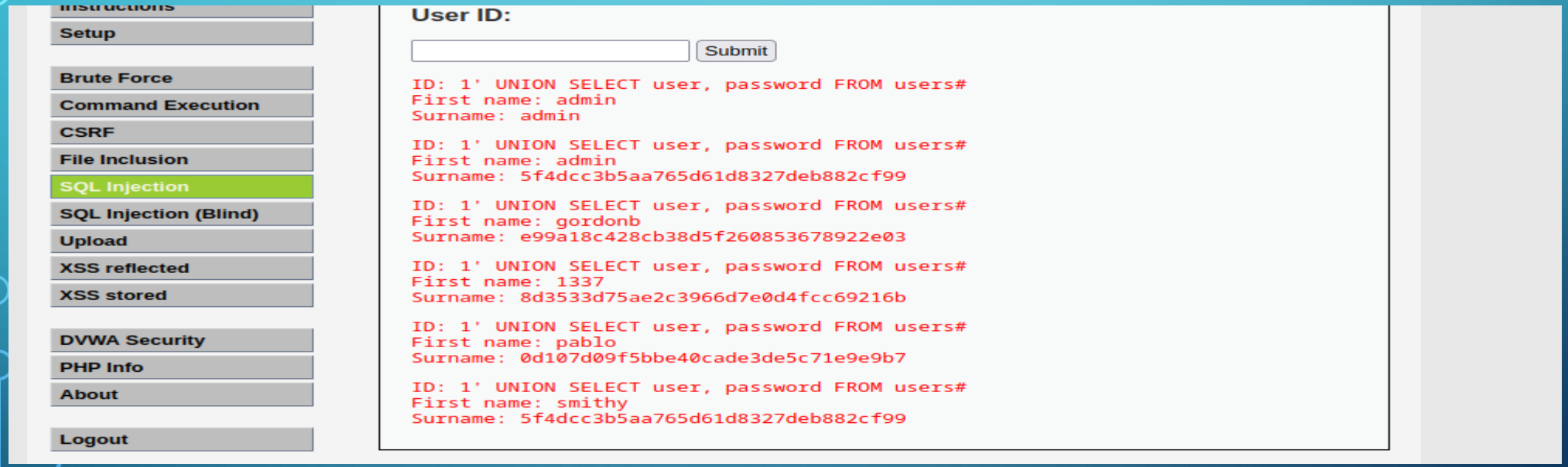
S6L3

LA TRACCIA DI OGGI CONSISTEVA TRAMITE UN TOOL DI KALI IN QUESTO CASO JOHN RIPPER DI CODIFICARE LE PASSWORD MD5 DAL DB DOPO AVER EFFETTUATO UNA SQL INJECTION



S6L3

```
4 password hashes cracked, 1 left

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --format=raw-md5 --wordlist= /home/kali/Desktop/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Remaining 1 password hash
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2024-01-10 12:13) 0g/s 88650p/s 88650c/s 88650C/s !@#$%..sss
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --format=raw-md5 --show= /home/kali/Desktop/rockyou.txt hash.txt
admin:password
gordonb:abc123
pablo:letmein
smithy:password

4 password hashes cracked, 1 left

┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=RAW-MD5 --show /home/kali/Desktop/rockyou.txt hash.txt
admin:password
gordonb:abc123
pablo:letmein
smithy:password

4 password hashes cracked, 1 left
```