Writeup

2.

直接代码审计，查手册后，$c=trim（file\_get\_contents($b)）：去掉变量b的收尾字母赋值给c，

Isset检测a是否为空

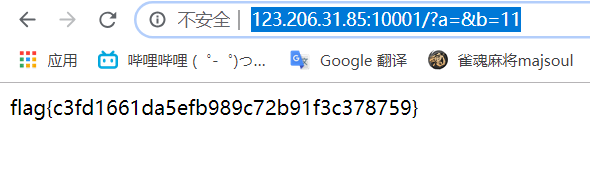
如果a=c则显示flag

B先初始化后，再get值，导致了b可以被再次赋值



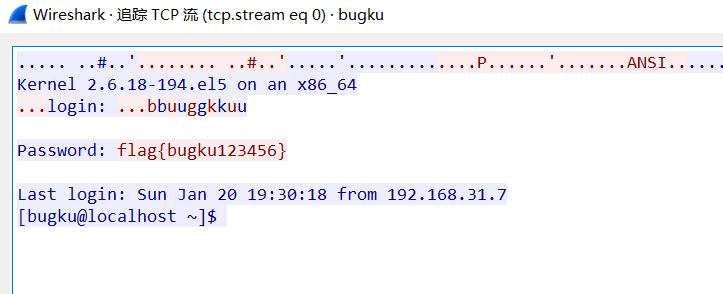
构造<http://123.206.31.85:10001/?a=&b=11>

出flag



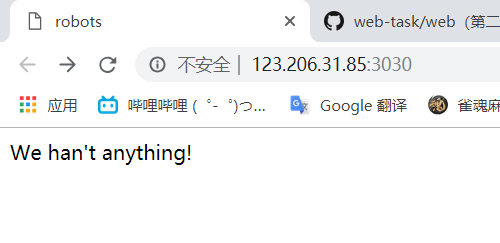
3.代码审计

Wireshark追踪tcp流

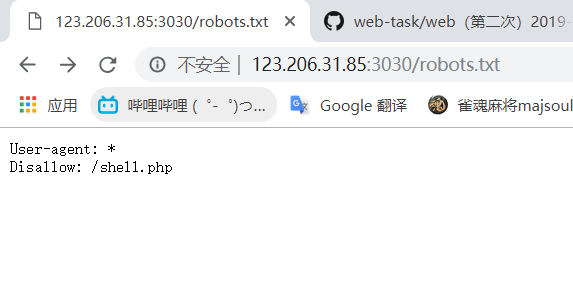


4.

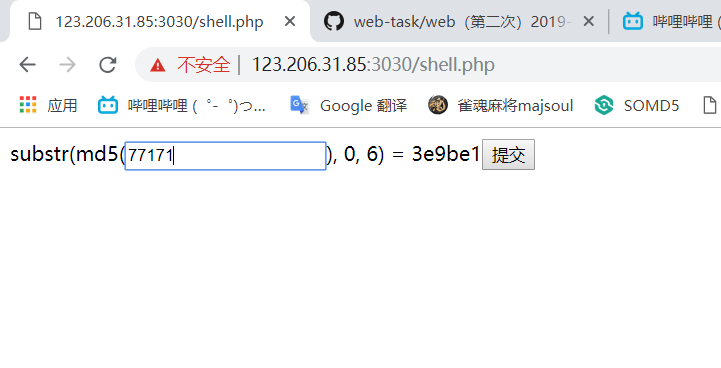
页标签为robots



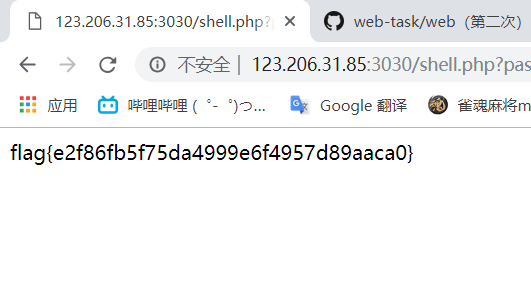
访问robots.txt



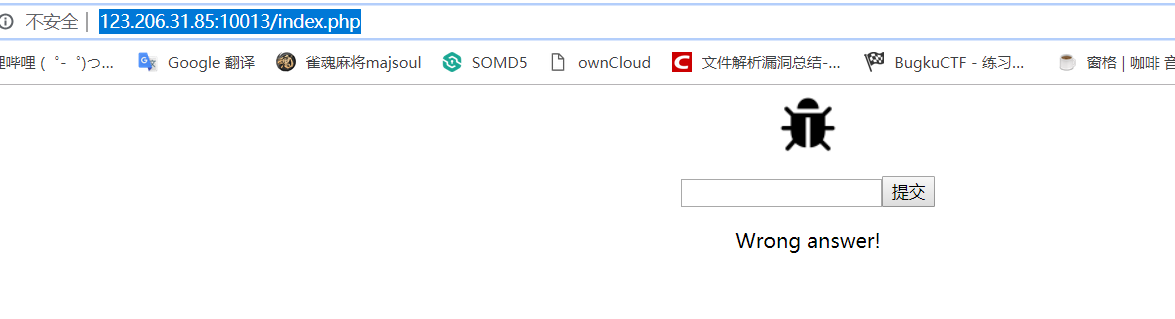
访问shell.php



MD5解密，提交

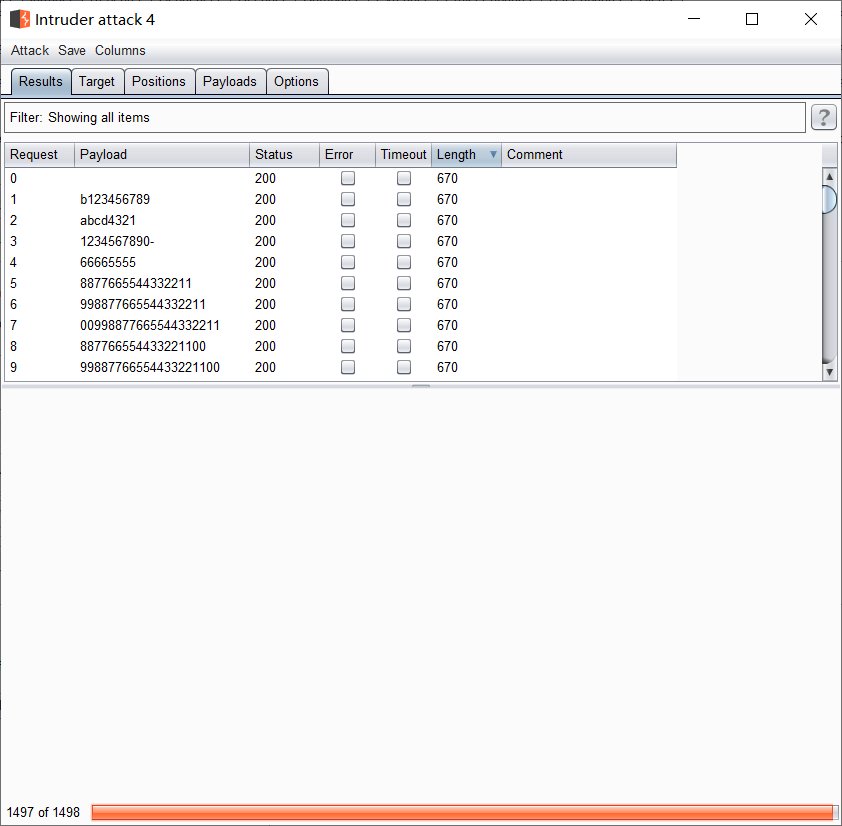


5

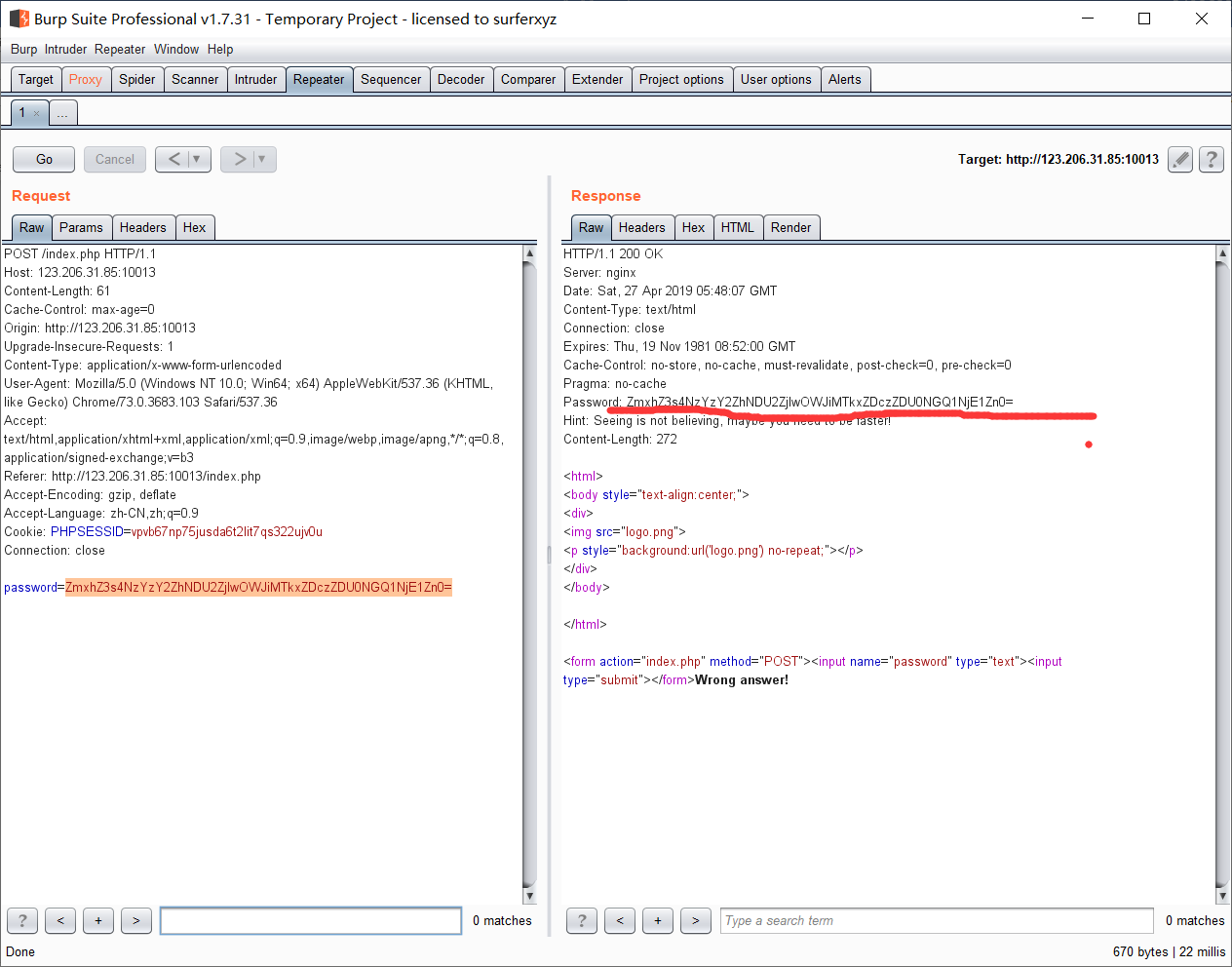


没有思路，

无脑爆破



无果，抓包分析



回包里有有趣的东西，提交



报错，

Base64转码

