__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 🙂

📊 Progress Tracker

Binary Exploitation

Cryptography

Forensics

General Skills

Reverse Engineering

Web Exploitation

I started with probably the easiest one… in general skills

1.

Obedient Cat 🔖

Tags: **picoCTF 2021** **General Skills**

AUTHOR: SYREAL

Description

This file has a flag in plain sight (aka "in-the-clear"). Download flag.

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

picoCTF{s4n1ty_v3r1f13d_1a94e0f9}

2.

Lets Warm Up 🔖

Tags: **picoCTF 2019** **General Skills**

AUTHOR: SANJAY C/DANNY TUNITIS

Description

If I told you a word started with 0x70 in hexadecimal, what would it start with in ASCII?

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.