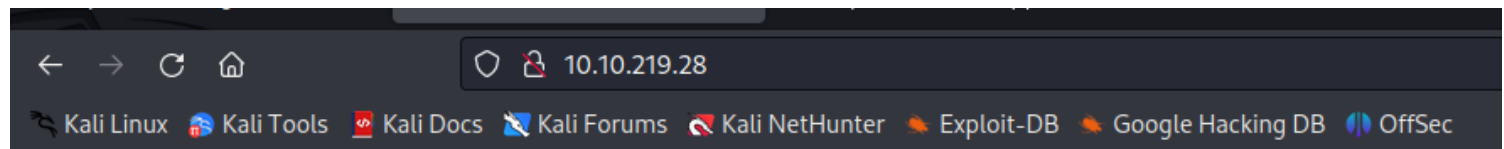


agent sudo

CTF agent sudo
IP=10.10.219.28

website



Dear agents,

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

From,
Agent R

APACHE HTTP SERVER version: 2.4.29
PHP
UBUNTU

nmap

```
# Nmap 7.93 scan initiated Sat Jul 8 14:15:05 2023 as: nmap -A -v -T4 -oN nmap10.10.219.28Scan.txt 10.10.219.28
Nmap scan report for 10.10.219.28
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (reset)
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 ef1f5d04d47795066072ecf058f2cc07 (RSA)
| 256 5e02d19ac4e7430662c19e25848ae7ea (ECDSA)
|_ 256 2d005cb9fda8c8d880e3924f8b4f18e2 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Annoucement
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=7/8%OT=21%CT=1%CU=40096%PV=Y%DS=4%DC=T%G=Y%TM=64A9A7D0
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=A)OPS(
OS:O1=M509ST11NW6%O2=M509ST11NW6%O3=M509NNT11NW6%O4=M509ST11NW6%O5=M509ST11
OS:NW6%O6=M509ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(
OS:R=Y%DF=Y%T=40%W=6903%O=M509NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

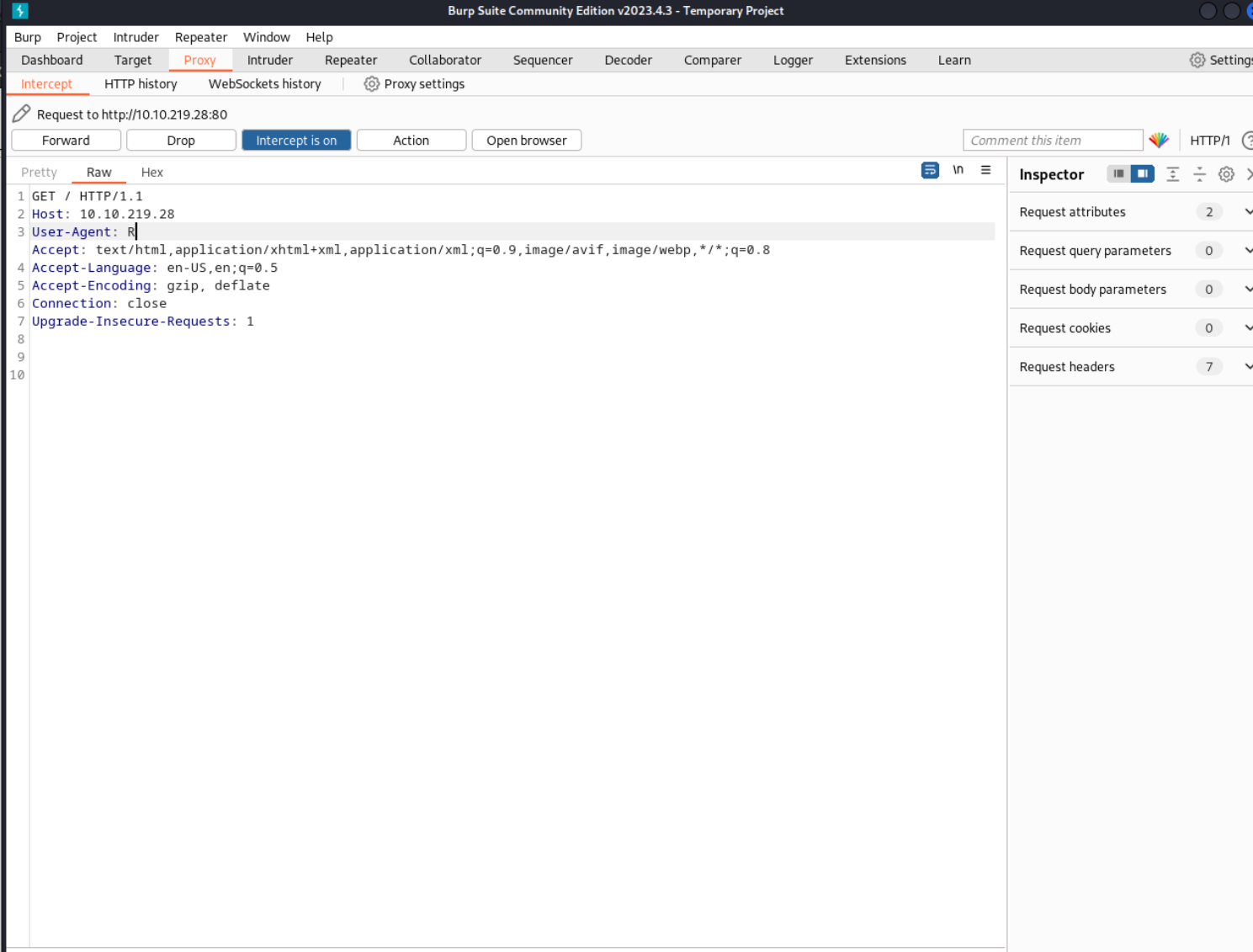
Uptime guess: 25.236 days (since Tue Jun 13 08:36:21 2023)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 154.21 ms 10.6.0.1
2 ... 3
4 223.28 ms 10.10.219.28

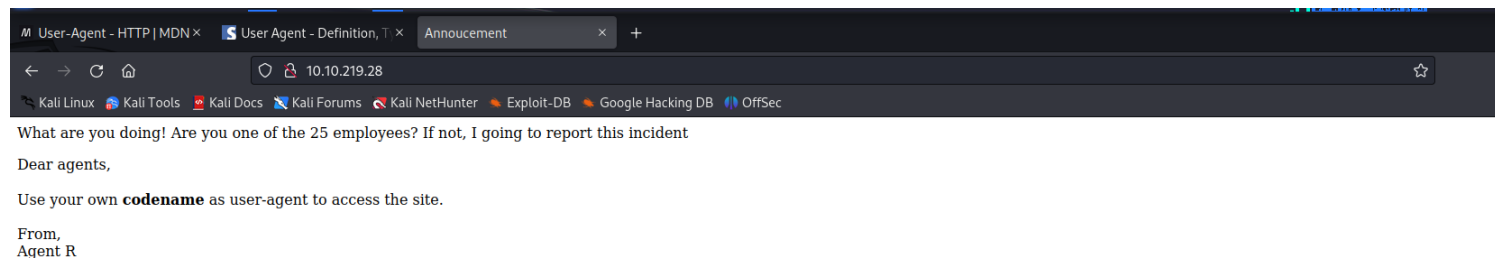
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jul 8 14:15:44 2023 -- 1 IP address (1 host up) scanned in 38.57 seconds
```

#####

```
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
```



INTERCEPT OFF



C

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


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




Burp Suite Community Edition 2.3.20 (64-bit) - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn  Settings






Intercept HTTP history WebSockets history  Proxy settings

 Request to http://10.10.219.28:80

 HTTP/1 (

Pretty **Raw** Hex   

```
1 GET /agent_C_attention.php HTTP/1.1
2 Host: 10.10.219.28
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Inspector     

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	7