Traccia: password cracking

Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

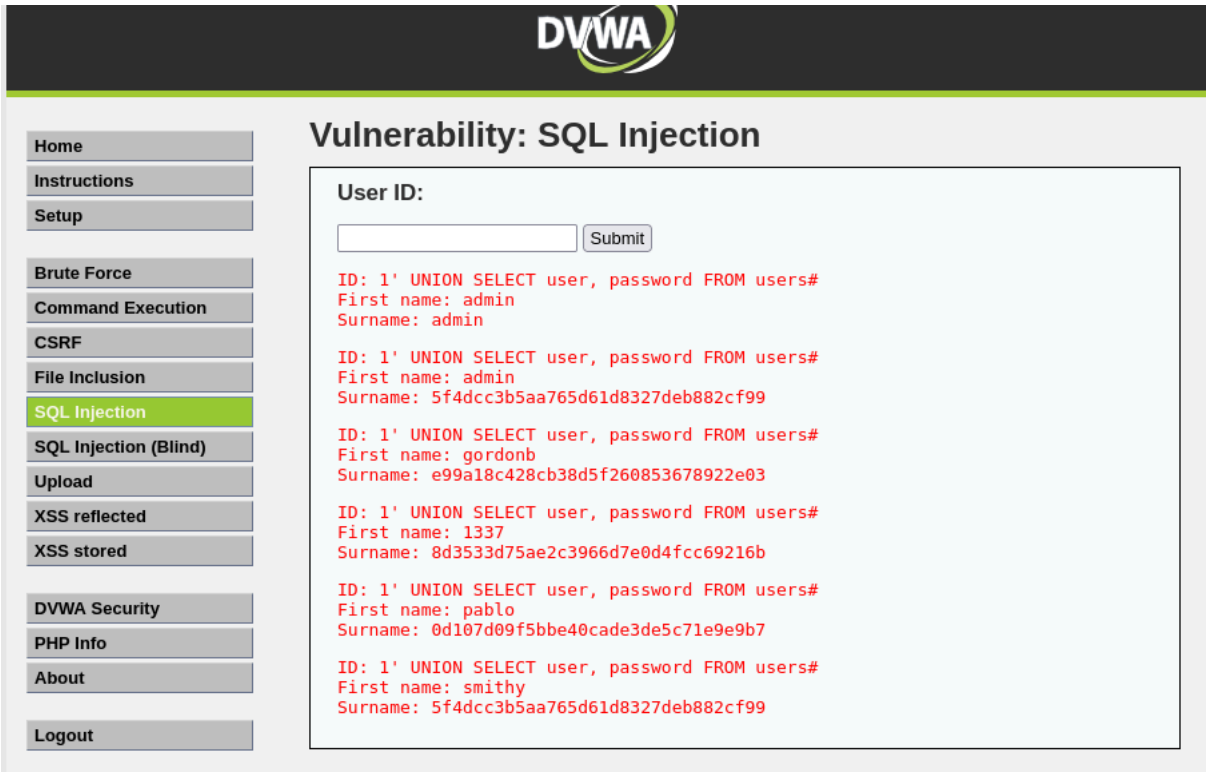
Se guardiamo meglio le password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto e provate ad eseguire delle sessioni di cracking sulla password con John the Ripper per recuperare la loro versione in chiaro.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

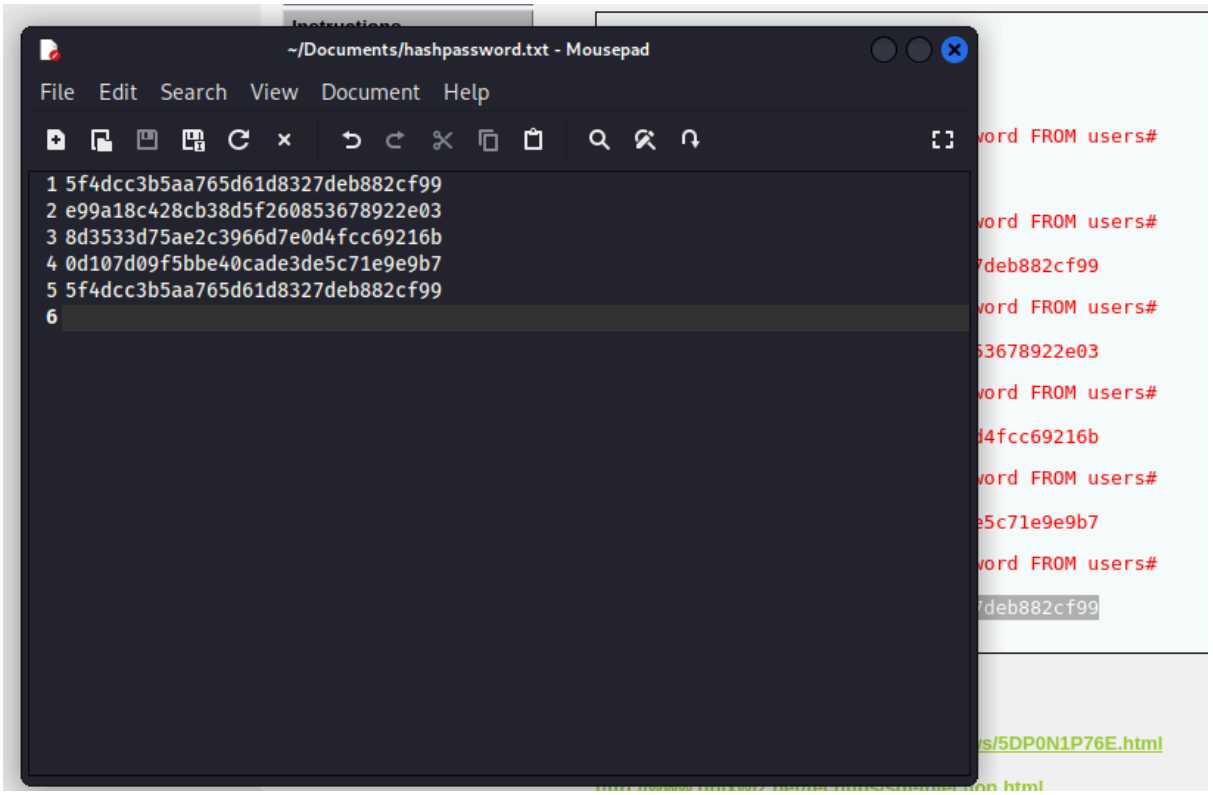
SVOLGIMENTO:

1.



ho trovato gli hash delle password con SQL

3.



ho creato un file txt con tutte gli hash delle password trovate da sql

```
solarwinds, SSH, sspr, Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE,
Sybase-PROP, tacacs-plus, tcp-md5, telegram, tezos, Tiger, tc_aes_xts,
HMAC-MD5, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512,

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Documents/hashpassword.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2025-10-10 13:50) 80.00g/s 61440p/s 61440c/s 92160C/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --show --format=raw-md5 /home/kali/Documents/hashpassword.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

prima di eseguire il comando corretto con john ovvero john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Documents/hashpassword.txt
ho dovuto scompattare il formato rockyou.txt perchè c'era ma non funzionava una volta scompattato il comando ha funzionato correttamente.

dopo di questo per vedere le password in chiaro ho usato il comando john --show --format=raw-md5 /home/kali/Documents/hashpassword.txt.

2. Spiegazione della tipologia e il meccanismo utilizzato per il cracking:

per questo tipo di cracking è stato usato un attacco di tipo dizionario ovvero wordlist, la tecnica prevede nel prendere una lista precompilata di parole candidate e verificare se le password in chiaro corrispondo all'hash presente nel target provando le varie parole e le varianti.
Questo tipo di attacchi sono efficaci quando le password sono deboli o presenti già in wordlist note.