研究生创新联盟高校首届“卓朗杯”研究生网络与信息安全技术大赛河北省选拔赛部分WP

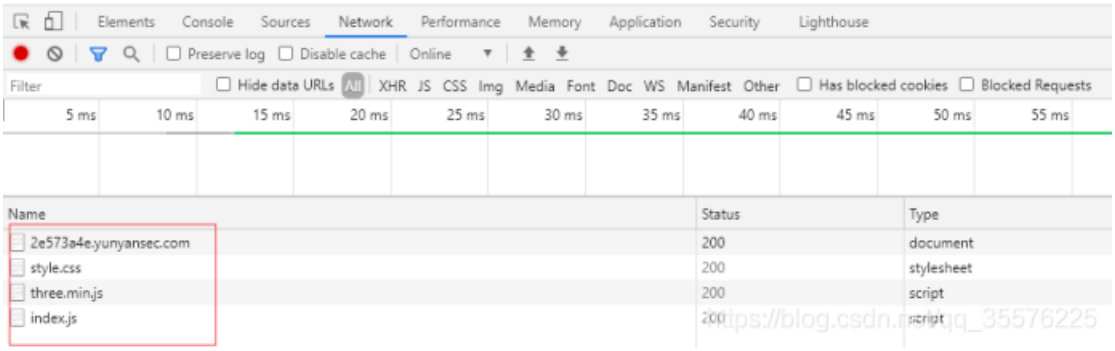
原创

爱吃素的武士 于 2020-10-26 16:57:54 发布 1403 收藏 3
分类专栏： ctf

本文链接：https://blog.csdn.net/qq_35576225/article/details/109292938

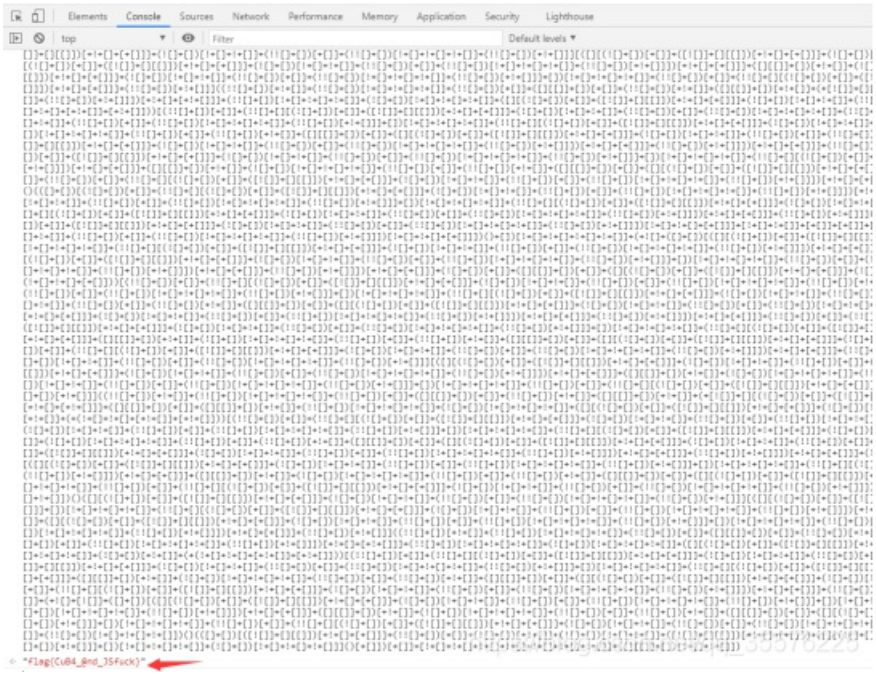
题目一 签到题

点击F12进入开发者模式，重新访问网页，得到几个样式文件。



在样式文件index.js中搜索flag，发现

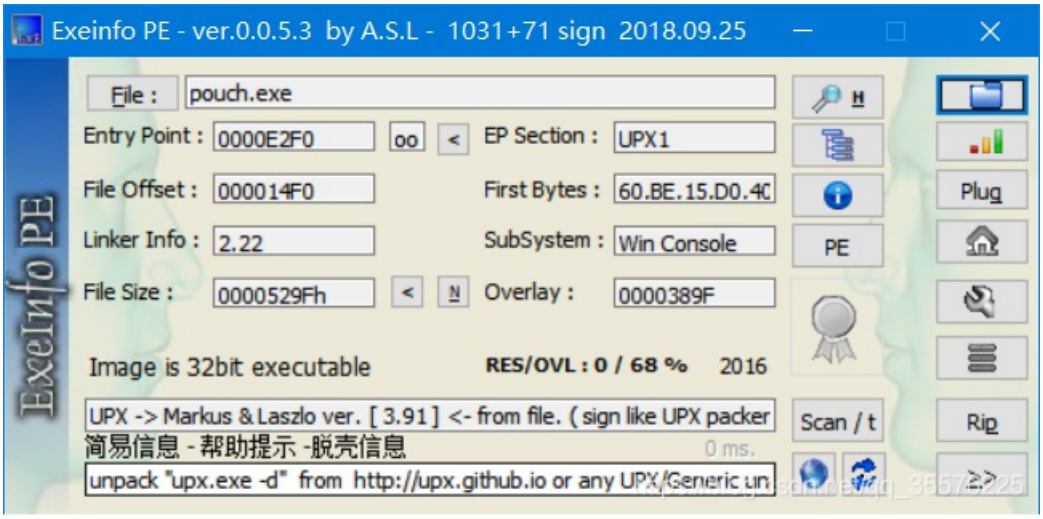
将这串代码复制到console控制台执行，得到最后的flag



flag{CuB4_@nd_JSfuck}

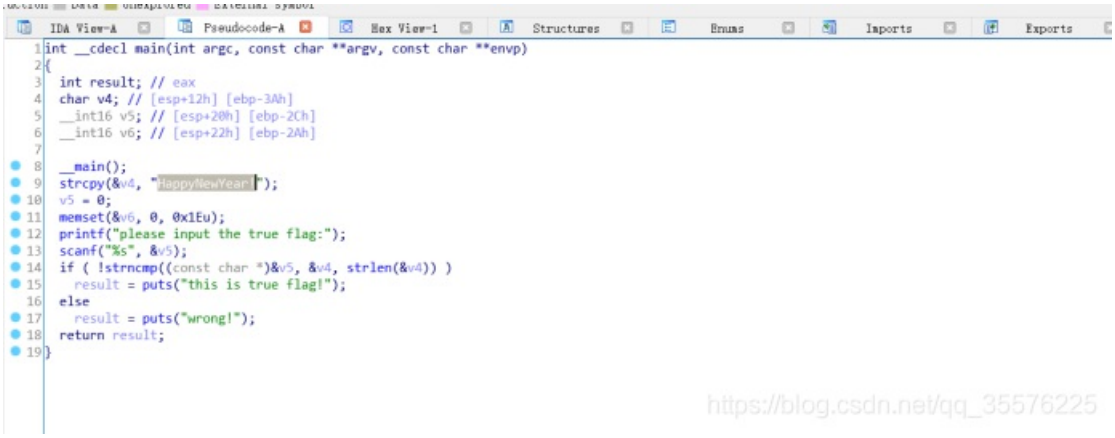
题目二 re1

1. （用Exeinfo PE查看发现用upx.exe加壳了。



2.用 upx.exe -d 指令去壳

3.用ida pro转为伪汇编



分析代码发现flag就是”HappyNewYear!”

题目三 密码学1

Base16解码

Base32解码

Base64解码

Base91解码，获取flag。

flag{base_n0t_3asy}

题目四 安卓1

解压apk，使用dex2jar软件反编译classes.dex编译成jar文件，然后使用jd-ui软件查看代码，搜索flag{，在MainActivity的showMessageTask中，找到flag的结果是当cnt=1000次之后既可以弹出正确结果，所以使用软件修改smali文件，让cnt=1，只需要胜利一次既可以弹出flag.

flag{107749}

题目五 misc1

用dtmf2num音频解码：

45774391614390919680552035340229102217126562041792203410479326635706552497458

16进制：

65336335336362656339366561386264653063323934653532306233376135 32

字符串：e3c53cbec96ea8bde0c294e520b37a52

flag{e3c53cbec96ea8bde0c294e520b37a52}

题目六 密码学2

从文件中看到有n1,n2,n3和c1,c2,c3，n很大，e很小，分析是低加密指数广播攻击，通过不同的模数得到不同的密文。

flag{8c17fb02684fa73e6a296a89b63b56bf}

题目七 misc4

解压文件，得到xxx,，添加拓展名.zip，解压得到word文件，通过vnc解密，得到解压密码!QAZ2wsx，将得到的文档转为zip格式再解压，得到一堆文件夹，打开word里的document.xml，在最后几行得到MZWGCZ33GY4TQZBVGFQTCOLEHBQTCMRRMNSTKOBRGQ4TSZBXMI3TAMJWGY4H2===，通过base32解码即可

flag{698d51a19d8a121ce581499d7b701668}