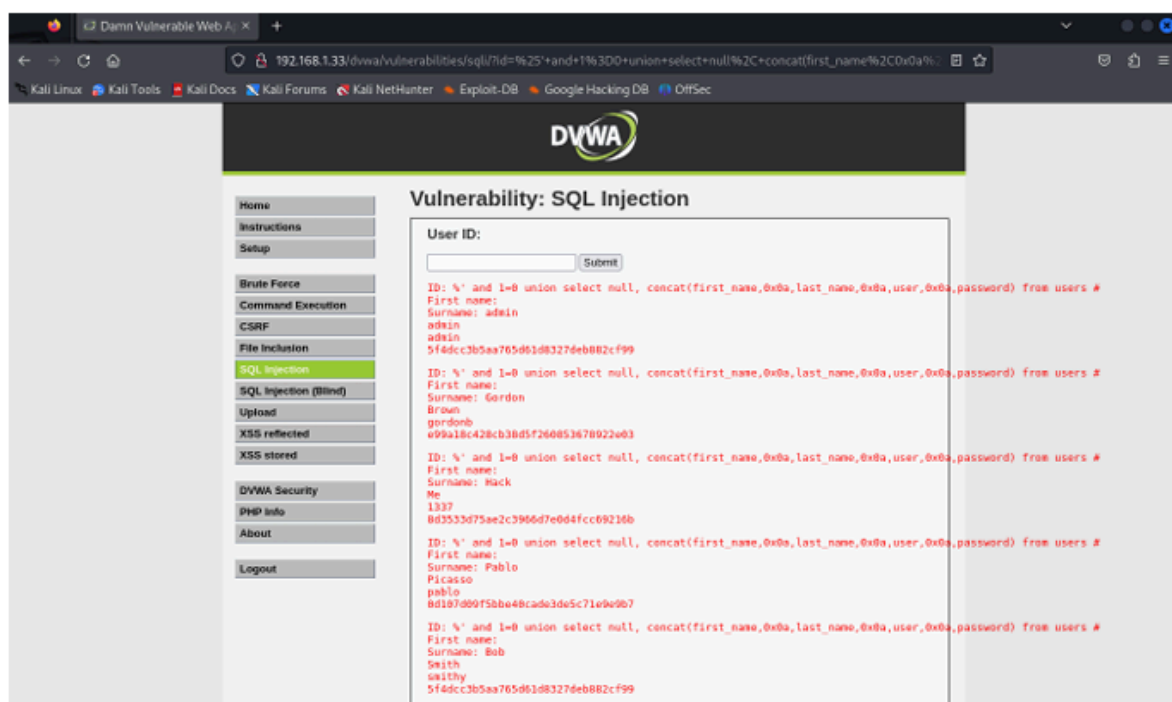


# Password cracking

Oggi proveremo a Trovare, usando john a trasformare il codice Hash della password

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:



Adesso prendiamo le password che in questo momento sono in codice hash

Ecco una tabella che riassume le informazioni fornite:

Utente	Password Hash MD5
admin	5f4dcc3b5aa765d61d8327deb882cf99
gordonb	e99a18c428cb38d5f260853678922e03
Hack me	8d3533d75ae2c3966d7e0d4fcc69216b
pablo	0d107d09f5bbe40cade3de5c71e9e9b7
smithy	5f4dcc3b5aa765d61d8327deb882cf9

Creiamo un file locale .txt e ci mettiamo dentro i codici hash

Adesso utilizziamo il comando:

`john --format = Raw-MD5 CrackMe.txt`

```

root@kali: /home/kali/Desktop
File Actions Edit View Help
(root@kali)-[/home/kali/Desktop]
# john --format=raw-md5 CrackMe.txt
stat: CrackMe.txt: No such file or directory

(root@kali)-[/home/kali/Desktop]
# john --format=raw-md5 CrackMe.txt
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=8
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 14:37) 11.62g/s 414767p/s 414767c/s 418339C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(root@kali)-[/home/kali/Desktop]
# john --show --format=raw-md5 CrackMe.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(root@kali)-[/home/kali/Desktop]
#

```

John è un software per craccare le password

John the Ripper è uno strumento di cracking delle password molto popolare disponibile su Kali Linux.

John prima di tentare una Brutalforce (va a tentativi finchè non la scopre) va a vedere nella sua tabellina per vedere se questi codici Hash sono presenti; se si va subito a tradurre.

