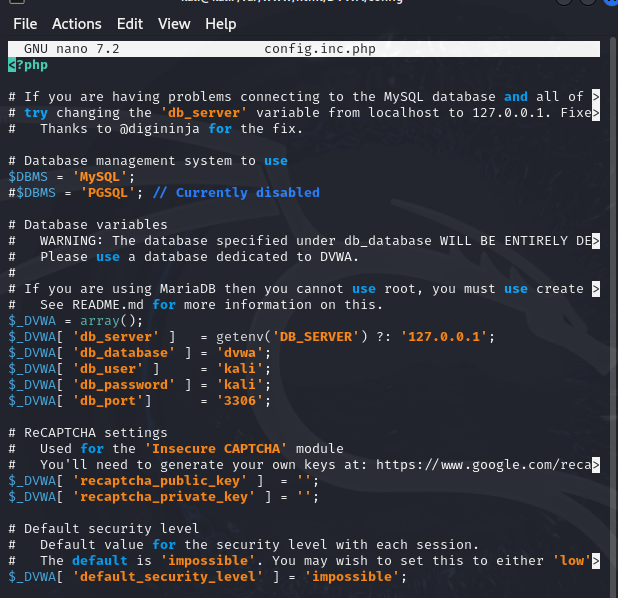
ESERCIZIO S3L2

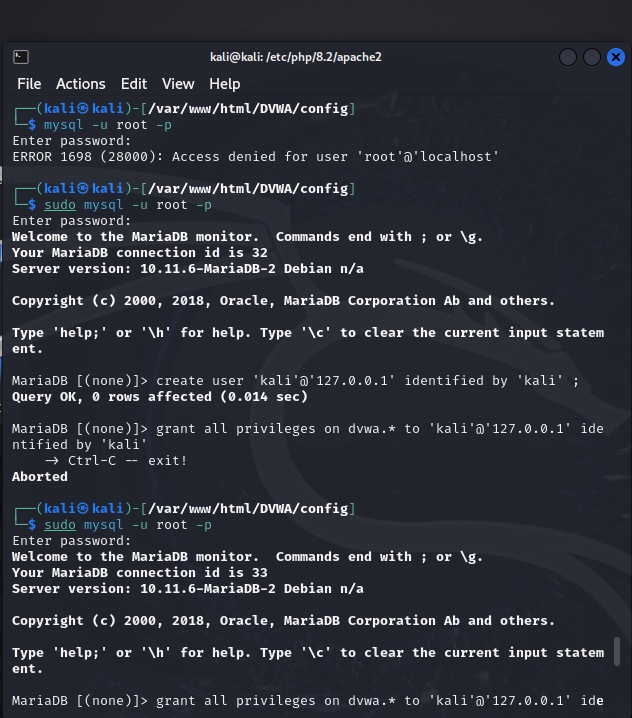
Nell’esercizio di oggi si vedrà come configurare una DVWA (damn vulnerable web application).

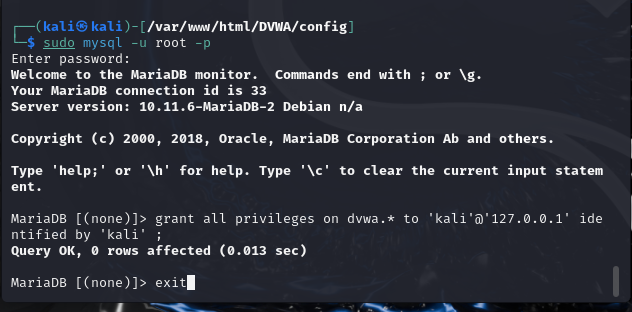
Inizialmente si è installato la web application DVWA, un progetto software che include intenzionalmente vulnerabilità di sicurezza, esso ci servirà per proseguire con l’esercizio richiesto. Successivamente si è cambiato nome utente e password nel file “config.inc.php” entrando con il comando ”sudo nano config.inc.php” ed inserendo per entrambi ‘kali’



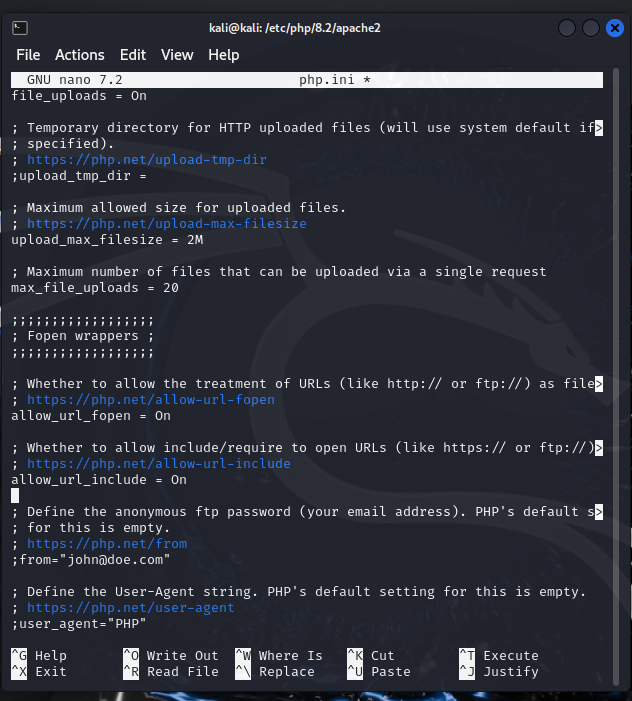
Dopo aver configurato le nostre credenziali abbiamo avviato il servizio web **Apache2** e il servizio database **mysql**, utilizzando i permessi di amministratore tramite il comando ‘sudo’.

**mysql** si è avviato tramite il database MariaDB ed abbiamo creato un’utenza (kali) assegnandogli i privilegi da amministratore:



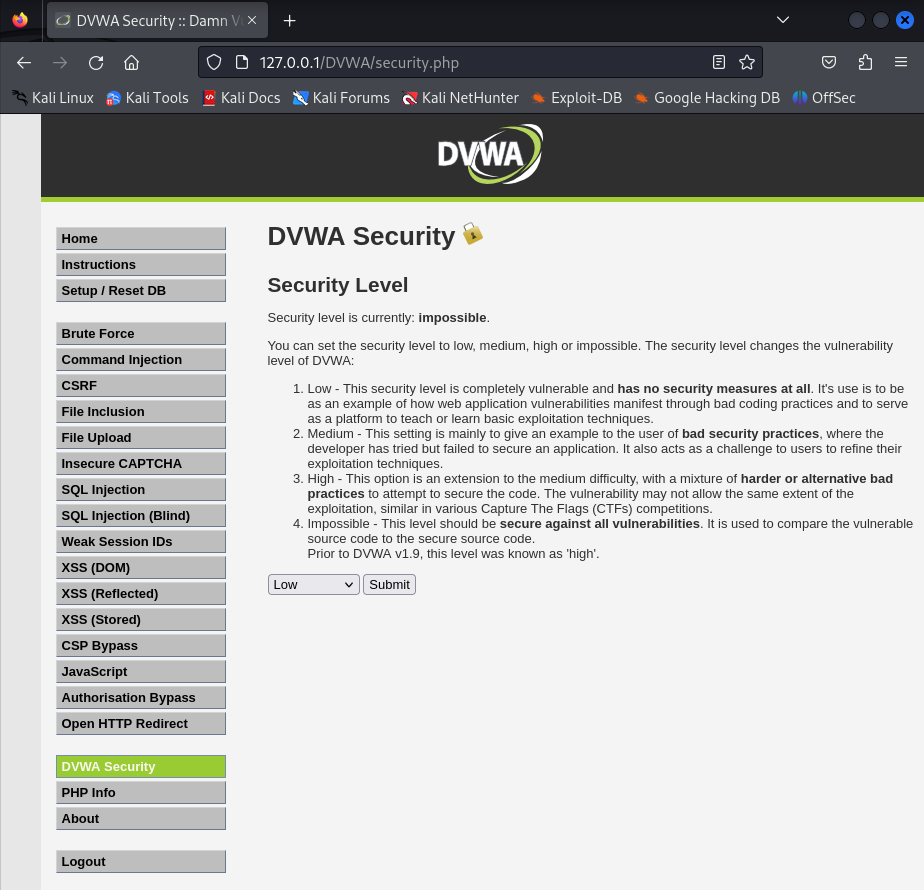


Si è effettuata anche la configurazione per il servizio web **apache2**, in particolare si è modificato il file ‘php.ini’ per consentire la richiesta di aprire gli URLs.

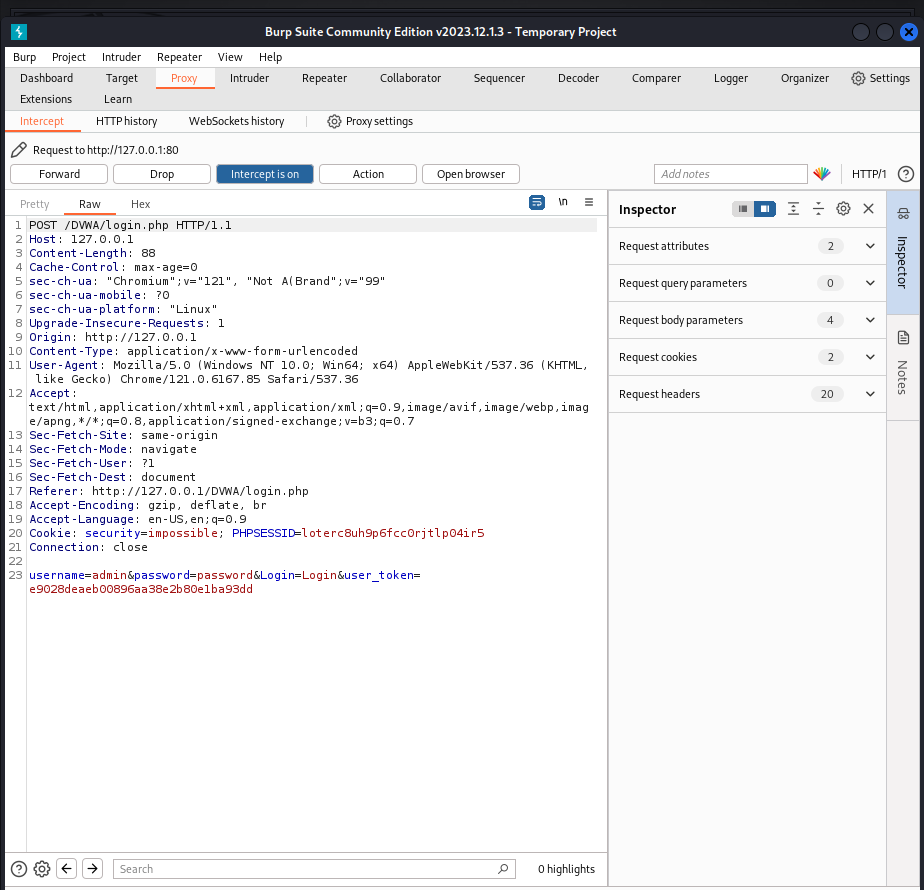


Successivamente si è creato un database su DVWA, si è effettuato l’accesso con username(**admin**) e password(**password**) e si è scelto il livello di sicurezza della web app settandolo al minimo (Low).

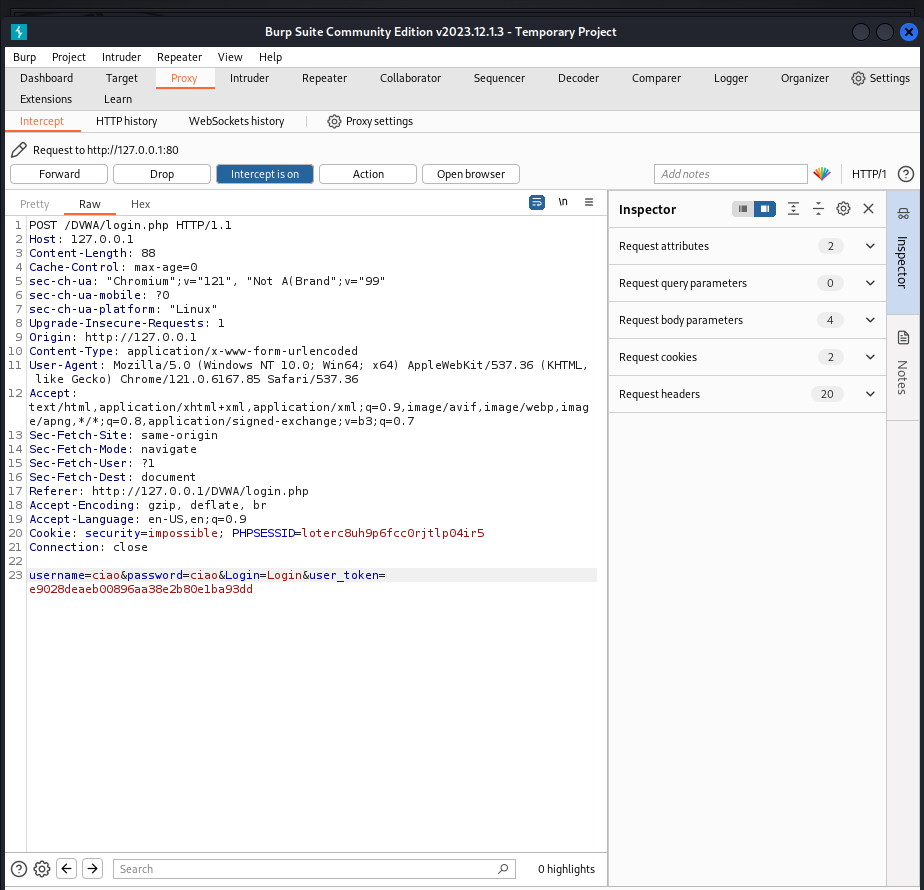
Più basso sarà il livello di sicurezza impostato, meno sarà complicato sfruttare le vulnerabilità.



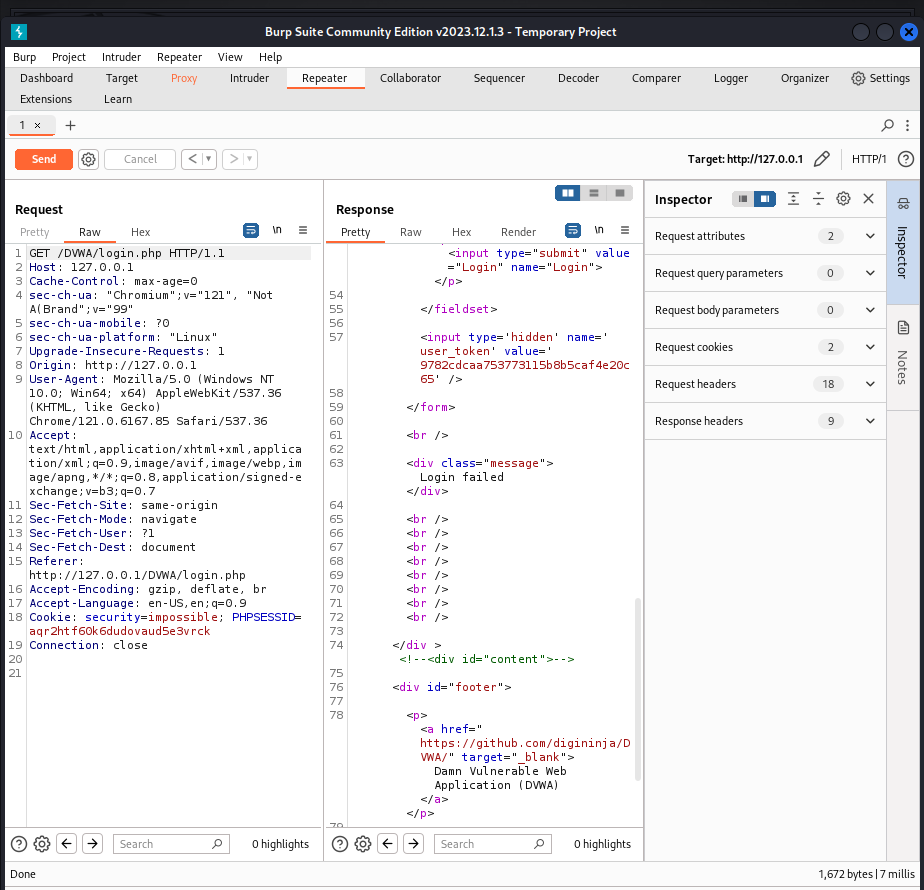
A questo punto si è fatto uso dell’applicazione **Burp Suite**, e si è scelto un progetto temporaneo. Attivando l’intercettazione della richiesta di login su Burp, si è poi effettuato l’accesso tramite browser all’indirizzo ‘127.0.0.1/DVWA’. Così facendo si è provato ad intercettare la nostra stessa richiesta di login fatta tramite browser.



Per verificarlo sono state cambiate username e password iniziali con delle credenziali sbagliate, proprio per verificare che fallisse il login.



Come ci si aspettava, con le credenziali errate non si è riuscito ad effettuare il login. Se ne ha evidenza nel body della http response dove si legge «Login failed» a riga 63.

  
  
  
Team 4  
Roberta - Andrea (db)- Mario (rt) – Antonio – Giammarco