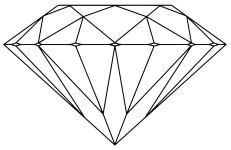
CRYPTONITE — TASK PHASE II



Congratulations for making it through TP-1.

You are now a part of **Cryptonite's** second task phase.

This will last from November 1 2024 to Jan 1 2025, with a break in between for endsems. A final, *offline* interview will be held at the end.

For this stage, you're going to be completing a set of selected challenges on CMU's PicoCTF platform:

https://play.picoctf.org/practice/

The **mandatory** challenge list is given below:

No.	Reverse Engg.	Forensics	Web Exp	Cryptography	Binary Exp
1	GDB baby step 1	trivial flag transfer protocol	SOAP	C3	buffer overflow 0
2	ARMssembly 1	tunn3l v1s10n	Forbidden Paths	Custom encryption	format string 0
3	Vault door 3	m00nwalk	cookies	miniRSA	flag leak

In addition to these mandatory challenges, you are also **required to complete *at least* 2 additional challenges in any two domains of your interest (medium difficulty and above only).**

You are also required to attach a final screenshot of your dashboard with your username and graph of all challenges solved in your repository's `README.md` file.

You are expected to make detailed writeups for each and every one of the challenges. They must include:

- The flag you found after solving the challenge.
- Your thought process and approach to the challenge.
- Every single new concept and point of knowledge you learned or improved upon through solving the challenge.
- Any incorrect tangents you went on while solving, and why.

A few other pointers:

- Avoid using screenshots for terminal output, use triple backticks instead.
- Include textual outputs and screenshots for *everything*.
- **Do not copy others' work or flags. Flags for Pico and pwn.college are unique, so we'll know.**
- **Your reasonings must be non GPTish and usage of any and all AI (for writeups) is not allowed.**

Writeups should go into a `picoctf/` directory in your task phase repos, and all domains should have a single file with all the writeups, e.g. `picoctf/Cryptography.md`.

RESOURCES

What is a CTF?

- https://www.youtube.com/watch?v=8ev9ZX9J45A

Reverse Engineering

- https://www.youtube.com/watch?v=1d-6Hv1c39c
- https://www.youtube.com/watch?v=gh2RXE9BIN8
- https://www.youtube.com/playlist?list=PLMB3ddm5Yvh3gf_iev78YP5EPzkA3nPdL

Forensics

- https://www.youtube.com/watch?v=giv0DQDSsjQ
- https://trailofbits.github.io/ctf/forensics/
- https://github.com/JohnHammond/ctf-katana

Cryptography

- https://ctf101.org/cryptography/overview/
- https://www.w3schools.com/python/
- https://youtube.com/playlist?list=PLBlnK6fEyqRhBsP45jUdcqBivf25hyVkU&si=u23UPPdx_UIInJ2i

Web Exploitation

- https://www.youtube.com/watch?v=iGDJ695dUEM
- https://www.youtube.com/watch?v=-Zea7GB2OwA
- https://www.youtube.com/playlist?list=PLhixgUqwRTjx2BmNF5-GddyqZcizwLLGP
- https://www.youtube.com/playlist?list=PLLKT__MCUeixCoi2jtP2Jj8nZzM4MOzBL

Binary Exploitation

- https://ctf101.org/binary-exploitation/overview/
- https://youtube.com/watch?v=CRTR5ljBjPM
- https://youtube.com/playlist?list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN&si=QAGypL3l6zjS_8Hm