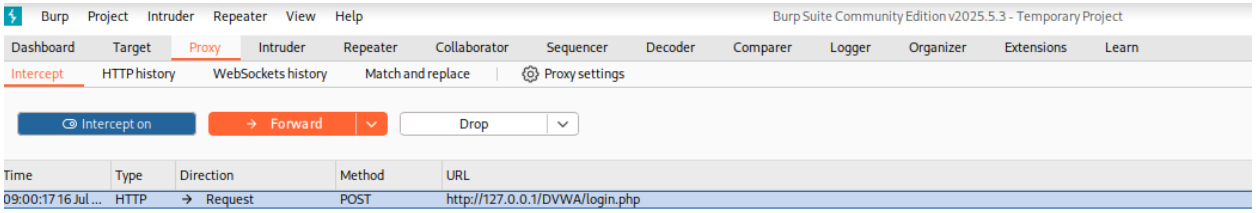
ESERCIZIO S3 L3

Per questo esercizio ho utilizzato **Burp Suite** per intercettare e modificare i parametri di login della **DVWA.**

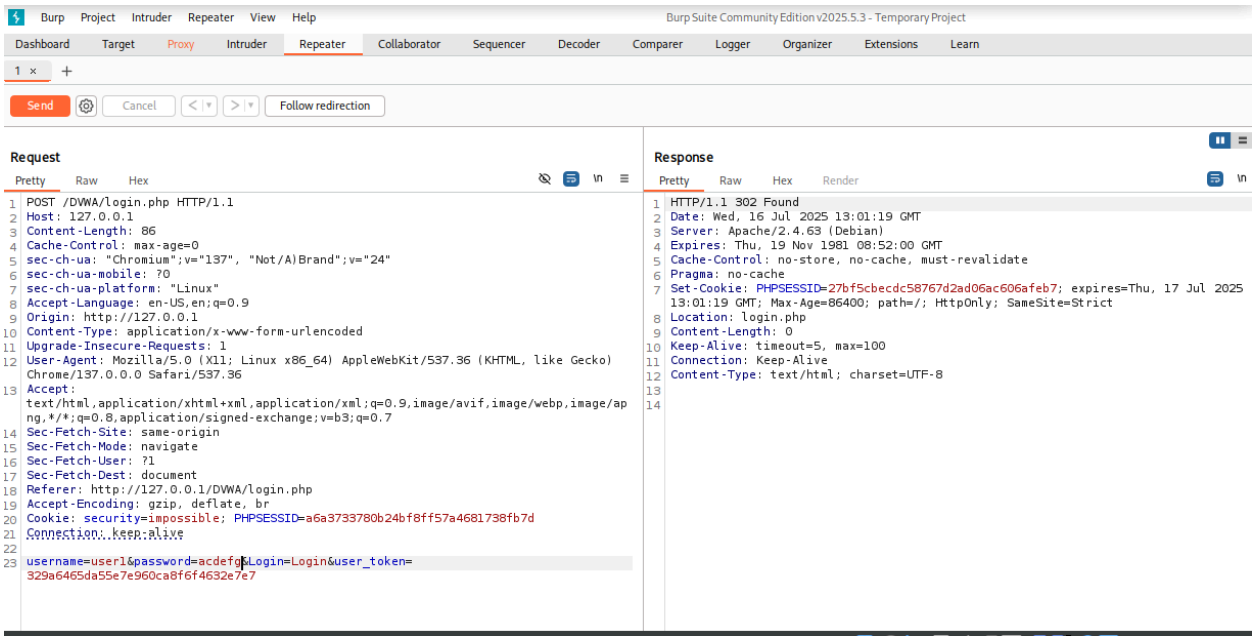
DVWA : Web App che contiene delle vulnerabilità per poterle testare.

Ho configurato **Burp Suite** con intercettazione attiva (**Interception on**) e navigato verso la pagina di login inserendo le credenziali standard admin/password.



Cosa faccio:

1. Vado su 127.0.0.1/DVWA nel browser
2. Inserisco admin e password nei campi login
3. Clicco Login → Burp intercetta la richiesta
4. Tasto destro → "Send to Repeater"
5. Nel Repeater modifico i parametri



Come da immagine ho inserito nella sezione **"Repeater"** parametri differenti:

Da **username=admin & password=password**
A **username=user1 & password=abcdefg**

Clicco su "Send" per poi leggere la risposta del server.

RISULTATO: Credenziali errate = accesso negato

CONCLUSIONI

Trovo molto interessante Burp Suite e le funzionalità viste e mi piacerebbe approfondire l'argomento. Con questa esercitazione ho compreso le seguenti funzionalità di Burp Suite:

Interception on : per iniziare ad intercettare
Proxy: per intercettare le richieste HTTP
Repeater: per modificare, inviare richieste multiple e testare
Send to Repeater: per trasferire richieste