Burp Suite è una piattaforma di testing di sicurezza web che aiuta a identificare vulnerabilità nelle applicazioni web. Include strumenti come scanner, proxy, e analizzatori per eseguire attacchi di tipo man-in-the-middle e altre tecniche di penetration testing.

Tramite l'esercitazione di oggi, abbiamo configurato un database MySQL che è un servizio di gestione di database open-source e Web Server Apache, che è un server web open-source che gestisce le richieste HTTP. Generalmente viene utilizzato per ospitare siti e applicazioni web.

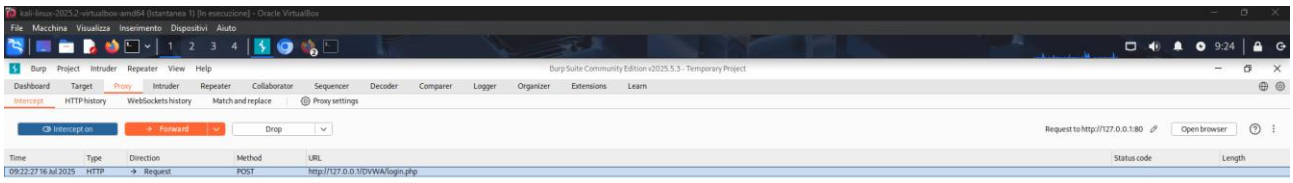
Una volta fatto queste configurazioni, abbiamo aperto un progetto temporaneo su Burp suite;

Burp Suite è una piattaforma di testing di sicurezza web che aiuta a identificare vulnerabilità nelle applicazioni web. Include strumenti come scanner, proxy, e analizzatori per eseguire attacchi di tipo man-in-the-middle e altre tecniche di penetration testing. Tramite il browser che offre Burp Suite (Chromium), abbiamo scelto come target del test il login di DVWA* (127.0.0.1/DVWA con l'obiettivo di imparare a modificare i parametri di login.

**DVWA: (Damn Vulnerable Web Application) è un'applicazione web volutamente vulnerabile, progettata per essere utilizzata da professionisti della sicurezza informatica e studenti per esercitarsi nell'identificazione e sfruttamento di vulnerabilità comuni nelle applicazioni web.*

Una volta aperto il browser e arrivati alla schermata login di DVWA, abbiamo attivato la funzione "Interception on" su Burp, questo ci permette, appunto, di intercettare tutte le richieste che manda il browser, esaminarle e/o modificarne i parametri.

In questa immagine possiamo notare la richiesta di login che abbiamo simulato su DVWA con i parametri corretti.



Una volta ottenuta la richiesta da parte del browser per il login, tramite la tab “Request” possiamo mandare la richiesta al “Repeater”.

Nel Repeater, possiamo modificare qualsiasi parte della richiesta HTTP, come parametri, header o corpo della richiesta, per analizzare come il server risponde a diverse varianti.

Questo strumento è utile per testare vulnerabilità, la manipolazione dei parametri o altre tecniche di attacco.

A ogni invio, possiamo visualizzare la risposta del server nella sezione di destra, che ci fornirà feedback sulla validità delle modifiche apportate, permettendoci di affinare i nostri test e identificare potenziali vulnerabilità.