# 实验 8　CTF（Capture The Flag）夺旗赛

## 一、 实验目的

1、熟悉静态反汇编工具 IDA Pro；

2、熟悉动态反汇编工具 OllyDbg；

3、掌握对二进制代码内部逻辑关系的分析；

4、掌握对二进制代码的修改和保存。

## 二、 实验原理

### 1. CTF

CTF 是一种流行的信息安全竞赛形式，可意译为“夺旗赛”。其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。

CTF 竞赛模式具体分为以下三类：

一、解题模式（Jeopardy）

在解题模式 CTF 赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的 CTF 竞赛与 ACM 编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向分析、漏洞挖掘与利用、Web 渗透、密码、取证、隐写、安全编程等类别。

二、攻防模式（Attack-Defense）

在攻防模式 CTF 赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。

三、混合模式（Mix）

结合了解题模式与攻防模式的 CTF 赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。

### 2. 解题

Flag 隐藏在 game.exe 的二进制代码中。通过对 game.exe 的修改，使 game.exe 能够顺利的执行，完成对 Flag 的解密。

## 三、 实验报告

1. 逆向分析 game.exe 二进制代码的主要逻辑结构和重要数据。
2. 修改 game.exe 二进制代码，获得最后的 Flag。实验报告要说明逆向分析、代码修改的具体过程，以及最后获得的 Flag。
3. 实验报告的提交时间见雨课堂截止时间。