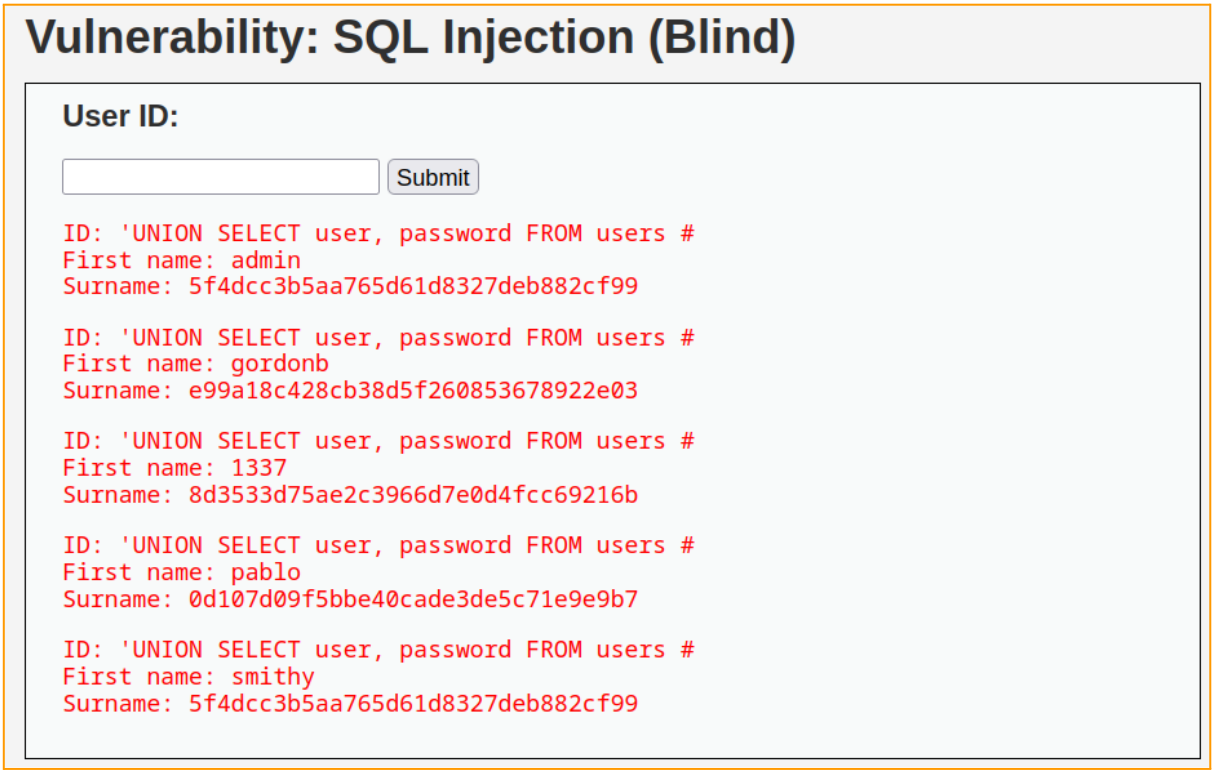
PASSWORD CRACKING

PENETRATION TESTING(2)

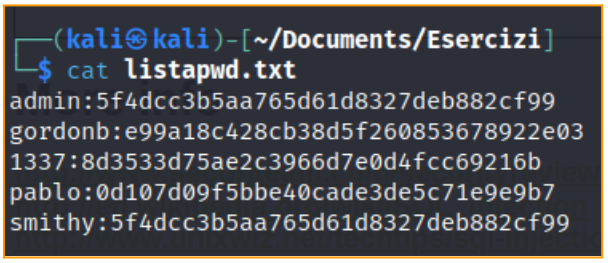
TRACCIA:
Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema. Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.
Recuperare le password dal DB come visto, e provare ad eseguire delle sessioni di cracking sulla password per recuperare la loro version in chiaro.

---

1) SCREENSHOT DELL'SQL INJECTION GIA' EFFETTUATA



Creo un file .txt dove inserisco gli hash da analizzare con JohnTheRipper abbinando il nome dell'utente con la relativa password.



In questa modalità JohnTheRipper utilizza un file in cui le password vengono confrontate con una lista di password.

2) DUE RIGHE DI SPIEGAZIONE DI COS'E' QUESTO CRACKING (QUALE TIPOLOGIA/QUALE MECCANISMO SFRUTTA)

La modalità Wordlist confronta l'hash con un elenco noto di potenziali corrispondenze di password, ciò implica che per eseguire l'attacco basato su dizionario (Wordlist) avremo bisogno di un dizionario. Quello più comunemente usato è la lista 'RockYou'.
Per eseguire l'attacco, avrà bisogno di 3 parametri

- Il formato dell'hash
- Il dizionario da utilizzare
- La lista di hash da crackare

Possiamo già trovare il file 'rockyou' nella directory `/usr/share/wordlists` in formato `.gz` vale a dire che è compresso nella directory

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirbuster      fern-wifi  legion      nmap.lst        sqlmap.txt  wifite.txt
dirb   fasttrack.txt  john.lst   metasploit  rockyou.txt.gz  wfuzz
```

Per decomprimere il file possiamo eseguire il comando `'gzip -dk rockyou.txt.gz'`

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# gzip -dk rockyou.txt.gz

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirbuster      fern-wifi  legion      nmap.lst     rockyou.txt.gz  wfuzz
dirb   fasttrack.txt  john.lst   metasploit  rockyou.txt  sqlmap.txt      wifite.txt
```

3) SCREENSHOT DELL'ESECUZIONE DEL CRACKING E DEL RISULTATO

Più debole è la password, più velocemente John riesce a capirla. Questo è il motivo per cui si consiglia sempre di avere password complesse.

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# john --wordlist=rockyou.txt --format=raw-md5 --verbosity=5 /home/kali/Documents/Esercizi/listapwd.txt
Created directory: /root/.john
initUnicode(UNICODE, UTF-8/ISO-8859-1)
UTF-8 → UTF-8 → UTF-8
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=5
Loaded 10 hashes with 1 different salts to test db from test vectors
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2023-09-23 23:04) 100.0g/s 72000p/s 72000c/s 96000C/s my3kids..soccer9
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.
```