This report will show what I have done, of which the CTF challenges which I created are the focus.

GitHub for the CTFS and the discord bot:

https://github.com/Outpacing82/Ctfs-and-discord-bot

CTF 1: Reverse Engineering

This CTF focuses on Binary Analysis, where the player is expected to reverse XOR operations to derive the key.

CTF 2: Binary Exploit

In this CTF, I referenced the week 2 wargames, where users are expected to use techniques like objdump, memory layout and buffer overflows to find the relevant function's address.

CTF 3: XSS (Cross-Site Scripting)

This was inspired by week 3's wargames, where we learned to not let user input show freely as they could make your website do anything. Attackers would need to test out different methods to see which one would achieve the goal listed in README.md.

CTF 4: Web Authentication

This is one of my harder CTFs, as it combines web authentication, session and cookie-handling, and even base64 data manipulation. The goal is to teach players that even small things like cookies can to serious vulnerabilities

CTF 5: SQL Injection

This is a simple CTF that simulates a weak login system, where the attacker must exploit improper input sanitisation to obtain a hidden flag

CTF 6: SSRF (Server-Side Request Forgery)

This CTF is mainly inspired by the newest wargames in week 7, where I had trouble understanding how etc/hosts aUect internal network accesses, and that lead to me designing a CTF that expects the player to manipulate URLS to access the flag.

Tools Learned:

Flask, PHP, SQLite3, discordAPI

Discord Bot

A discord bot that has several commands related to general security concepts. Here are some features and their security impact:

- !ipInfo: Puts the given ip into VirusTotal, and separates the checks of antivirus companies into two categories, Harmless and Malicious
- !linkInfo: Puts the given link into VirusTotal, and separates the checks of antivirus companies into four categories, Harmless, Suspicious, Malicious and Undetected.
- !ctf: gives out the repo of one of the six CTFs that I made at random
- Simple scam message filter: commonly used phishing terms would be automatically removed, and the person who sent the message will be given a warning.