1. The target has a specific web application running that we can find by looking into the HTML source code. What is the name of that web application?

```bash

┌─[eu-academy-6]─[10.10.14.54]─[htb-ac-1522420@htb-64gaaygog6]─[~]

└──╼ [★]$ nmap -sC -sV 10.129.150.44

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-18 00:34 CST

Nmap scan report for 10.129.150.44

Host is up (0.16s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 71:08:b0:c4:f3:ca:97:57:64:97:70:f9:fe:c5:0c:7b (RSA)

| 256 45:c3:b5:14:63:99:3d:9e:b3:22:51:e5:97:76:e1:50 (ECDSA)

|\_ 256 2e:c2:41:66:46:ef:b6:81:95:d5:aa:35:23:94:55:38 (ED25519)

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

|\_http-server-header: Apache/2.4.41 (Ubuntu)

|\_http-title: elFinder 2.1.x source version with PHP connector

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

```

Tên của ứng dụng web là : elFinder

P/s :elFinder

```bash

search elFinder

use 4

```

A screenshot of a computer

Description automatically generated

1. Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?