IDF实验室 抓到一只苍蝇 WriteUp

转载

weixin_33961829 于 2015-05-17 15:06:00 发布 66 收藏
文章标签： php
原文链接：http://www.cnblogs.com/smallnight/p/4509740.html

题目链接：http://ctf.idf.cn/index.php?g=game&m=article&a=index&id=57

WriteUp: 下载下来是个网络抓包文件，使用WireShark打开，查看网络通讯过程，第13号报文为POST，提交数据为

```
{"path":"fly.rar","appid":"","size":525701,"md5":"e023afa4f6579db5becda8fe7861c2d3","sha":"ecccba7aea1d48268437
```

上传了fly.rar，知道文件长度和校验和。

通过Edit-Find Packet查找Rar!（Rar文件头），Search in Packet bytes，得39号报文，其在163号重新组装。

通过File-Export Objects-HTTP，第163、289、431、577、729号报文都是通过HTTP传输了字节流，保存文件001，002....

用WinHex打开001，呃，文件头并不是Rar!，估计上传的时候会有校验和之类的吧，把Rar!前面0x16C个字节去掉，对其他文件作同样处理，然后合并为一个文件flag.rar。

flag.rar，7zip直接报错，有没有搞错。用WinRar打开，提示加密文件和文件头损坏，难道文件有错误，校验了MD5，一样的，so，到处找密码，找不到啊！！！

无奈下去翻讨论记录，有人提到伪加密，去Rar官网下文件格式描述（4.0的安装有包含），先跳过MAIN_HEAD，来到File header，HEAD_FLAGS的定义为0x04为加密文件，将0x17的0x84改为0x80，保存后就可以正确解压了。

解压后是一个在屏幕跑苍蝇的程序Orzzzzzzz，WinHex看到文件尾有个PNG什么的，提取出来，是张二维码，扫一扫得flag。

转载于:https://www.cnblogs.com/smallnight/p/4509740.html