

A Zena based CTF Team

ABOUT / CALENDAR / GYM / LEARNING / PRESS / WRITE-UP

X-MAS CTF - Catana

DEC 12, 2018

zangobot - zxgio

The program tries to compute a sequence of very big numbers and it uses them to decode the flag. The function at address ①x00400556 contains the generator of that sequence (it is not **PIE**, hence the functions are loaded always at the same addresses). We translated it into python code:

```
def catalan(a1,a2,a3):
    result=0
    if a1 ==a2 and a2==a3: return 1
    if a1 > a2: result= catalan(a1, a2+1,a3)
    if a1 > a3 and a2>a3: result += catalan(a1,a2,a3+1)
    return result
```

By googling the first results of the sequence, we understood that it is a famous mathematical series called Catalan Numbers.

The program tries to compute this sequence for numbers from 1 to 36, and it is computationally unbearable. Moreover, not all the computations are necessary because the program multiplies the computed value with an entry of a matrix, which hardcoded into the program. Only few entries are different from zero, so it's a waste of CPU!

To overcome this issue, we dumped the matrix using **radare2** and we precomputed the first 36 catalan numbers. Then, we used fridato re-write the catalan function to avoid any computation, and we replaced it with a lookup table.

And we are done! Here you can find the file of the challenge. The flag is X-MAS{c474l4n_4nd_54n74_w3r3_600d_fr13nd5_1_7h1nk}.

ZenHack

Powered By Gravity
Made with ♥ on { { Jekyll } }

ZenHackTeam

A Zena based CTF Team