

# 攻防世界 Reverse高手进阶区 2分题 Guess-the-Number

原创

[思源湖的鱼](#) 于 2020-12-01 13:59:09 发布 97 收藏

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

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/110381880](https://blog.csdn.net/weixin_44604541/article/details/110381880)

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Reverse高手进阶区的2分题

本篇是Guess-the-Number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

下下来一个jar

扔进jd-gui

```
6a8bee79ee404194bb8a213a8a0e211d.jar
META-INF
MANIFEST.MF
guess.class
guess
  XOR(String, String) : String
  guess()
  main(String[]) : void

import java.math.BigInteger;

public class guess {
    static String XOR(String _str_one, String _str_two) {
        BigInteger i1 = new BigInteger(_str_one, 16);
        BigInteger i2 = new BigInteger(_str_two, 16);
        BigInteger res = i1.xor(i2);
        String result = res.toString(16);
        return result;
    }

    public static void main(String[] args) {
        int guess_number = 0;
        int my_num = 349763335;
        int my_number = 1545686892;
        int flag = 345736730;
        if (args.length > 0) {
            try {
                guess_number = Integer.parseInt(args[0]);
                if (my_number / 5 == guess_number) {
                    String str_one = "4b64ca12ace755516c178f72d05d7061";
                    String str_two = "ecd44646cfe5994eb35bf922e25dba";
                    my_num += flag;
                    String answer = XOR(str_one, str_two);
                    System.out.println("your flag is: " + answer);
                } else {
                    System.err.println("wrong guess!");
                    System.exit(1);
                }
            } catch (NumberFormatException e) {
                System.err.println("please enter an integer \nexample: java -jar guess 12");
                System.exit(1);
            }
        } else {
            System.err.println("wrong guess!");
            int num = 1000000;
            num++;
            System.exit(1);
        }
    }
}
```

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

分析一下就是两串字符XOR就得到flag

或者满足下判断条件输入 **309137378**

然后就能得到flag

## 结语

简单题



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)