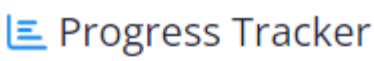
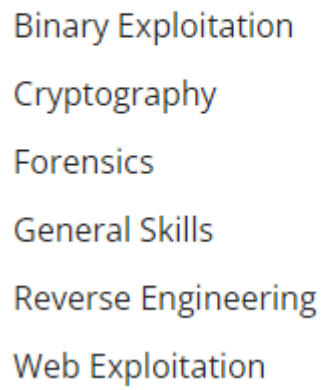
Progress in Capture The Flag (CTF) Challenges

This documentation provides a comprehensive overview of my journey and progress in the field of cybersecurity through participation in Capture The Flag (CTF) challenges in ***https://play.picoctf.org/****. Explore my experiences, victories, challenges, and learnings as I navigate the diverse landscape of CTFs, honing my skills, and advancing my expertise in information security.*

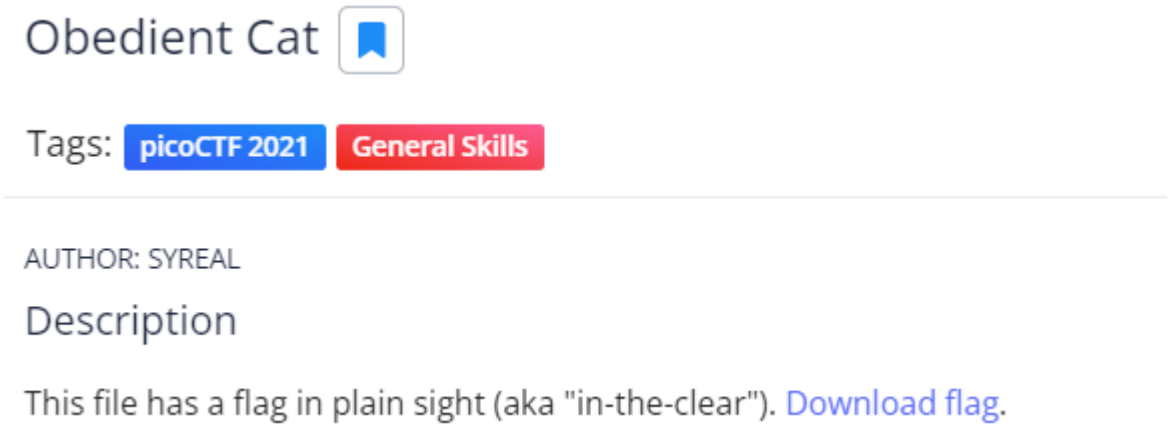
So first I learned about CTFs on 24th of February 2024. As I was looking up for some starting projects for cyber security I found out this site and started checking it more. I saw some videos on YT about it and decided to take part and test my skills or at least a bit more about… everything 🙂





I started with probably the easiest one… in general skills

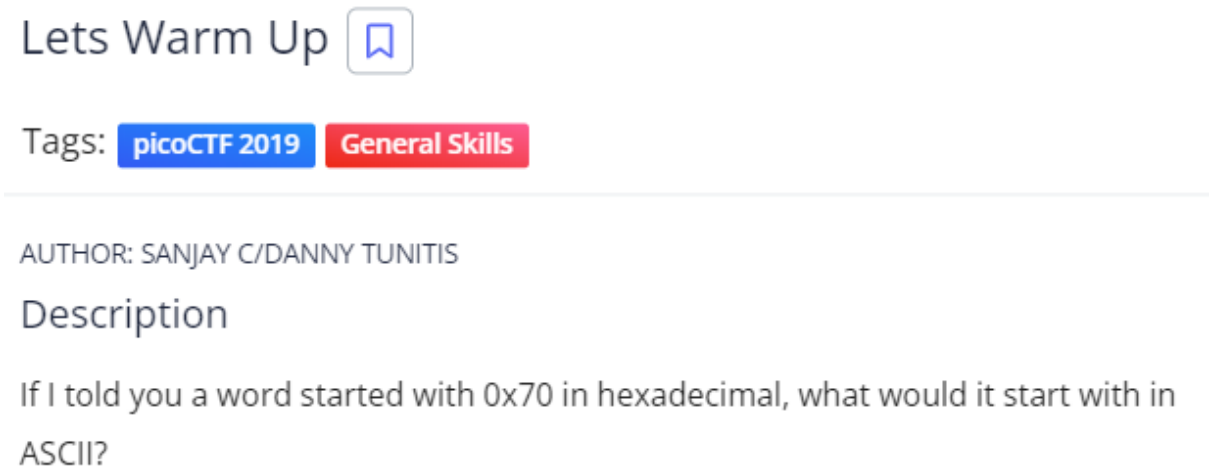
1.



There are some hints if you want to use them, <u>the second two are for linux.</u>
After I downloaded the file, I opened it in notepad and the answer was there:

picoCTF{s4n1ty_v3r1f13d_1a94e0f9}

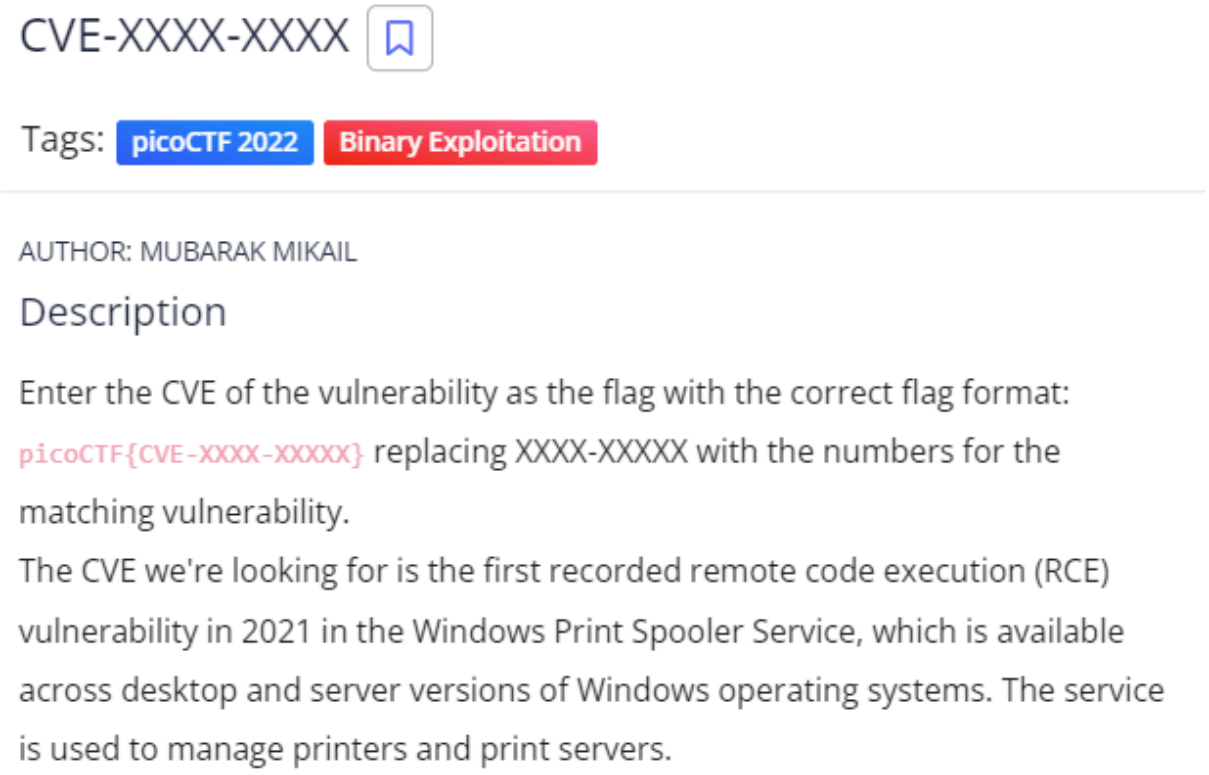
2.



In hexadecimal, each digit represents four bits. The hexadecimal value "70" translates to binary as "01110000".
Now, referring to an ASCII table, we can find that the binary value "01110000" corresponds to the character "p".

picoCTF{P}

3.



So the third one I was a bit curious about, but all I got about it was this 2021 Windows Print Spooler Service… I've decided to google it and found out this: https://nsfocusglobal.com/windows-print-spooler-rce-vulnerabilities-cve-2021-1675-cve-2021-34527-mitigation-guide/

So the answer was right infront of me
picoCTF{CVE-2021-34527}