

DECRIPTAZIONE DVWA

```
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2
3 gordonb:e99a18c428cb38d5f260853678922e03
4
5 1337:8d3533d75ae2c3966d7e0d4fcc69216b
6
7 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
8
9 smithy:5f4dcc3b5aa765d61d8327deb882cf99
10
```

Usando l'exploit del dvwa SQL injection ricaviamo username e password. Però troviamo dei dati criptati, in questo caso dobbiamo tradurli, usiamo John The Ripper.

```
File Edit Search View Document Help
1 root:*:0:root:/root:/usr/bin/zsh
2 daemon:*:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:*:2:bin:/bin:/usr/sbin/nologin
4 sys:*:3:sys:/dev:/usr/sbin/nologin
5 sync:*:4:65534:sync:/bin:/bin/sync
6 games:*:5:60:games:/usr/games:/usr/sbin/nologin
7 man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:*:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:*:8:mail:/var/mail:/usr/sbin/nologin
10 news:*:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:*:39:39:ircd:/run/ircd:/usr/sbin/nologin
17 _apt:*:42:65534::/nonexistent:/usr/sbin/nologin
18 nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:*:998:998:systemd Network Management:./usr/sbin/nologin
20 systemd-timesync:*:997:997:systemd Time Synchronization:./usr/sbin/nologin
21 messagebus:*:100:107::/nonexistent:/usr/sbin/nologin
22 tss:*:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false
23 strongswan:*:102:65534::/var/lib/strongswan:/usr/sbin/nologin
24 tcpdump:*:103:110::/nonexistent:/usr/sbin/nologin
25 usbmux:*:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
26 sshd:*:105:65534::/run/ssh:/usr/sbin/nologin
27 dnsmasq:*:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
28 avahi:*:107:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
```

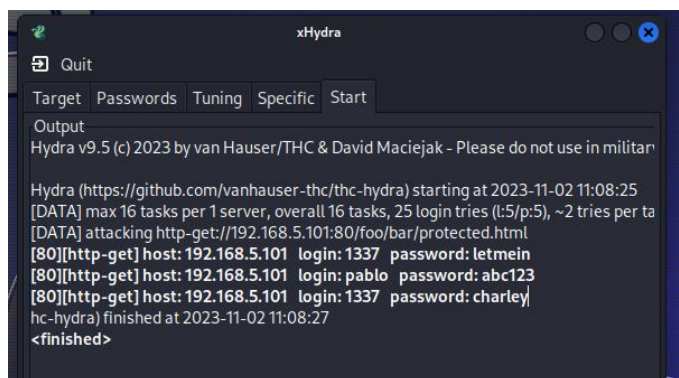
Creiamo un file usando la lista integrata su kali di Password e la lista criptata Shadow, usando un comando "unshadow" una i 2 files generando uno nuovo, chiamato HASHES.

```
(kali@kali)~[/Desktop]
$ john --format=raw-md5 fiel
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done! Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (?)
password (?)
abc123 (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2023-11-02 11:03) 5.319g/s 189734p/s 189734c/s 191368C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

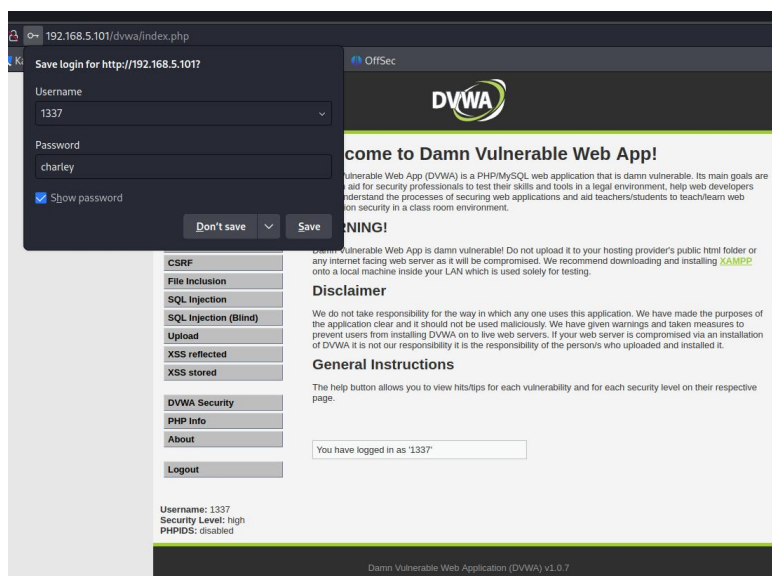
(kali@kali)~[/Desktop]
$ john --show --format=raw-md5 fiel
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

Usando questa nuova lista ora possiamo decifrare le pwd codificate usando il comando Format raw md5, comando che traduce il file.



Ora avendo a nostra disposizione sia username che pwd decifrate possiamo usare hydra per confermare quali di queste funziona.



Ed in effetti usando l'ultima combinazione siamo riusciti ad accedere alla pagina.