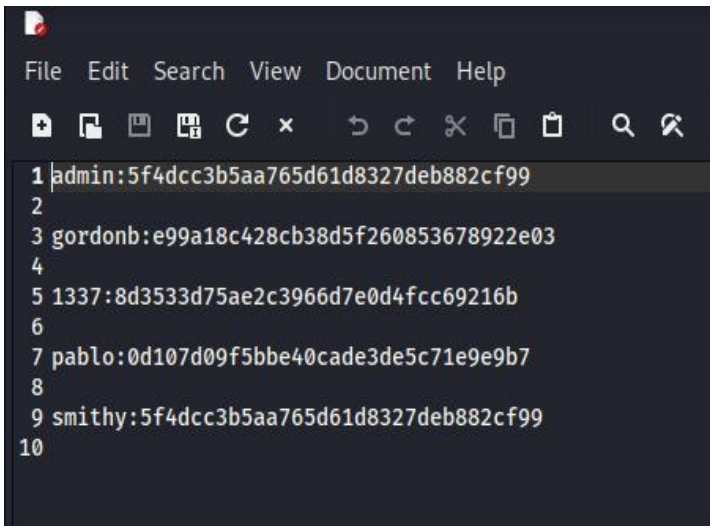
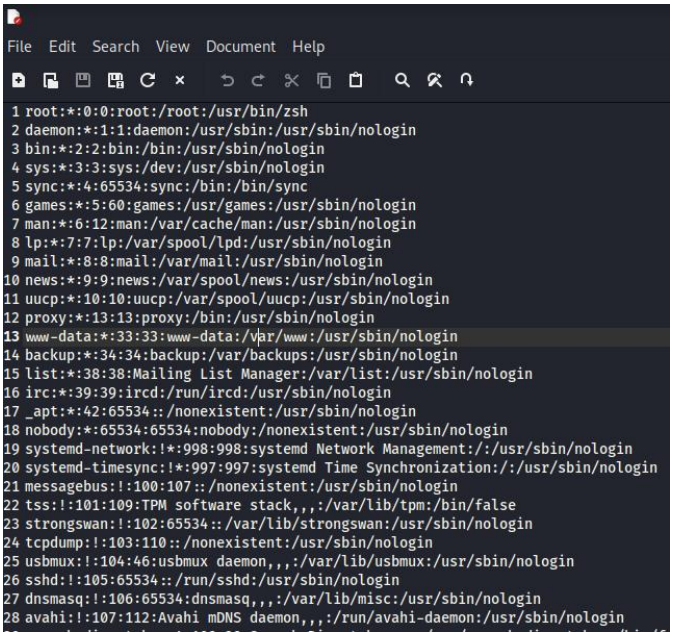
DECRIPTAZIONE DVWA



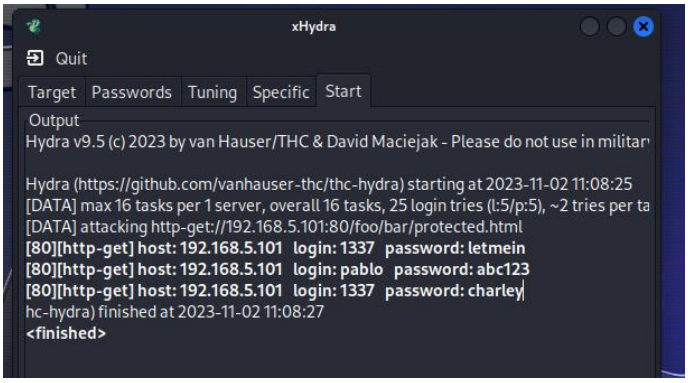
Usando l'exploit del dvwa SQL injection ricaviamo username e password. Però troviamo dei dati criptati, in questo caso dobbiamo tradurli, usiamo John The Ripper.



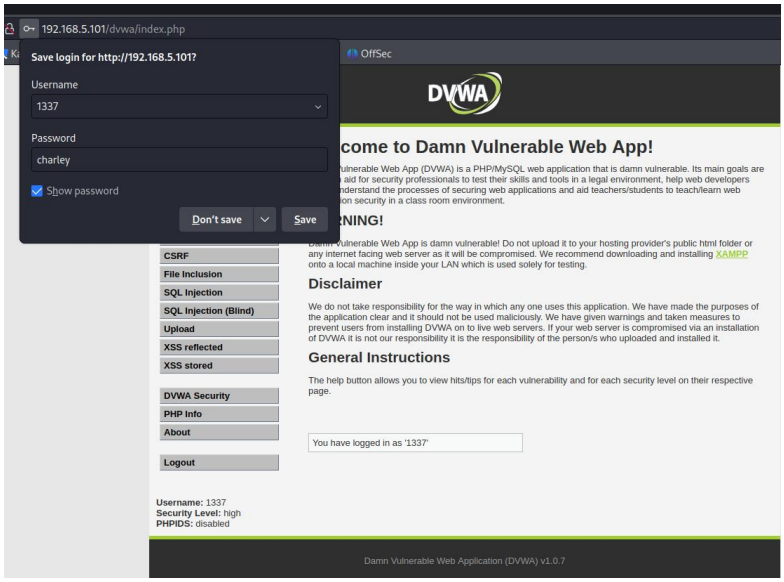
Creiamo un file usendo la lista integrata su kali di Password e la lista criptata Shadow, usando un comando "unshadow" une i 2 files generando uno nuovo, chiamato HASHES.

```
┌──(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 8×3])
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.