

# 攻防世界 Misc高手进阶区 7分题 传感器2

原创

思源湖的鱼  于 2021-02-04 15:29:34 发布  237  收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [crc](#) [misc](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_44604541/article/details/113642842](https://blog.csdn.net/weixin_44604541/article/details/113642842)

版权

## CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

### 前言

继续ctf的旅程

攻防世界Misc高手进阶区的7分题

本篇是传感器2的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

### 解题过程

题目描述

**题目描述:** 已知ID为0x8893CA58的温度传感器未解码报文为: 3EAAAAA56A69AA55A95995A569AA95565556 为伪造该类型传感器的报文ID (其他报文内容不变), 请给出ID为0xDEADBEEF的传感器1的报文校验位 (解码后hex), 以及ID为0xBAADA555的传感器2的报文校验位 (解码后hex), 并组合作为flag提交。例如, 若传感器1的校验位为0x123456, 传感器2的校验位为0xABCDEF, 则flag为flag{123456ABCDEF}。

根据传感器1的结果, 可以分析出来, 编码的可以分为0024D {ID}41{校验位}

0024D 8893CA58 41 81

0024D 8845ABF3 41 19

由于校验位是8位二进制所以猜测是CRC8

```
#!/usr/bin/python
```

```
def crc(x,y):  
    while(x>y):  
        l = len(bin(x)) - len(bin(y))  
        t = int(bin(y)[2:]+ '0'*l,2)  
        x ^= t  
    return x  
m = 0  
for i in range(0x200):  
    if i < 100:  
        continue  
    if crc(0x24d8893ca584100,i) == 0x81 and crc(0x24d8845abf34100,i) == 0x19:  
        m = i  
        print i  
        break  
print hex(crc(0x00024ddeadbeef4100,m))  
print hex(crc(0x00024dbaada5554100,m))
```

```
263  
0xb5  
0x15
```

得到flag: `flag{b515}`

## 结语

CRC