

CSAW CTF 2016 Quals: evidence.zip

Category: Forensics

Points: 100

Solves: 170

Description:

As part of CSAW CTF's ongoing efforts to terminate cheaters with extreme prejudice, we were supposed to have evidence incriminating a handful of teams in this zip file. I do not know what happened, but I do not think the evidence actually made it in there...

Write Up:

So to be honest it's a miracle that I actually even solved this challenge.

"string evidence.zip" gave a massive dump of gibberish, but if you were paying attention, you would've noticed this at the end of the terminal.

```
" ...
JDzq<ilvf|5'*PK
galf
out/rxo802ayx4
3ht{
out/zhatnf5maf
1iv_
out/50lshu1ue6
n4i1
out/14o803swdq
3w
out/nppjdd2wdg
d33n
out/e9ydsxwetg
rf#_
out/0eetjrxpdm
elee
out/otuj3jrezt
neff
out/m70ohrycax
out/mpi3z4x5jt
out/meoflsxv4v
out/8y10tp04b2
out/eui6ltoijl"
```

If you put it all together you'll get {neffeleerf#_d33n_3w_n4i1iv_3ht}galf which was the reverse of the actual flag.

Michael Vu

Flag

```
flag{roses_r_blue_violets_r_r3d_mayb3_harambae_is_not_kill}
```