

# W8D2

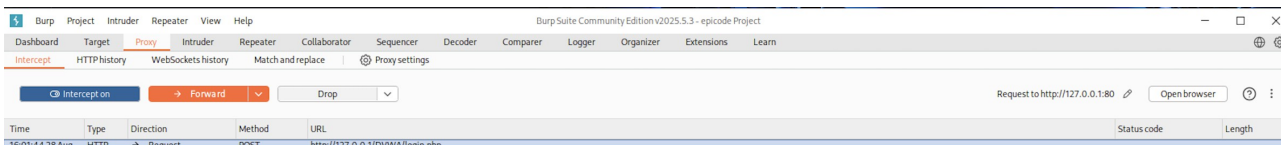
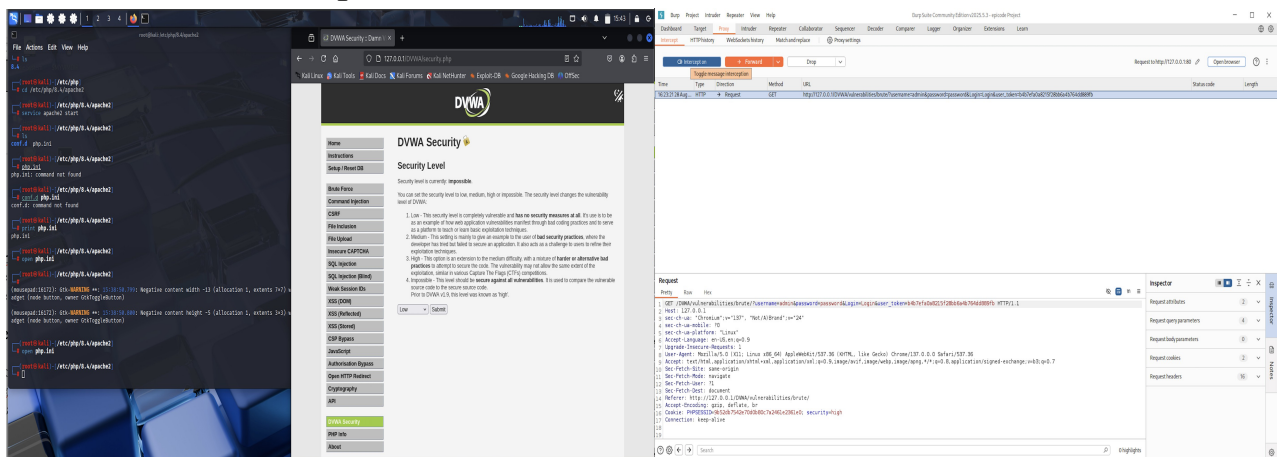
## DVWA e Burp Suite + Facoltativo

DVWA -Damn vulnerable web application e' un applicazione web volutamente vulnerabile usata per fare pratica con la sicurezza informatica.

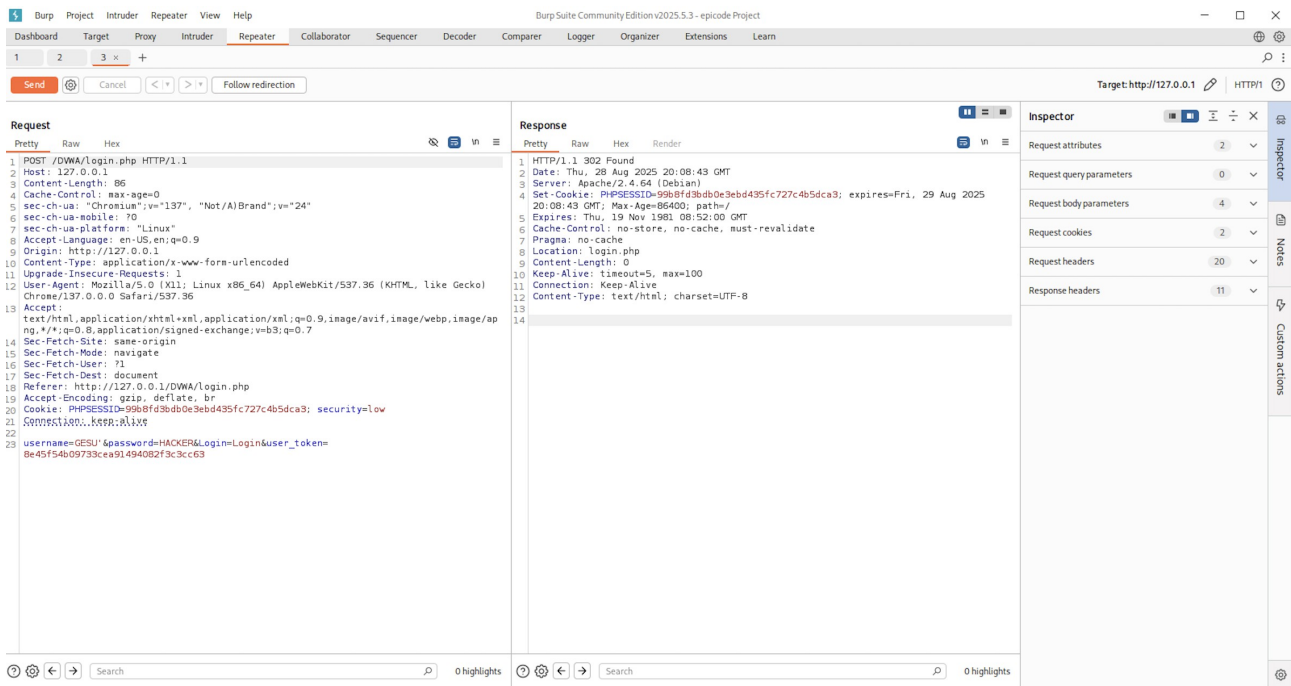
L'esercizio come primo step ci richiede l'installazione e configurazione di DVWA tramite Kali linux.

Per l'installazione e la configurazione e' stata utilizzata la guida consegnata da EPICODE.

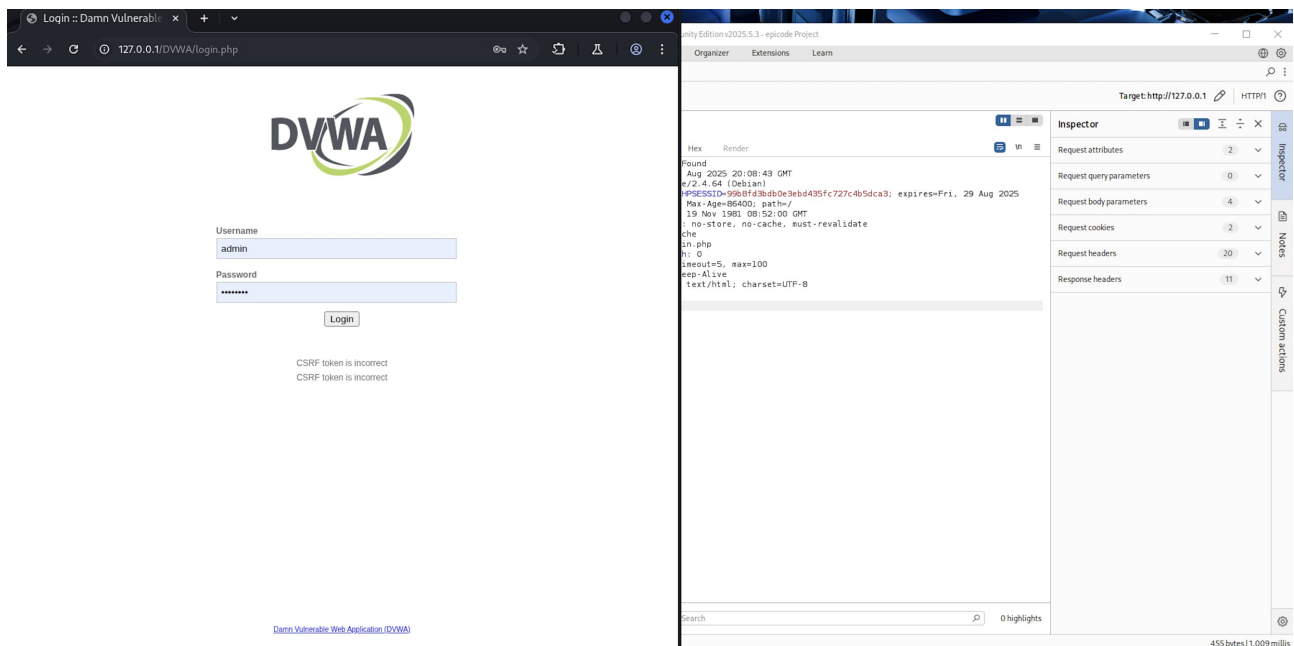
La possibilita' di utilizzare METASPLOITABLE per utilizzare la DVWA l'ho esclusa a priori perche' saltava dei passaggi importanti , come l'installazione tramite terminale e la sua configurazione , che alla fine fanno sempre parte della pratica e assimilazione delle nozioni.



L'installazione e' stata eseguita correttamente sia di DVWA che di Burp Suite tramite il browser integrato in Burp suite mi sono collegato all'indirizzo ip 127.0.0.1/DVWA e impostato LOW come livello di sicurezza. L'esercizio ci chiede di cambiare la user e la password nella pagine di Burp suite.



Cambiando user e password logicamente il login fallisce. Quando si cambiano dei dati bisogna mandare la modifica al repeater. Per far si che le pagine vengano caricate bisogna sempre intervenire sul Forward.



Cambiando il livello di sicurezza della DVWA si notano alcuni cambiamenti nel comportamento dell'applicazione.

Per esempio nel livello basso di sicurezza non esiste nessuna protezione CSRF

Cosa che cambia appena iniziamo a mettere livelli superiori.

Sara' molto interessante vedere come si comporteranno sia Burp Suite sia DVWA con dei veri attacchi , Brute force ,SQL O XSS

The screenshot displays the Burp Suite Community Edition v2025.5.3 interface. The top menu bar includes options like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the menu is a toolbar with buttons for Intercept on, Forward, and Drop. The main panel shows a list of intercepted requests. The selected request is an HTTP POST to http://127.0.0.1/DVWA/security.php, timestamped 16:18:07 28 Aug. The request details are shown in the 'Request' tab, and the 'Inspector' tab on the right provides a structured view of the request's components.

**Request**

```
5 sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DVWA/security.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=9652db7542e70d0b80c7a2461e2961e0; security=medium
21 Connection: keep-alive
22
23 security=medium&seclev_submit=Submit&user_token=d6d718a0a9a86762ea5f2a0f66500d28
```

**Inspector**

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 3
- Request cookies: 2
- Request headers: 20