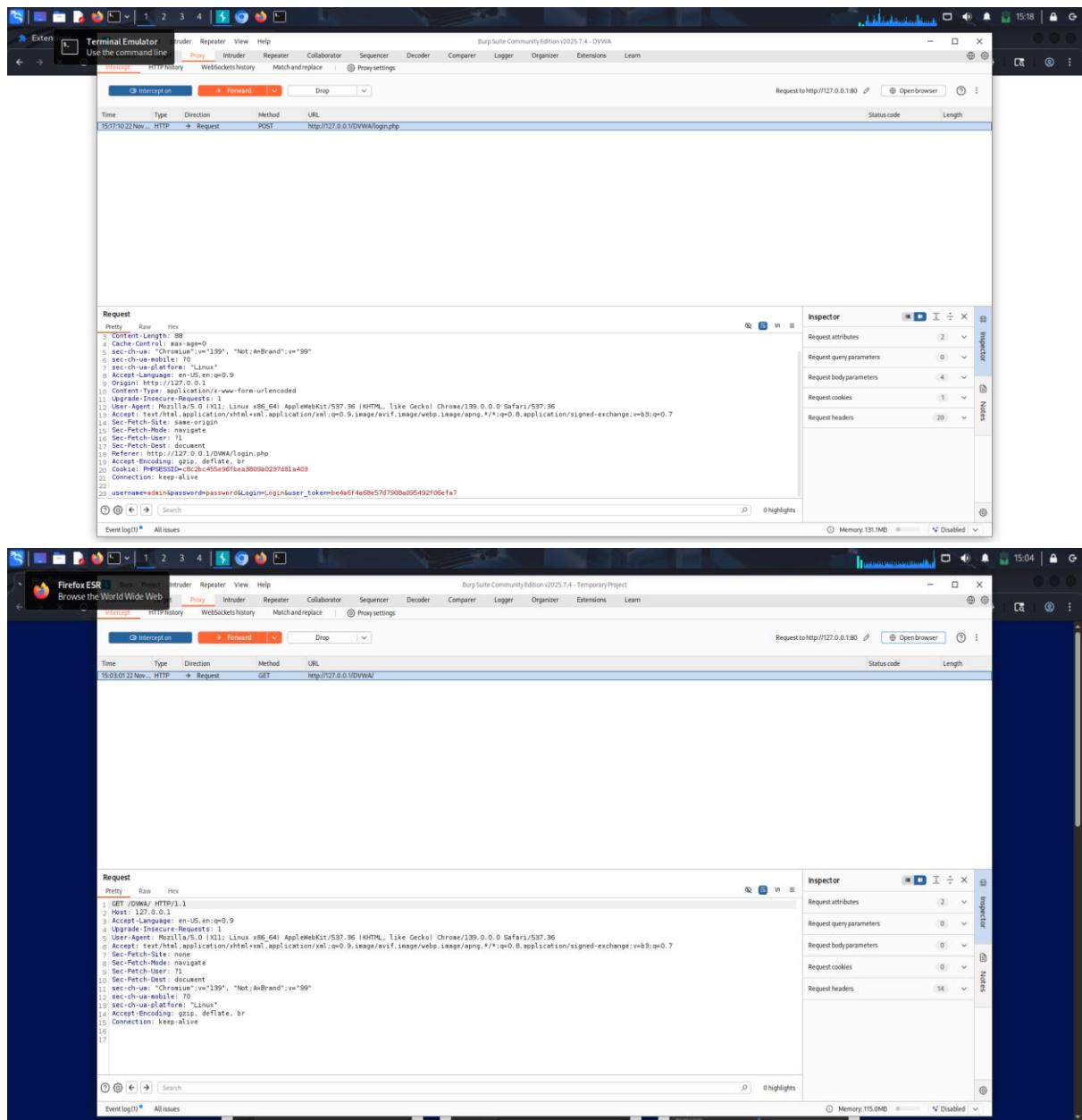


W8D1\_esercizio DVWA e Burpsuite

Tramite l'utilizzo dello strumento Burp suite è stata intercettata una richiesta di accesso sulla DVWA come si vede chiaramente in figura, in cui si riporta come è facilmente individuabile sia il nome utente che la password di accesso al servizio.



The screenshot shows the DVWA Security page. On the left, there's a sidebar with various attack types like Brute Force, Command Injection, and SQL Injection. The main content area has a heading 'DVWA Security' with a yellow exclamation mark icon. Below it is a section titled 'Security Level' with the current setting 'low'. A detailed description follows, mentioning four levels: Low (completely vulnerable), Medium (bad security practices), High (medium difficulty), and Impossible (secure against all vulnerabilities). A dropdown menu allows changing the security level from 'Low' to 'High'. Below this is a section for 'Additional Tools' with a link to 'View Broken Access Control Logs'.

Tramite lo strumento intruder si possono modificare i parametri ad esempio quelli di accesso e password inviando altre richieste al serever.

The screenshot shows the Burp Suite interface. In the 'Intruder' tab, a 'Sniper attack' is being run against the URL <http://127.0.0.1>. The payload configuration panel on the right shows a 'Simple list' of payloads with count 0. The 'Payload processing' panel below it contains rules for enabling and disabling payloads. The bottom status bar indicates 1/1 match, 1 payload position, and length 941.

Si vedranno successivamente in maniera più approfondita le varie attività e funzioni del servizio Burp suite