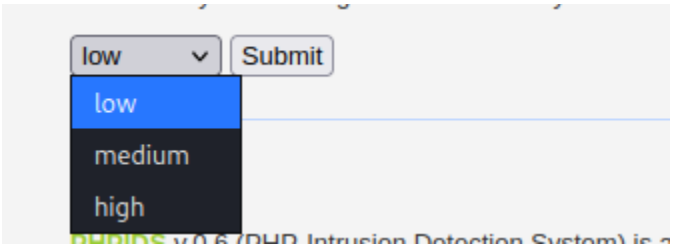
REPORT PROGETTO 02/12/2022

FRANCESCO PERSICHETTI

L’esercitazione di oggi consiste nell’exploitare le vulnerabilità di

1. SQL injection (blind), recuperando le password degli utenti presenti nel DB
2. XSS stored, andando a recuperare i cookie di sessione della vittima per inviarli alla macchina dell’attaccante

Per iniziare l’esercizio bisogna come prima cosa configurare il livello di sicurezza della DVWA su low

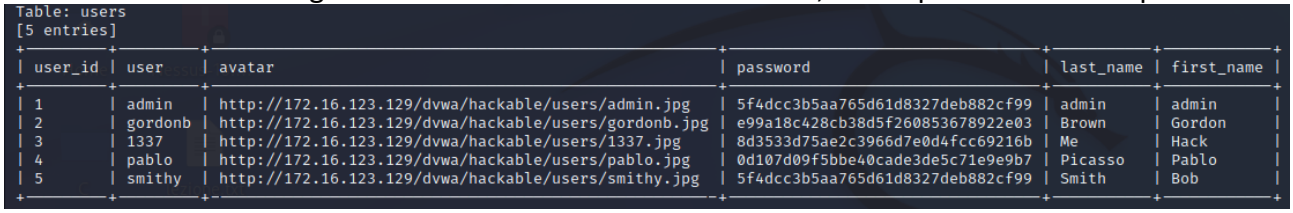


1.

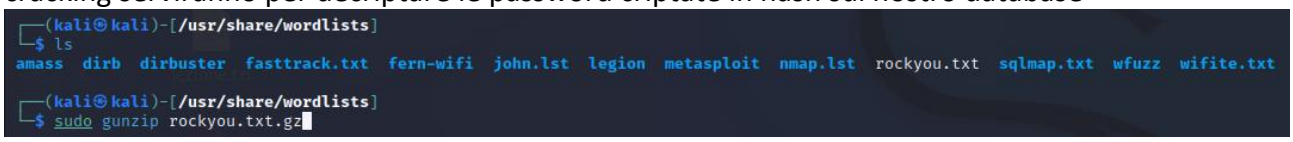
Per trovare le password degli utenti vado nella sezione “SQL injection blind” per scrivere nel form la query con cui farmi ridare le informazioni cercate

Oppure dal prompt dei comandi con il tool SQLmap con il comando seguente

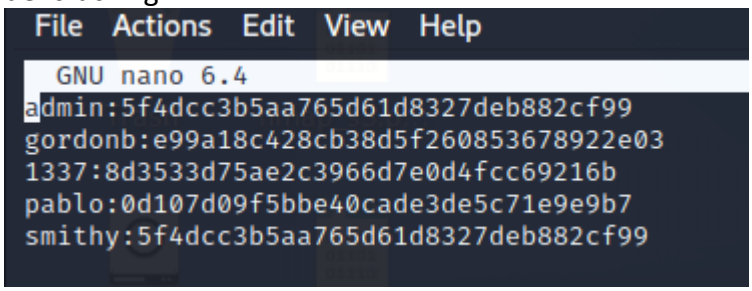
E come risultato mi vengono restituite le colonne del database, tra le quali username e password



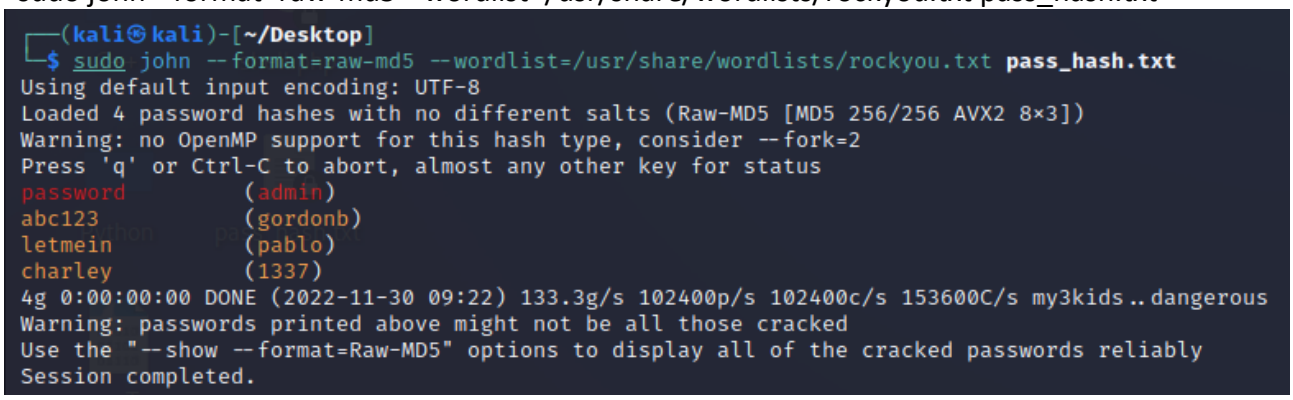
Per iniziare ho estratto il file “rockyou.txt” contente una “common password list”. Questo file si trova all’interno della wordlists di kali e con il comando “sudo gunzip rockyou.txt.gz” vado ad estrarre il contenuto. Al suo interno ci sono una lista di password che con l’aiuto del tool di cracking serviranno per decriptare le password criptate in hash sul nostro database



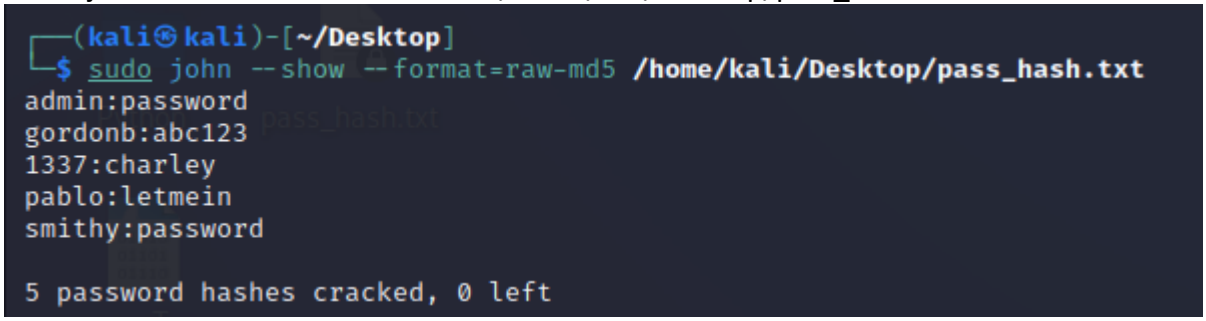
Dopodiché creo un unico file di testo chiamato “pass_hash.txt” dove vado a mettere insieme le coppie utente-password, come richiesto dal tool “John the ripper” per il corretto funzionamento del cracking



In conclusione, usando il tool di cracking “John the Ripper” data la sua efficacia nel gestire parallelamente i task per ridurre i tempi di cracking, stampo le password decriptate con il comando
“sudo john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt pass_hash.txt”



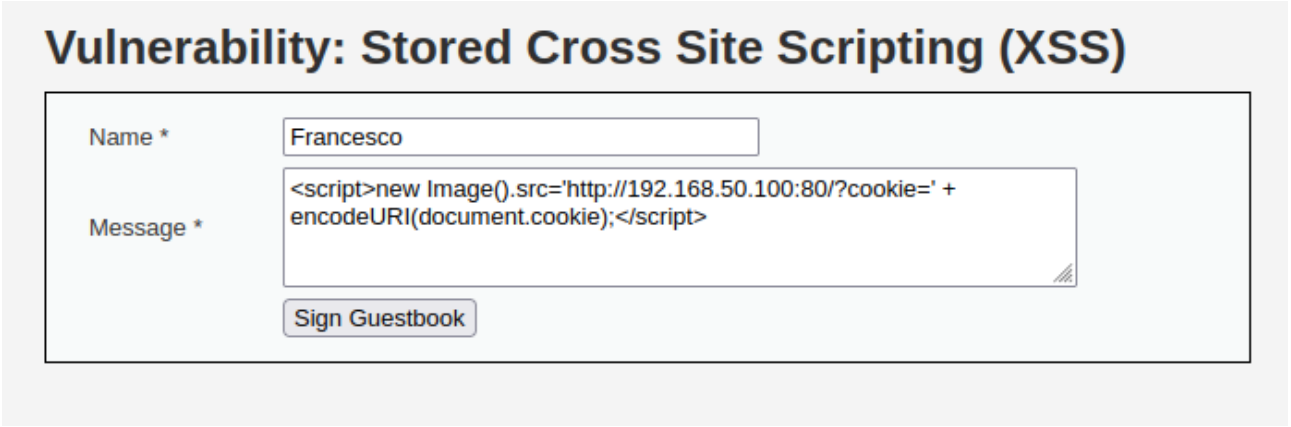
Al termine della sessione di cracking per vedere tutte le password trovate basta dare il comando “sudo john --show --format=raw-md5 /home/kali/Desktop/pass_hash.txt”



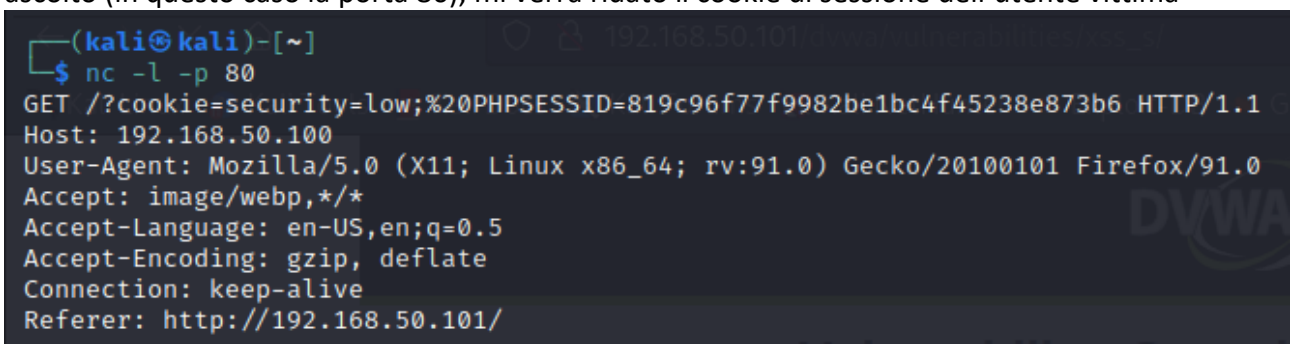
In realtà questo modo di carpire le informazioni passando una semplice query nel form si addice molto più alla classica SQLi. La SQLi Blind dovrebbe rendere la vita più difficile e non mostrare il contenuto del proprio DB così facilmente, ma questo dipende dalla configurazione della macchina vittima (in questo caso Metasploitable). Per fare una prova di come possa rispondere una SQLi Blind su una macchina configurata meglio sono entrato in locale su DVWA e provando a fare la stessa query la risposta del DB è stata questa

2.
Vado nella sezione XSS stored e scrivo il mio scripting persistente per farmi inviare i cookie di sessione della vittima (Metasploitable) alla mia macchina attaccante(kali).
Nel textbox “Message” del XSS stored per poter scrivere tutto lo scripting devo aumentare la “maxlength” ispezionando la textarea

Dopodiché inseriamo il nostro codice malevolo

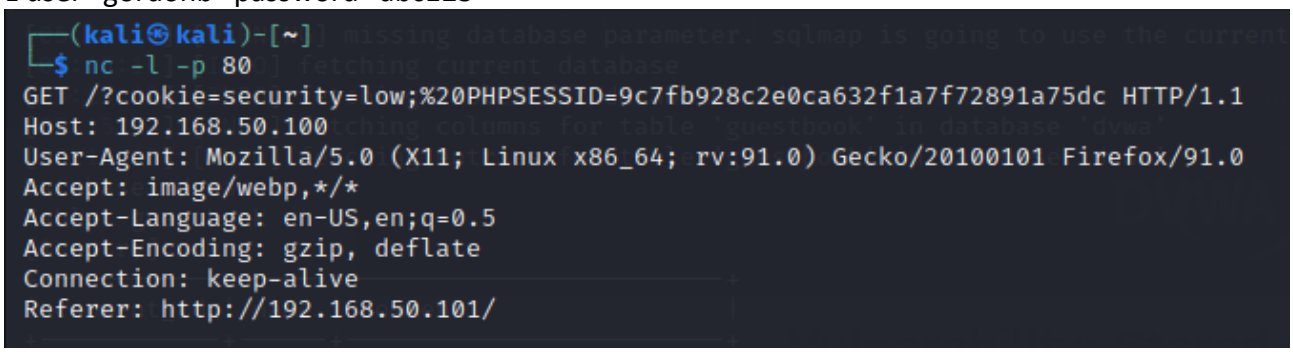


E andando su kali utilizzando netcat con il comando “nc -l -p 80”, dove lo switch “-l” serve per restare in ascolto e lo switch “-p” serve a indicare la porta su cui il servizio deve rimanere in ascolto (in questo caso la porta 80), mi verrà ridato il cookie di sessione dell’utente vittima

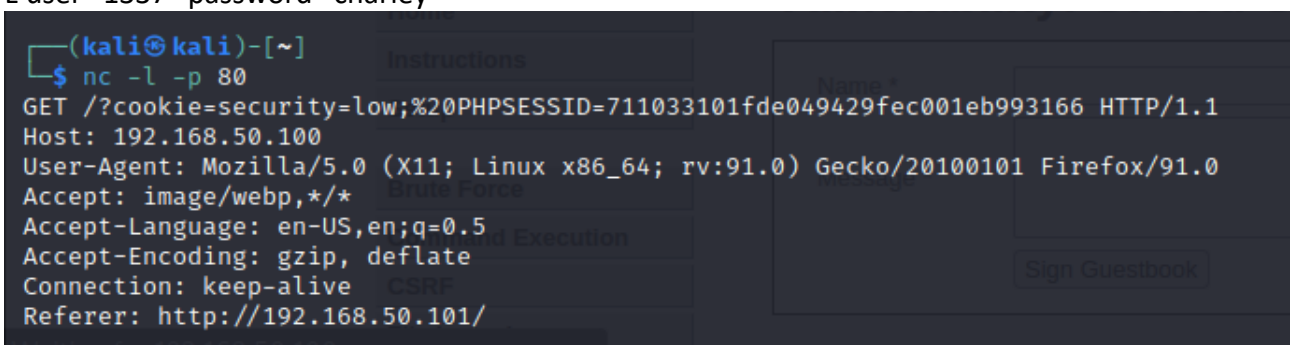


Il cookie trovato appartiene alla sessione aperta con l’user “admin” e password “password”. Si possono prelevare i cookie di sessione di tutti gli altri utenti presenti nel DB utilizzando le credenziali trovate con la SQLi fatta precedentemente

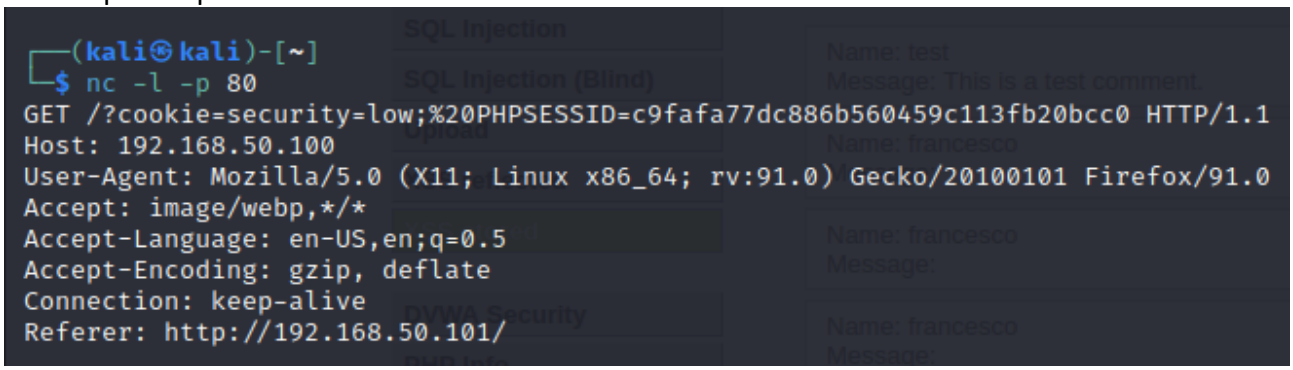
L’user “gordonb” password “abc123”



L’user “1337” password “charley”



L’user “pablo” password “letmein”



L’user “smithy” password “password”