HGAME Week2 Writeup

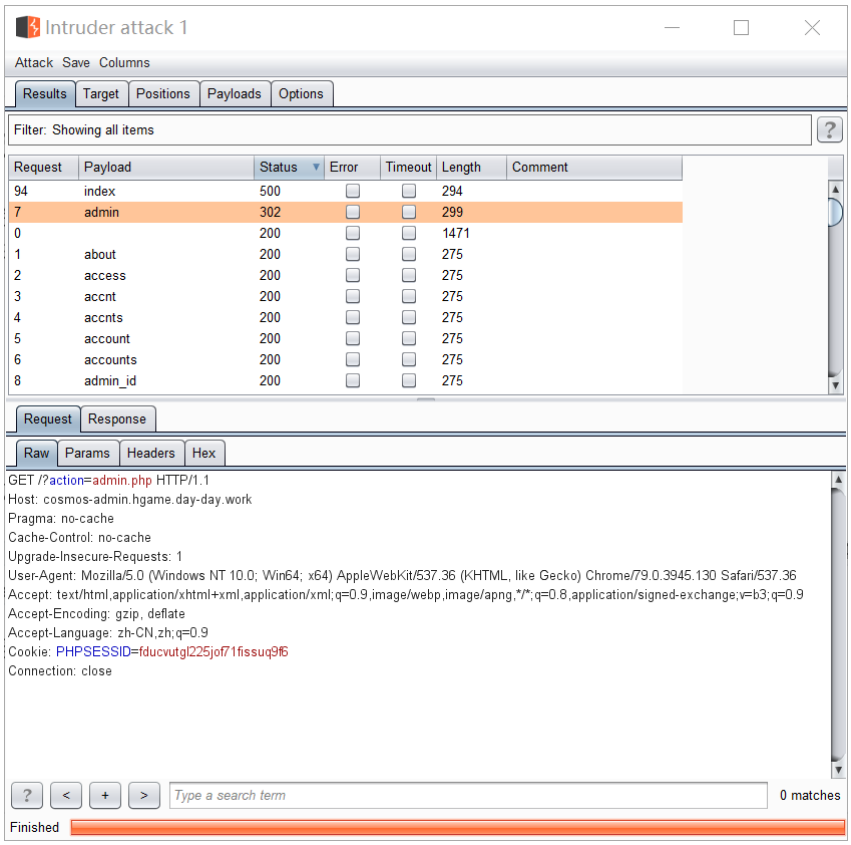
（我还是太菜了555...

WEB

Cosmos的博客后台

看这吸引人的后台登录界面，一开始还以为是SQL注入，结果在注入了好久之后才得知不是注入。根据题意，估计是从获取php入手。

用bp和一份网上搞到的网站常用目录进行intruder爆破，得到admin.php存在重定向，说明这就是我们获取php源码的目标



用php://filter获取base64加密过的php源码

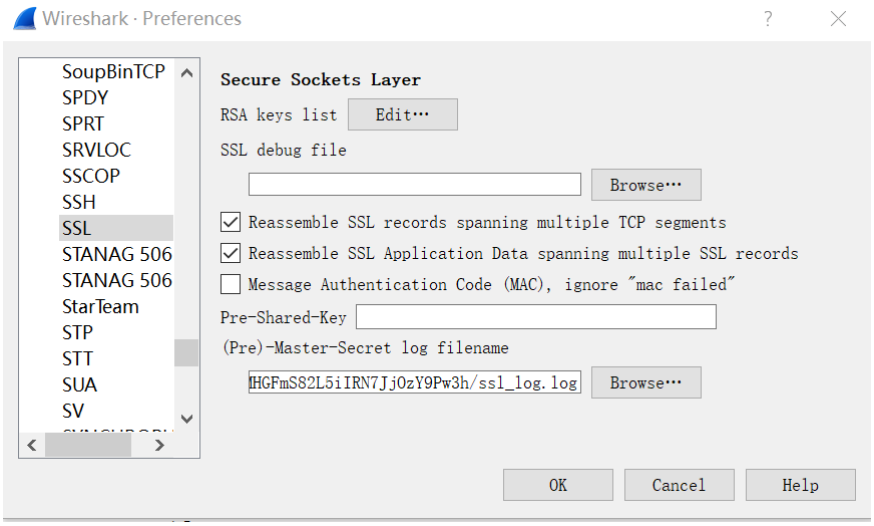
`http://cosmos-admin.hgame.day-day.work/?action=php://filter/read=convert.base64-encode/resource=admin.php`

base64解密后得到php源码，然后就分析了一通....还是没得出结果，看来得恶补一下php了.....

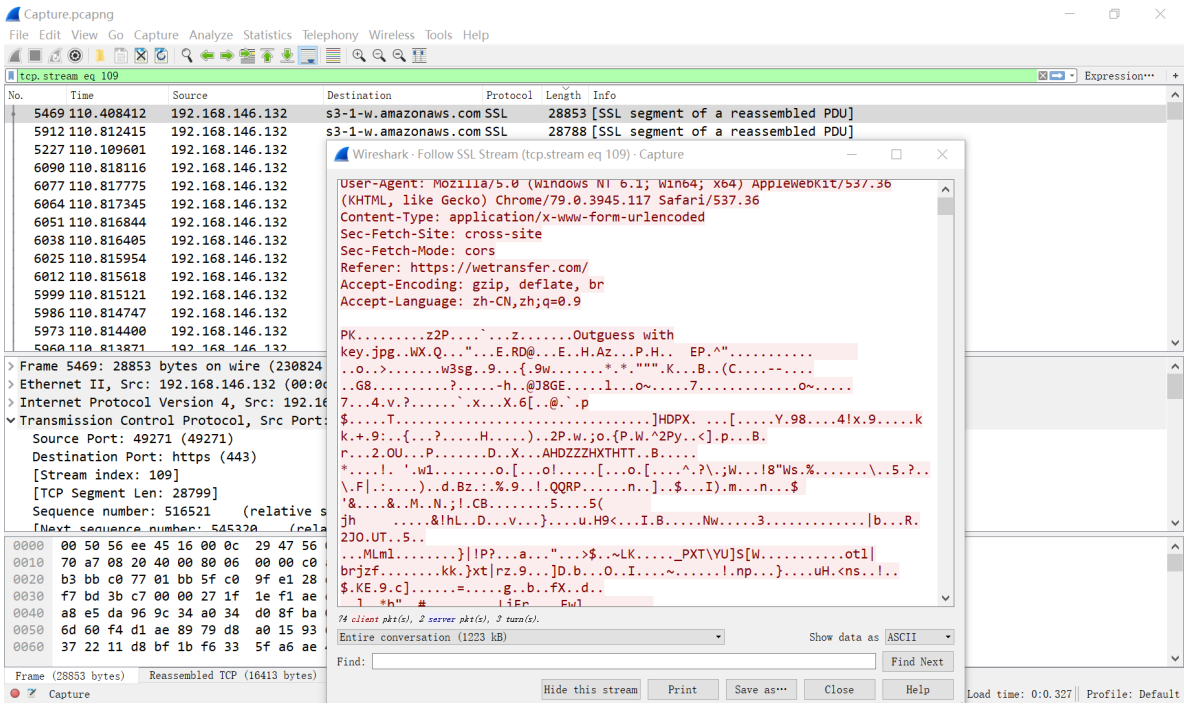
MISC

Cosmos的午餐

打开压缩包发现.pcapng文件和.log文件，利用谷歌学习了一下SSL加密的原理以及在wireshark中如何用.log文件解密



用.log秘钥配置好Wireshark中SSL协议后，将流量包按长度降序排序，得到最大的流量包后跟踪SSL流，又看到了熟悉的PK...开头标示。



按上周同样的操作丢进010editor去头去尾得到zip压缩包，解压得到图片。又根据题目的提示：Cosmos喜欢往图片备注塞东西，就右键属性看到备注中有key。

结合图片的名称outguess with key，谷歌后可以知道outguess是隐写的一种（一开始还没想到是隐写，谷歌搜的时候纯粹主要是想知道outguess这个单词啥意思.....结果一搜就搜出来了

```
root@LAPTOP-4B5UOOVR:~/src/hgame# outguess -k gUNrbbdR9XhRBDGpzz -r ana.jpg
Reading ana.jpg....
Extracting usable bits:   1161827 bits
Steg retrieve: seed: 3, len: 24
```

得到隐写的内容：一个地址，打开后下载压缩包，再打开就是二维码，扫出flag

所见即为假

一开始看到对联还以为要用二进制之类的，后来再看压缩包名字AllFake，以及题目根本没提示密码在哪，可以想到这其实是个伪加密（还好上周学改文件十六进制文件的时候有关注到，这次马上就反应过来了）。打开010editor将伪加密修改掉，得到不需要密码的压缩包，解压得到图片Flag_In_Picture，同时根据提示F5 key，谷歌一下之后可以知道是F5图片隐写。

用F5-steganography工具提取出得到16进制字符串，转换为文本得到flag