**PwCTF**

**Description:**

Students will participate in several main categories of challenges, and each individual challenge will have a flag in the form: **flag{<flag\_goes\_here>} OR PwCTF{<flag\_goes\_here>} (NOTE: These ARE NOT an actual flag)**. These flags will be submitted on the CTFd platform found here: <https://usa.pwctf.com>. The main goal of the Capture the Flag (CTF) is to be the student with the most points at the end of the CTF.

**Scenario:**

Evil threat actors are attempting to bring down the infrastructure of Metropolis. We need your help to find what was breached and how.

**Rules:**

The CTF will run from 11:00 AM on February 15th to 11:00 AM on February 16th (24 hours total). The CTFd platform uses point values to determine who wins; the more difficult the challenge, the more points it is worth. The student with the most points when the CTF ends will be crowned victor! Ties will be broken based on who had the higher score first. Hacking the scoring server or sharing flags is off limits and will result in disqualification, but you are encouraged to use resources like google, classmates, and the PwC representatives to solve the challenges.

**Prizes:**

Prizes will be given to 1st place, 2nd place, and 3rd place. The prize catalog can be found [here](https://docs.google.com/document/d/1hu9Ok9mOjoV1AF_usymxCW6ClnmmaLZQ9FrMFdXsO20/edit). In order to receive prizes you MUST be a HackUNT participant and be physically present at the competition.

**Recommendations:**

The recommended materials for CTF participation include the following:

* Laptop with 8GB RAM (and charger 😁)
* Kali Linux (64-bit) VM **OR** Linux Dual Boot (64-bit)
  + NOTE: The CSE machine is 32-bit and most executables in this CTF are 64-bit

GOOD LUCK

We appreciate you reading the rules, here’s a flag: flag{rul3s\_ar3\_important\_too} **(NOTE: This IS an actual flag)**