# Evil Corp Challenge

Group No: #1

Group Members: Hemanth Bojja (11702675), Vamsi Pavan Krishna Dasineni (11658186), Aryanth Reddy Kondreddy (11696947), Sushmitha Inapakuthika (11696399).

## Introduction:

The "Evil Corp" challenge is a pwn (exploitation) category challenge in cybersecurity competitions. It is designed to assess participants' skills in identifying and exploiting vulnerabilities in a simulated environment. Participants are required to find and exploit
vulnerabilities within the challenge to gain control or access to specific resources.

## Abstract:

Pwn challenges typically involve finding security vulnerabilities in software or systems. Participants need to analyze the given scenario, understand the vulnerabilities present, and devise an exploit. The goal is to demonstrate the ability to think like a hacker and exploit weaknesses for educational purposes. The "Evil Corp" challenge allows participants to showcase their technical skills in a competitive environment. It helps assess participants' proficiency in reverse engineering, exploit development, and vulnerability analysis. Competing in such challenges can enhance participants' knowledge and practical skills in cybersecurity.

## Key Components:

The challenge incorporates essential elements, including a snippet of assembly code containing various security vulnerabilities, a target system with specific functionalities and flags to retrieve, exploitation techniques such as stack smashing and return-oriented programming (ROP), and a scoring mechanism that rewards participants based on the complexity of the vulnerabilities exploited.

## Types of Methodologies:

Common exploitation techniques in pwn challenges include buffer overflows, format string vulnerabilities, and use-after-free exploits. Participants may need to write or modify exploit code to gain control over the target system. Understanding memory management, assembly language, and debugging techniques are essential for success.

## Expected Outcomes:

The supposed outcomes this project will be a flag which is basically an exploited vulnerability in the code. By doing implementing various techniques.

## Implementation:

This project will first start with scanning for vulnerabilities in the given code. We can find the vulnerabilities by various techniques like using Nessus scanning techniques, Ghidra, burp suite etc.

After finding the vulnerability will be creating an exploitation code to start the exploitation process of exploitation against the given code. After running the code, we will be receiving a flag if the exploitation process is success. In our case we didn't able to get the flag, which means we are not successfully able complete the challenge.

## Conclusion:

The "Evil Corp" challenge offered us the opportunity to enhance our skills in reverse engineering, vulnerability assessment, and exploitation techniques. It served as a practical application of assembly code analysis, a fundamental skill for cybersecurity professionals. Additionally, the challenge promoted healthy competition and encouraged us to think creatively to solve complex security problems.