

Week 2 MISC Write Up

easy password

描述

听说你们有人喜欢暴力解题，那么就来暴力一下，测测电脑性能吧。

hint:小写字母+数字

这题还要啥wp，丢进AZPR暴力跑一会就出来了，反正应该没人比我花的时间长orz。

```
hgame{0pos_You_Sound_m3_HAHA}
```

mysterious file header

描述

hint 1: order, in order?

hint 2: 怎么才能够运行它呢

hint 3: 四个数字排在一起可能是什么呢，Web选手一看就知道

hint 4: $4 \times 3 \times 2 \times 1 = 24$

讲真，这题纯属是为了提高难度才这样出的。出了些脑洞给一些选手带来了不适，对此我感到十分偷税（逃

不过我hint都给到了这份上了，应该还是有些人有思路的。

这题主要是为了让你们分清docx zip jar文件格式之间的略微区别才出的，不过第二周分数不能那么低，出题人又懒得出题，嘛实际结果就是只有13人做出来。。。。。

不管怎样，遇到这种文件先binwalk看一下，会发现有zip结束标志，接着加上扩展名为zip打开，发现应该是个jar文件，于是改成jar运行一下会发现运行不了，那么就要去看看是哪里出了问题，这里可能会有些同学Java环境的classpath路径没配好，导致运行不了。。这就不是出题人的锅了sigh~

和正常的jar文件对比一下会发现文件头不一样，那么根据hint1我们就可以改一下文件头为50 4b 03 04这样就能成功运行了。好第一步就做出来了

运行之后会发现有四个按钮，都点一遍后只会显示4个不同的数字，那么根据hint3，对数字敏感的话应该会猜出这四个数字应该是ip，不过这里测题的时候有人说太简单了，那么我就直接把ip打乱了顺序，于是才有了hint4，它的意思是一共有24种可能，不过我看交上来的wp里有人猜一猜，就知道肯定是以118开头的orz，大佬们的思路真是高端，学生机伤不起，找到正确ip后进入第一篇文章结尾拿到flag

```
hgame{Y0u_Mu5t_know_f1le_header_and_java}
```