramite il comando 'service mysql start' per poi connetterci al database con 'mysql -u root -p' e la password che abbiamo cambiato in precedenza. Creiamo quindi un'utenza e i privilegi dell'utente:

```
(root@Andrea) ~ (/var/www/html/DVWA/config)
# service mysql start

(root@Andrea) ~ (/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 (1.698 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.006 sec)

MariaDB [(none)]> exit
Bye

(root@Andrea) ~ (/var/www/html/DVWA/config)
#
```

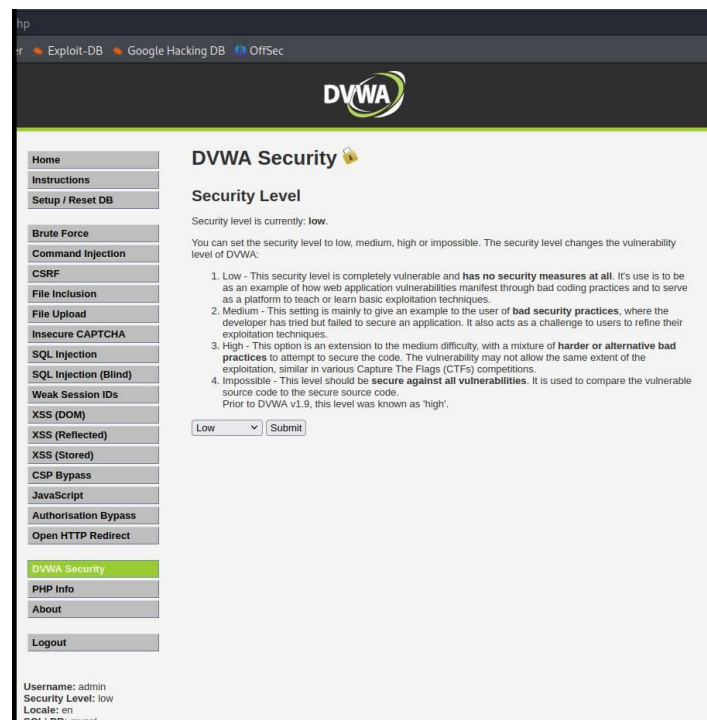
Una volta configurato passiamo al servizio 'Apache', un servizio open-source utilizzato come web server. Un po' come con MYSQL, andiamo a configurare il servizio attraverso il comando 'nano php.ini' per attivare la voce 'allow_url_include' su on. A questo punto se inseriamo l'indirizzo '127.0.0.1/DVWA/setup.php' potremo entrare, tramite user e password di default (admin, password), all'interno della famosa Web Application DVWA con la quale possiamo cambiare il livello di sicurezza per poter fare pratica su diversi gradi di vulnerabilità.

```
(root@Andrea) ~ (/var/www/html/DVWA/config)
# service apache2 start

(root@Andrea) ~ (/var/www/html/DVWA/config)
# cd /etc/php/8.2/apache2

(root@Andrea) ~ (/etc/php/8.2/apache2)
# nano php.ini

(root@Andrea) ~ (/etc/php/8.2/apache2)
# service apache2 start
```



A questo punto utilizzeremo il tool BurpSuite per andare ad intercettare le richieste e i dati che si scambiano i due siti: l'indirizzo di DVWA è in http, quindi i dati saranno in chiaro e potremo vedere username e password digitati dall'utente in fase di login.

In questo modo diventa molto semplice andare ad impossessarsi di dati sensibili quali credenziali, carte di credito, indirizzi etc..

Da qui, una volta intercettato il nostro indirizzo nella sezione proxy, possiamo andare ad ottenere in chiaro i dati sensibili e a modificare manualmente il valore dell'username (admin) e della password (password).

