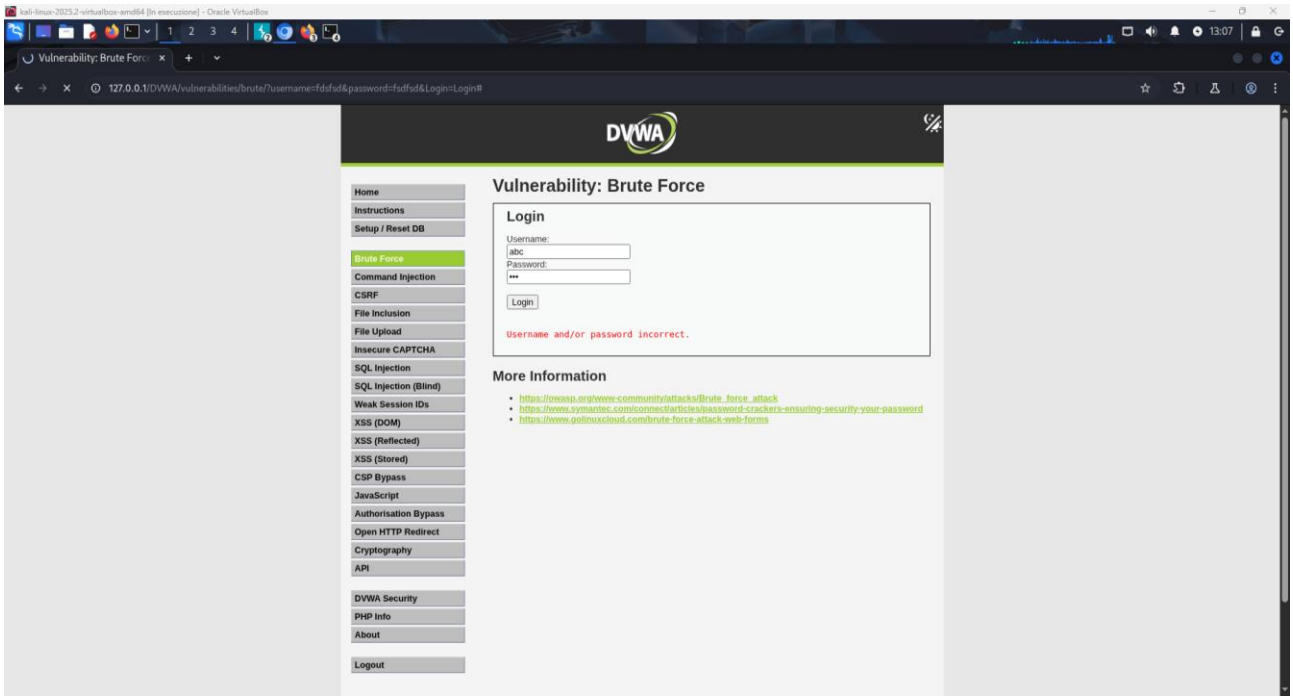
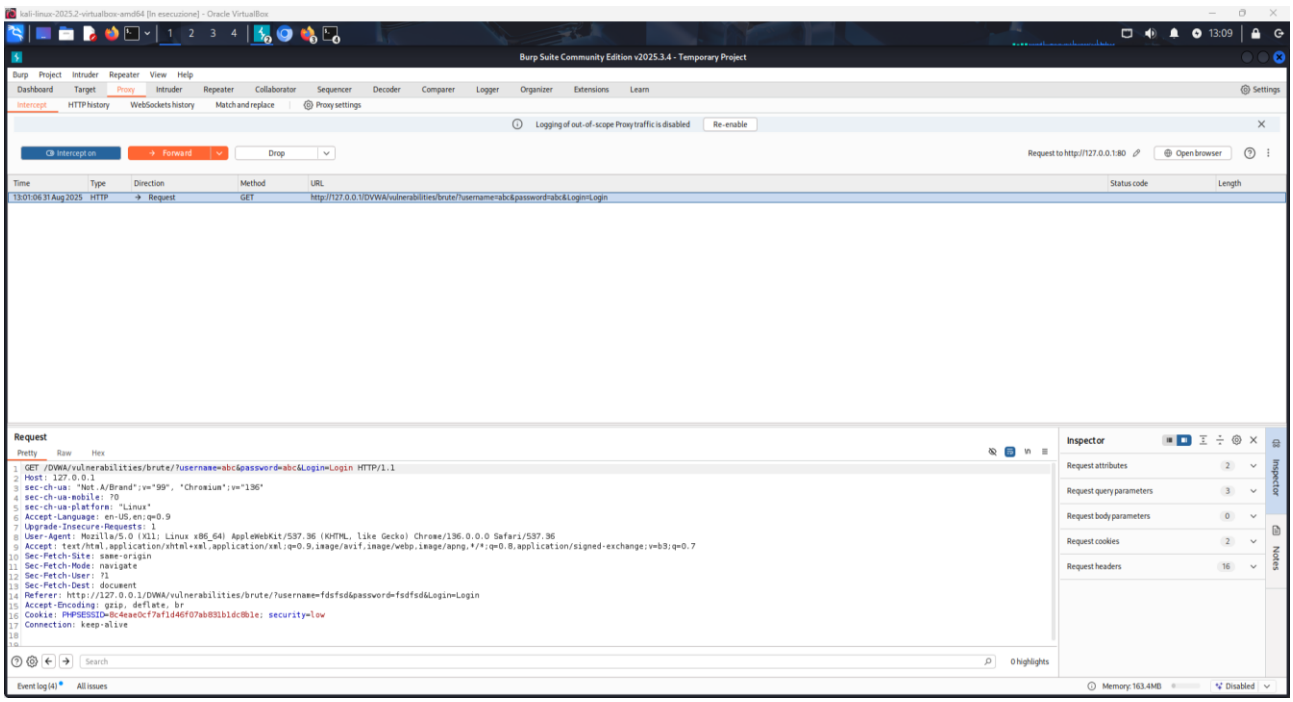
Ciao Valerio, non so se questo esercizio vada bene perché non ho capito molto bene il metodo di consegna, comunque per farti capire che ho capito farò questo che spero vada bene:

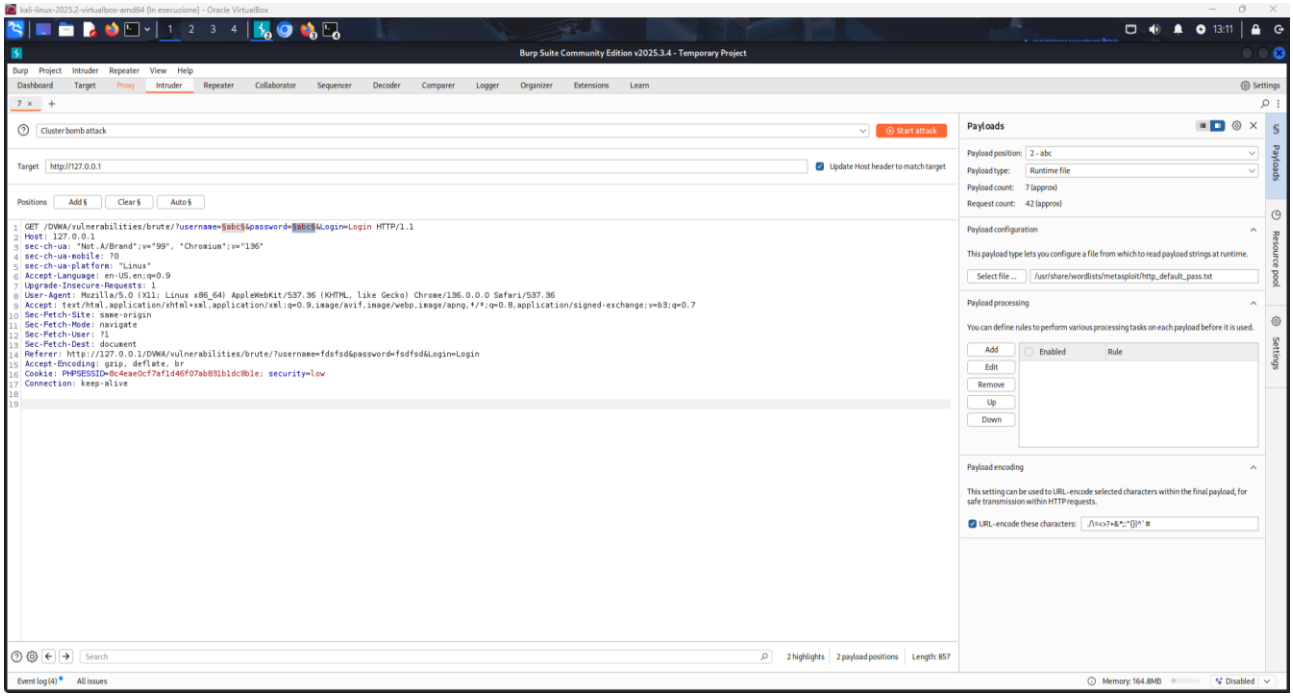


Sbagliamo appositamente la password perché noi non la “sappiamo” quindi simuliamo questa cosa qui.



Ovviamente prima di sbagliare la password apriamo il nostro burp suite e lo mettiamo in ascolto (o intercettazione)

Sbagliando la password ci apparirà questo risultato e cliccandoci sopra vediamo la username e la password che abbiamo usato noi.

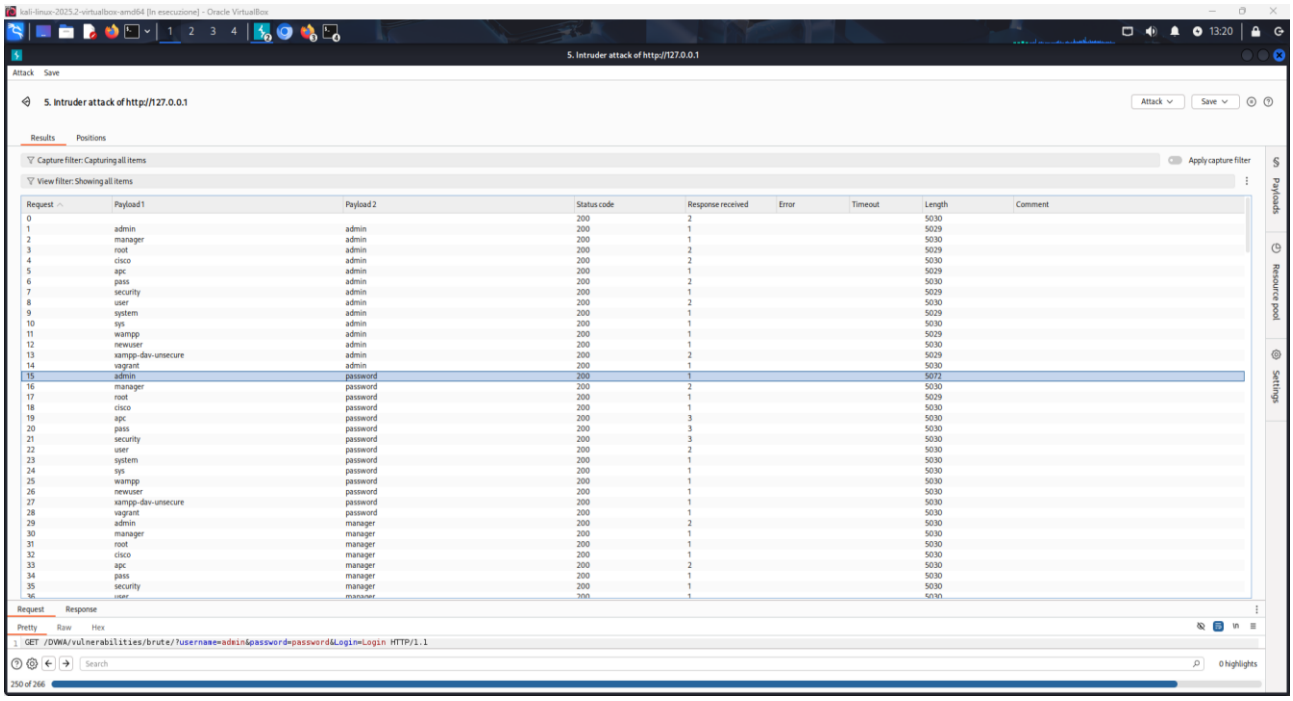


Tasto destro e mandiamo tutto all'intruder. Cambiamo il parametro "Sniper Attack" con il parametro "Cluster Bomb Attack" in quanto lo Sniper riesce a sostituire un payload alla volta (quindi o username o password) mentre il cluster bomb può fare due cose contemporaneamente.

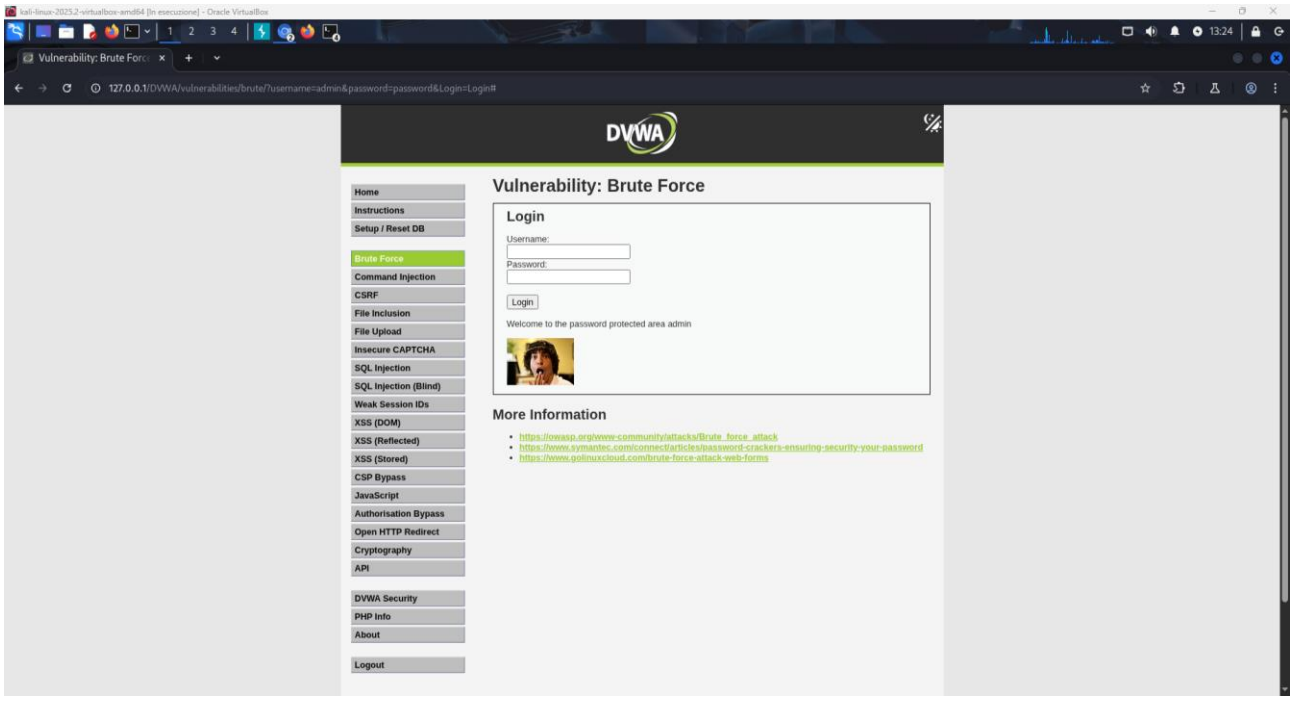
Diamo la posizione dei payload che in questo caso saranno l'username e la password sbagliate.

A destra configuriamo il tutto mettendo:

in payload position la posizione 1 ovvero la prima posizione che abbiamo evidenziato; poi configuriamo il payload type mettendolo su Runtime file; andiamoci a selezionare i file già preimpostati nel sistema che troviamo in /usr/share/wordlist/metasploit/http_default_users.txt e così completiamo il primo payload. Il secondo payload avrà gli stessi passaggi del primo solo cambiamo il file che da quello precedente passa a /usr/share/wordlist/metasploit/http_default_pass.txt



Iniziamo l’attacco e al suo termine vediamo che in lenght solo un numero è diverso da tutti gli altri. (Quello evidenziato)



In conclusione mettiamo l’username e la password (admin e password) che ci ha fornito Burp e siamo dentro!