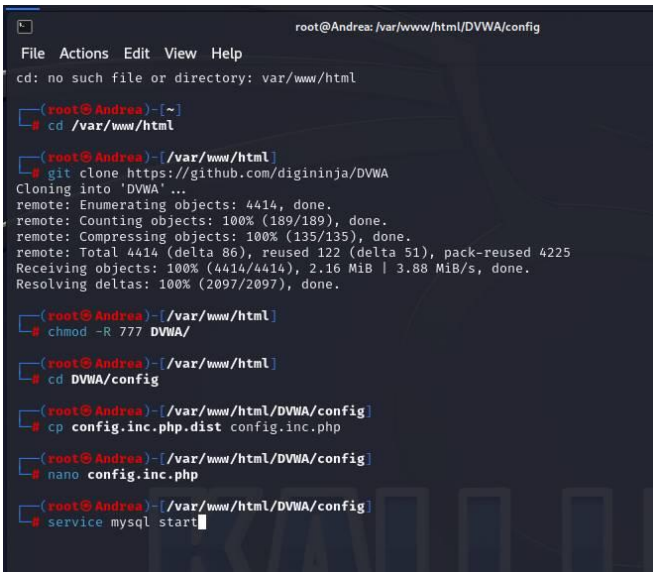
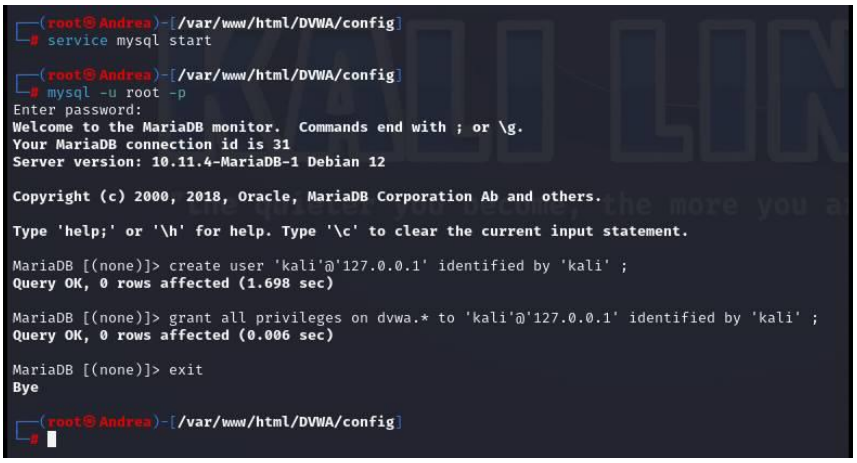
# Settimana 3 Esercizio 3

## Esercizio Web Application

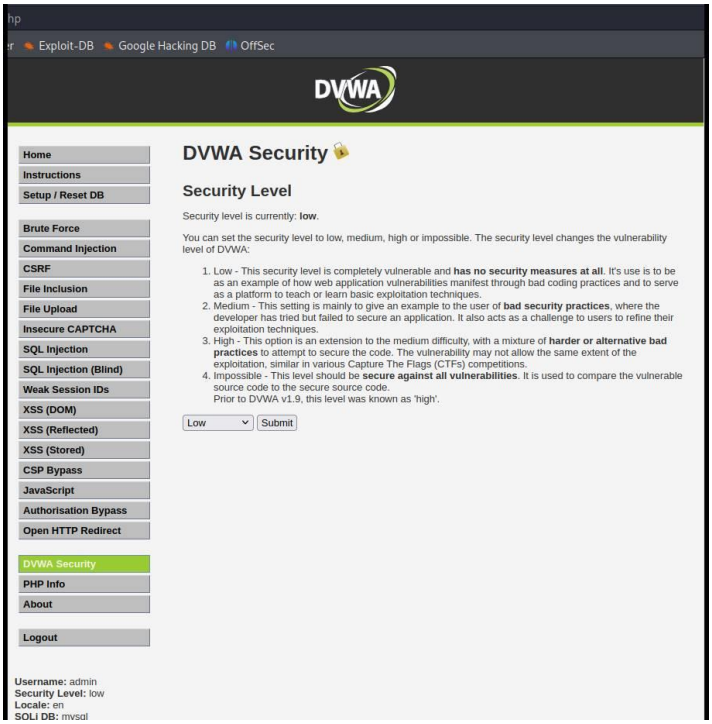
Le WEB APPLICATION sono vere e proprie applicazioni che operano a livello di Web Server e, nella maggior parte dei casi girano per mezzo di web browser.
Nell'esercizio andremo ad installare la web application DVWA tramite terminale con utenza *'root'* su kali andando ad inserire i comandi in figura per poter andare a modificare username e password così da renderlo più semplice (tramite comando ***'nano** config.inc.php'* .




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:




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.




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).