REPORT 09-11-2022

FACCILONGO DOMENICO

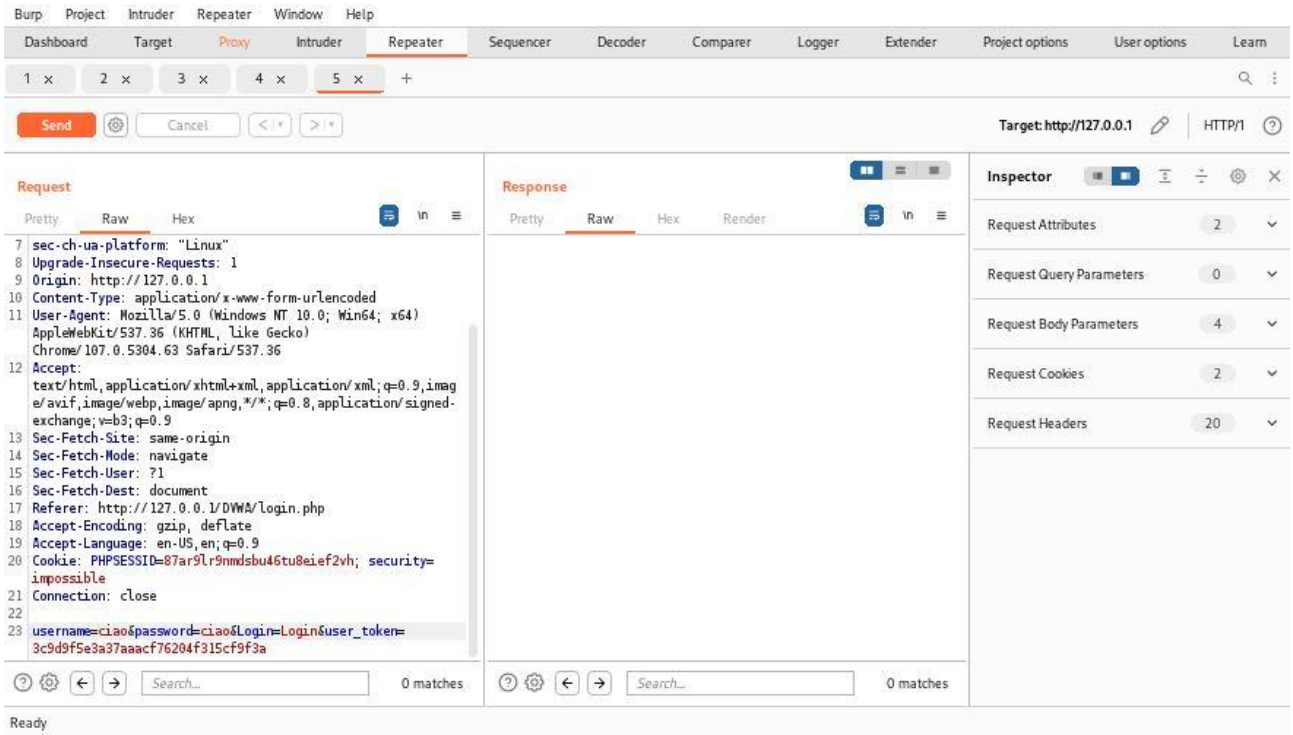
WEB APPLICATION – PREPARAZIONE AMBIENTE

TASK:

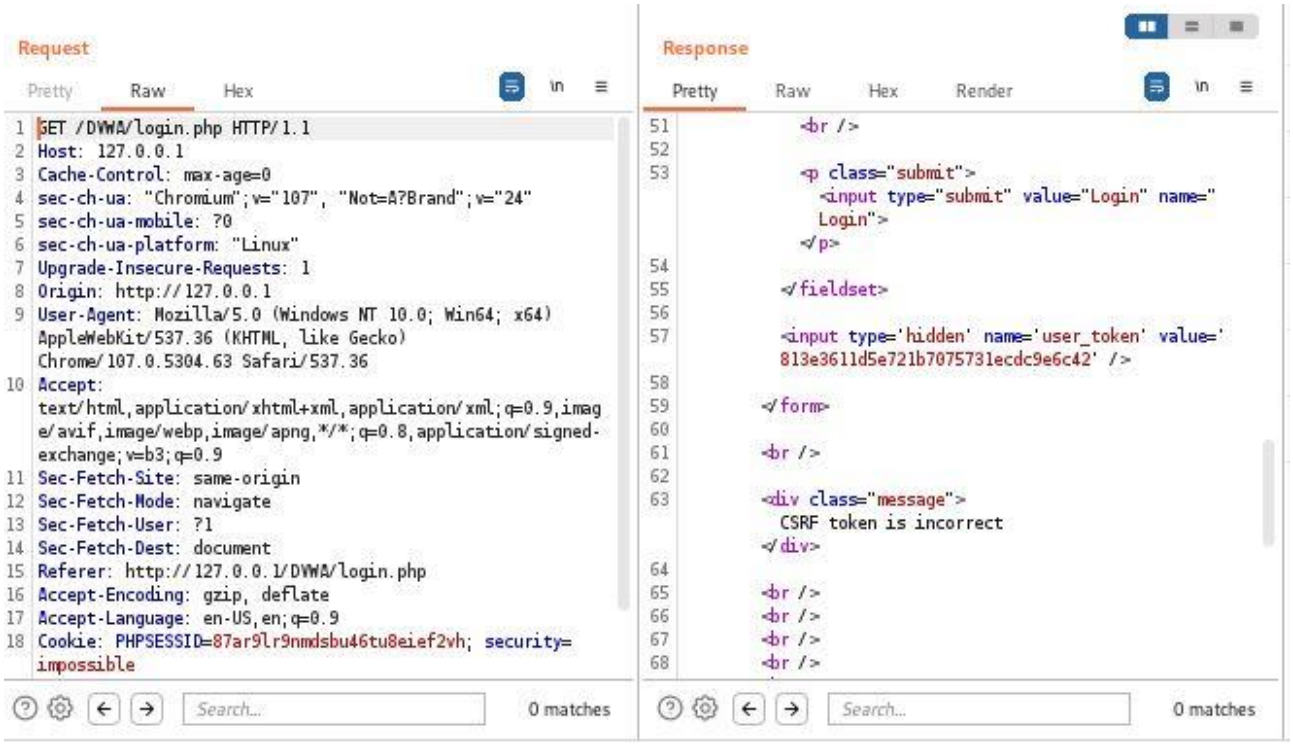
- Attraverso l'ausilio di Burpsuite andare a verificare nella fase di login le credenziali inserite. Provare a cambiare le credenziali ed analizzare la risposta.

ANALISI E VALUTAZIONI:

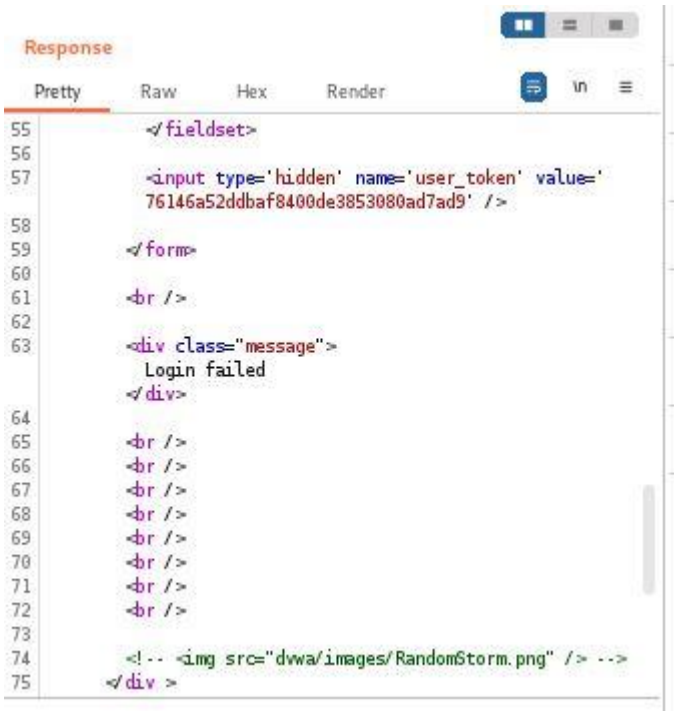
Dopo aver configurato e successivamente avviato il servizio di mysql e apache2 andiamo nella pagina del browser di firefox con url 127.0.0.1/DVWA/setup.php e dopo aver eseguito i passaggi fino ad arrivare al login basterà inserire le credenziali. Quest'ultimo passaggio però lo eseguiamo all'interno di Burpsuite in modo tale da captare le credenziali inserite. Di fatti nel momento di login intercettiamo la richiesta da parte del server di tipo POST da cui ritroviamo proprio le credenziali inserite:



Nella figura in alto abbiamo già modificato le credenziali scrivendone delle nuove, sta di fatto che procedendo di fatti con l'invio del pacchetto POST ma con credenziali "sbagliate" la risposta sarà del tipo "CSRF token is incorrect".



Avremo potuto modificare la sicurezza e impostare da ”impossible” a “possible” per testare effetivamente se avrebbe potuto farci entrare ma con credenziali differenti modificate direttamente dal pacchetto POST di burpsuite.



Come ultimo test abbiamo sbagliato di proposito il login direttamente dal browser notando effettivamente dal pacchetto risposta del Server che il “Login failed”.