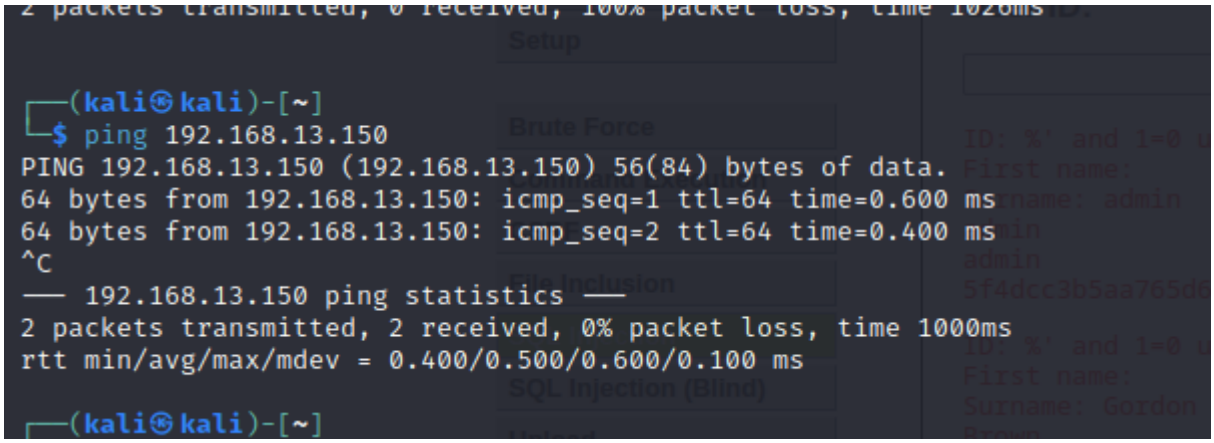
Build Week 2 Giorno 1

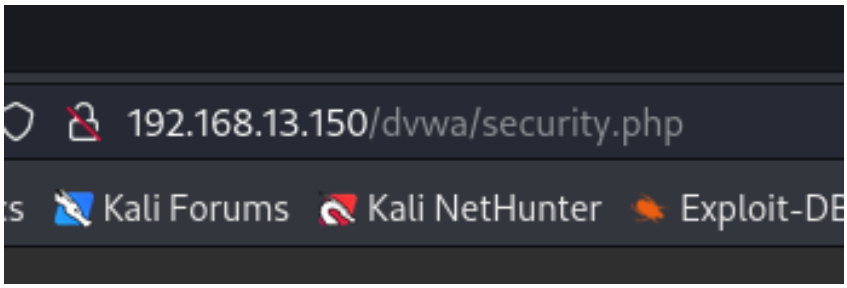
SQL Injection

Andiamo prima di tutto a settare le macchine virtuali in modo da farle comunicare sulla sottorete .13 dando a Kali Linux e Metasploitable i rispettivi indirizzi IP:

- 192.168.13.100
- 192.168.13.150

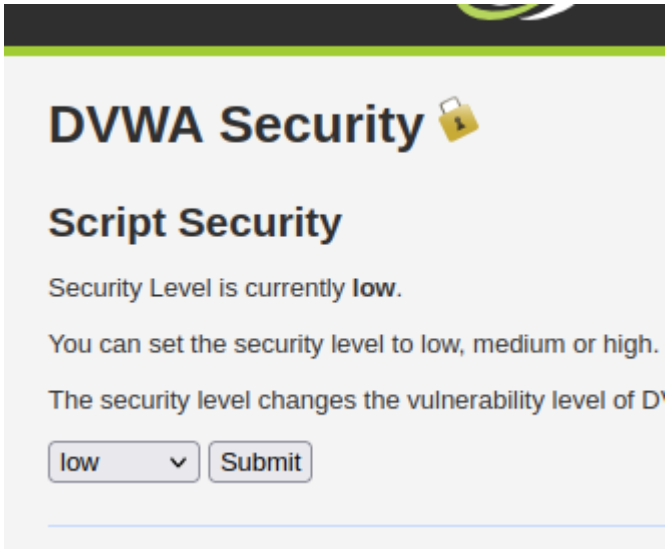


Colleghiamoci alla DVWA di Metasploitable attraverso il browser e impostiamo il livello di sicurezza a “LOW”



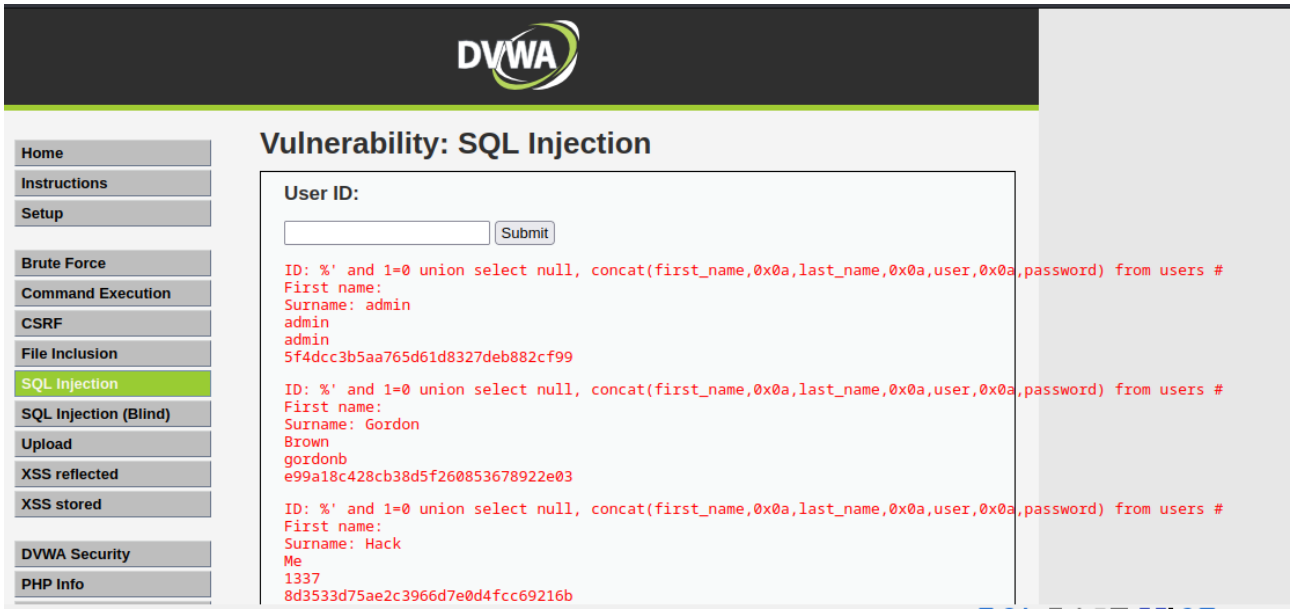
Il primo login lo andremo ad eseguire con l’utente di default:

Admin
Password

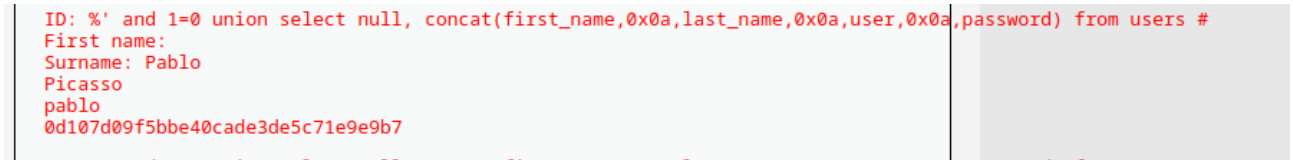


Colleghiamoci ora alla sezione dedicata all'SQL Injection e inseriamo il seguente script per ricavare tutti gli utenti presenti sulla piattaforma con i relativi hash delle password

%' and 1=0 union select null,
concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

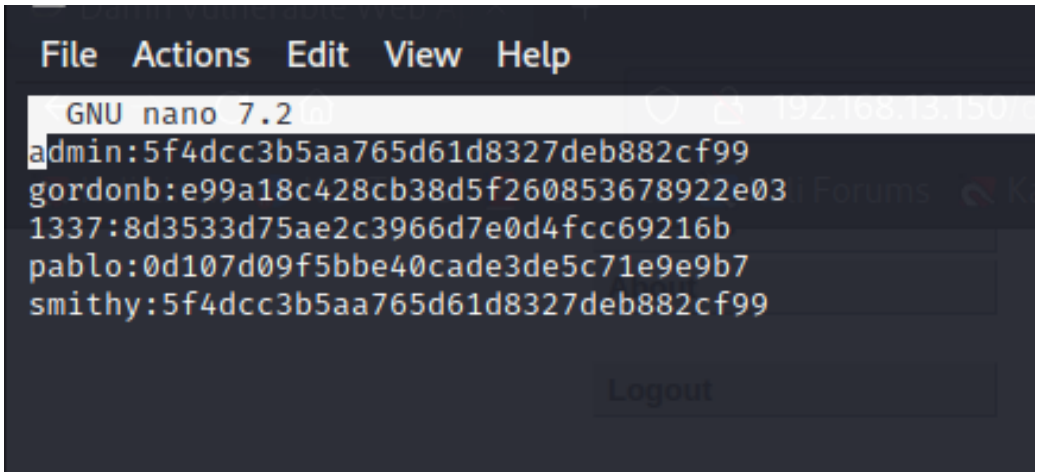


Ricaviamoci ora quello di nostro interesse, l'utente **"Pablo"**

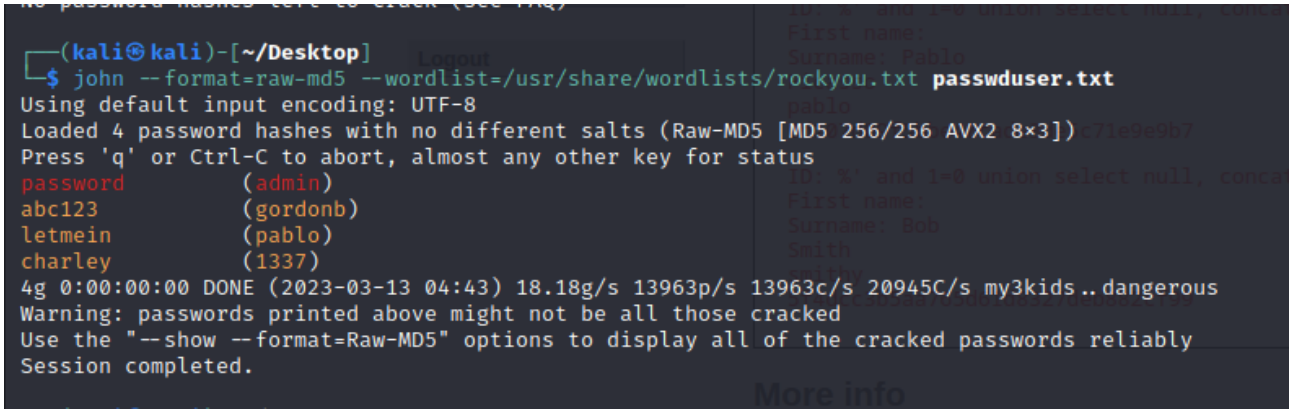


Come possiamo vedere lo script ci permette di ricavare oltre alla password hashata anche il relativo nome e cognome dell'utente

Creiamo ora un file di testo contenente gli hash delle password ricavati attraverso lo script sulla DVWA per poterlo poi dare in pasto al nostro tool dedicato John the Ripper



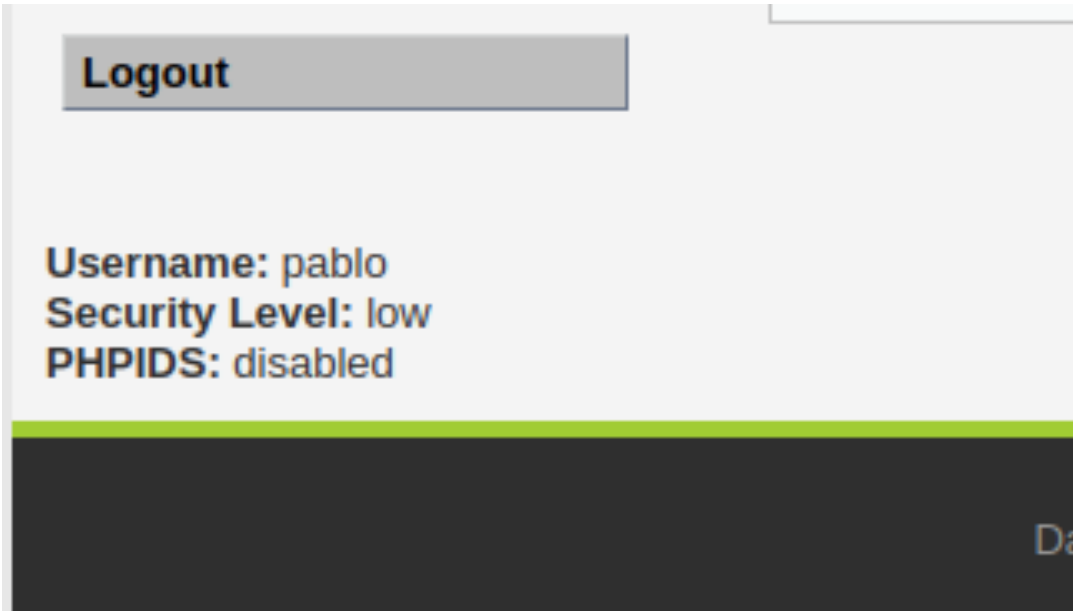
Una volta compreso quello che è il metodo di hash delle password utilizzato che in questo caso è l'md-5 andiamo a configurare JtR caricandovi un file pregenerato contenente delle password in chiaro con i relativi hashing e il nostro file di testo per farne una comparazione e capire quelle che possono essere le password utilizzate dagli utenti



È evidente che John the Ripper è riuscito nel suo intento trovando le varie password degli utenti

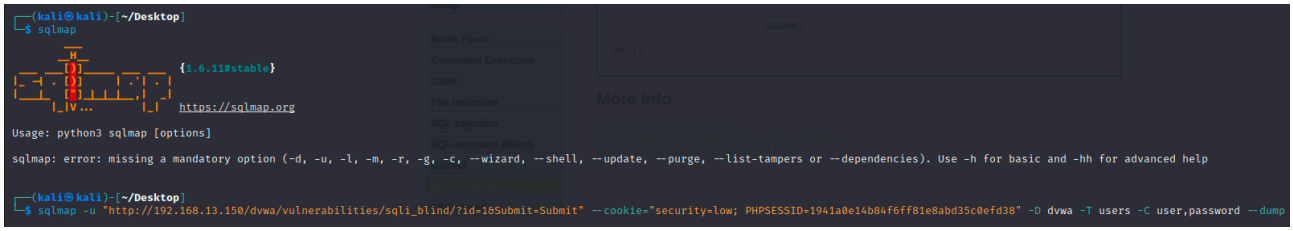
Per verificare che il lavoro sia stato eseguito in maniera corretta andiamo a riloggarci all'interno della DVWA di Metasploitable con l'username e la password

"pablo" e "letmein"



BONUS

Sfruttiamo SQLMAP per andare a recuperare gli user e relative password presenti sulla DVWA di Metasploitable con la funzione di decriptazione delle password in maniera automatica



Output generato: