攻防世界题目练习--MISC新手关（7~12）

原创

一日三省小白 于 2019-10-26 00:02:14 发布 5470 收藏 10
分类专栏： 小白

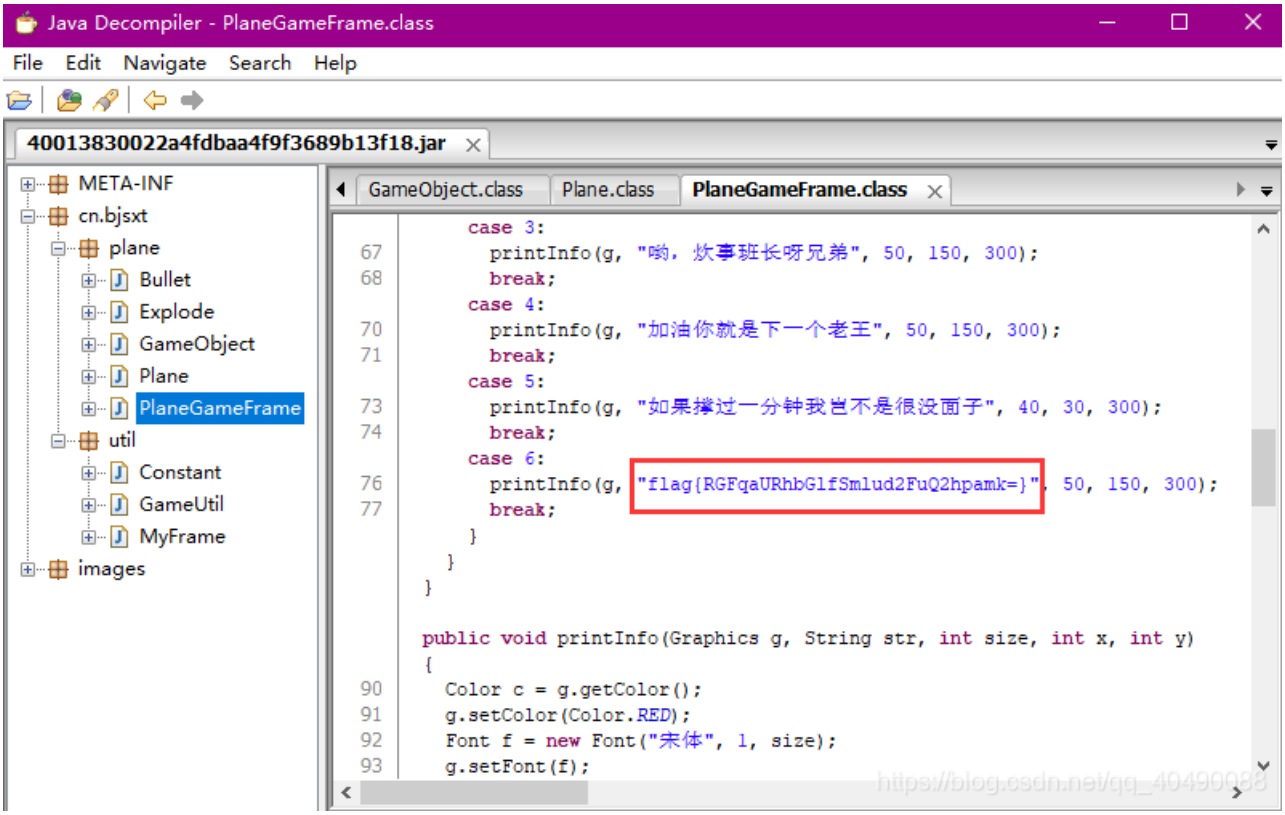
题目地址：攻防世界MISC

题目7：坚持60s

题目描述：菜狗发现最近菜猫不爱理他，反而迷上了菜鸡

解决：

一个jar包，利用java的反编译工具jd-gui打开jar包，可在PlaneGameFrame类中找到flag

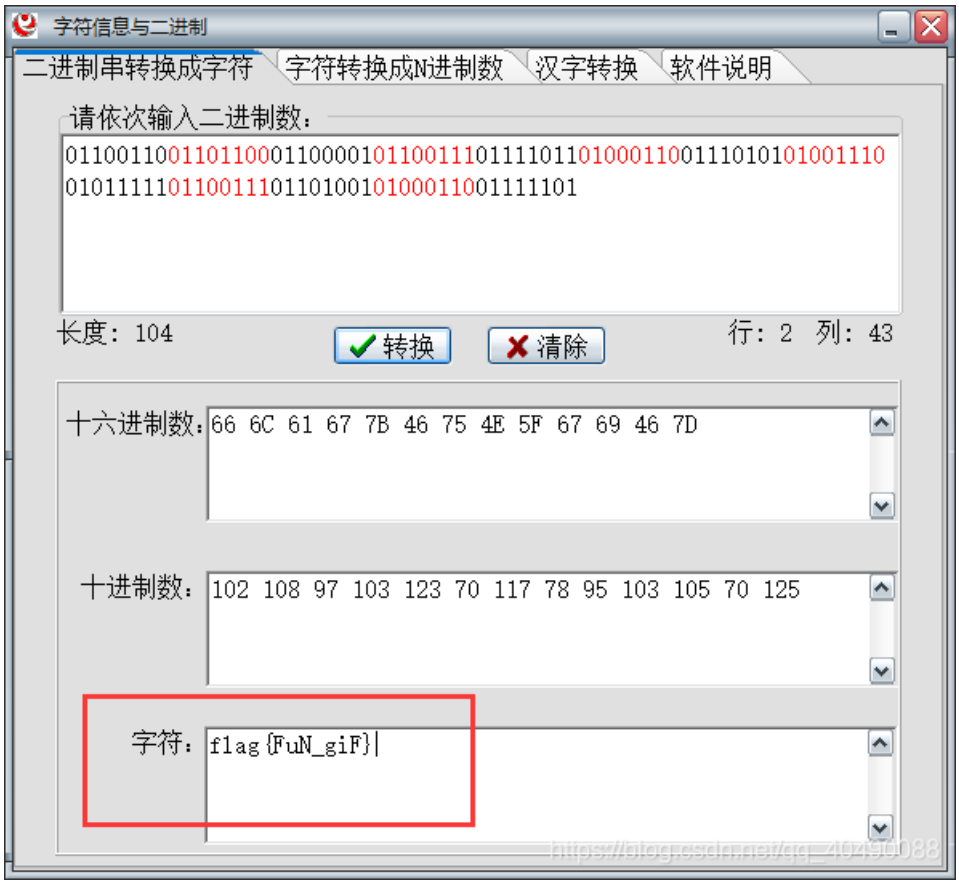


题目8：gif

题目描述：菜狗截获了一张菜鸡发给菜猫的动态图，却发现另有玄机

解决：

下载后发现是一个压缩包，解压后，有104张图，都是黑白图组成的，非此即彼，类似于二进制，视白色图为0，黑色图为1，得到一长串二进制编码，通过工具转换为字符串，得到flag



题目9：掀桌子

题目描述：菜狗截获了一份报文如下

c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e

生气地掀翻了桌子(ノ °□°）ノ ︵ ┻━┻

解决：

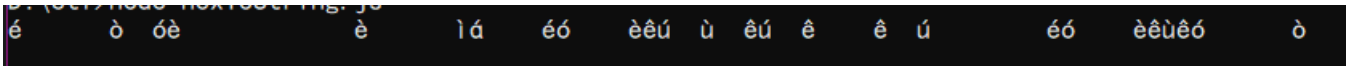
一串十六进制编码，两两一位，转换成十进制，再根据ASCII码转换为字符

写一段js脚本，运行一下

```
function hexToStr(hexStr) {
    var hexArr = hexStr.substr(2);
    var len = hexArr.length;
    var curCharCode;
    var resultStr = [];
    for(var i = 0; i < len;i = i + 2) {
        curCharCode = parseInt(hexArr.substr(i, 2), 16);
        resultStr.push(String.fromCharCode(curCharCode));
    }
    return resultStr.join("");    //字符数组->字符串
}

var str = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3
console.log(hexToStr(str));
```


是乱码..因为每个转换后的ASCII码值都大于127，不是有效字符

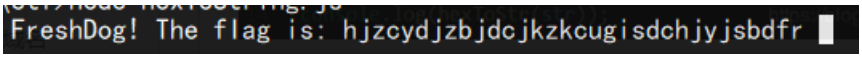


试着将每个转换后的十进制先减去128，再转为字符

```
function hexToStr(hexStr) {
    var hexArr = hexStr.substr(2);
    var len = hexArr.length;
    var curCharCode;
    var resultStr = [];
    for(var i = 0; i < len;i = i + 2) {
        curCharCode = parseInt(hexArr.substr(i, 2), 16)-128;
        resultStr.push(String.fromCharCode(curCharCode));
    }
    return resultStr.join("");    //字符数组->字符串
}

var str = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8e
console.log(hexToStr(str));
```


再运行一遍



可看到flag值

题目10：如来十三掌

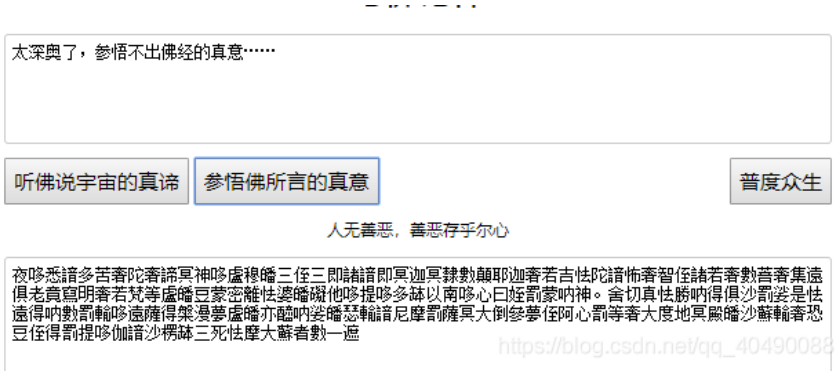
题目描述：菜狗为了打败菜猫，学了一套如来十三掌。

解决：

下载后发现为一串看不懂的文字，网上搜索发现有一个“与佛论禅”的网站，应该可以解密

网站地址：与佛论禅

开始直接粘贴进去，好像解不了..



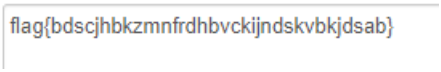
之后尝试白话转“佛说”

发现格式要在前面加上佛曰：

第一反应将其进行BASE64解密，但是解码失败，据题意，十三...ROT13编码。

将其先ROT13再加密一次即解密，之后再进行BASE64解码

得到flag值



BASE64解码网址：http://tool.oschina.net/encrypt?type=3

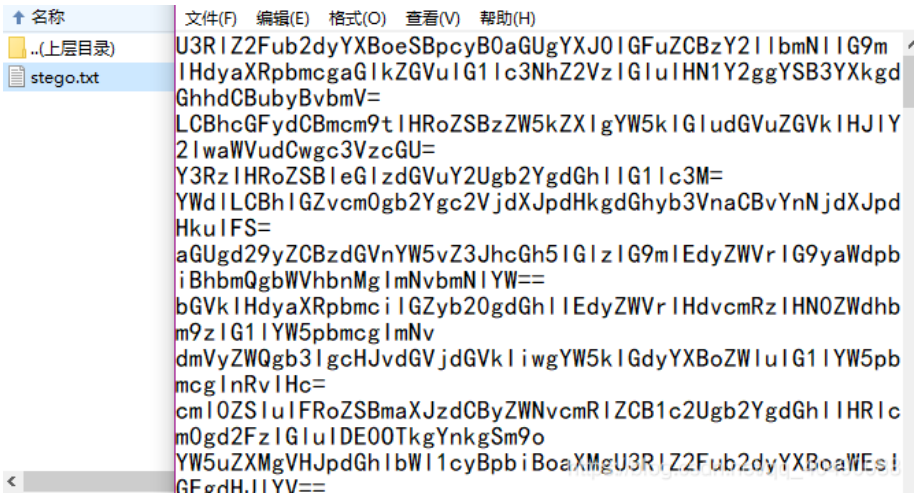
ROT13解码网址：https://www.jisuan.mobi/puzzm6z1B1HH6yXW.html

题目11：base64stego

题目描述：菜狗经过几天的学习，终于发现了如来十三掌最后一步的精髓

解决：

如来十三掌的最后一步，即BASE64解密，在压缩软件里打开这个文件



发现有很长的BASE64编码。

...查看writeup后，涉及到BASE64隐写

原理与题解参照一位大神博客：https://www.tr0y.wang/2017/06/14/Base64steg/

题目12：功夫再高也怕菜刀

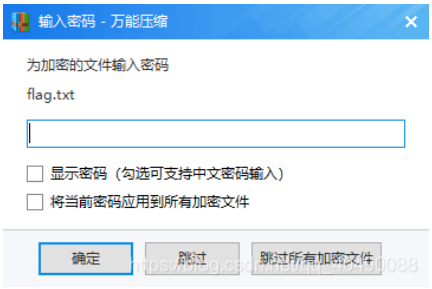
题目描述：菜狗决定用菜刀和菜鸡决一死战

解决：

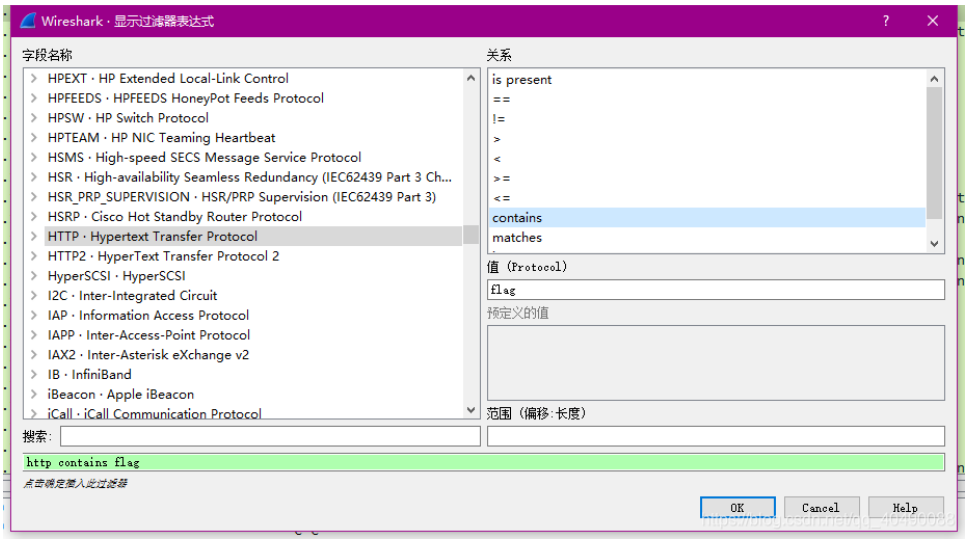
（查看了别人的writeup...）

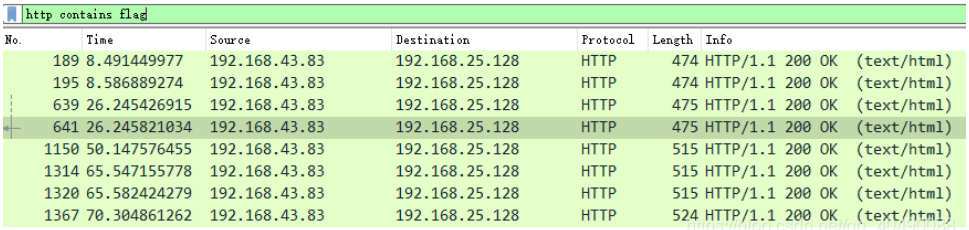
将该文件拖到foremost应用程序上，用foremost分离文件中的隐藏文件，输出结果为一个压缩文件

打开发现解压需要密码



用wireshark打开该pcapng数据包，通过表达式搜索流量包中是否有flag





http contains flag

No.	Time	Source	Destination	Protocol	Length	Info
189	8.491449977	192.168.43.83	192.168.25.128	HTTP	474	HTTP/1.1 200 OK (text/html)
195	8.586889274	192.168.43.83	192.168.25.128	HTTP	474	HTTP/1.1 200 OK (text/html)
639	26.245426915	192.168.43.83	192.168.25.128	HTTP	475	HTTP/1.1 200 OK (text/html)
641	26.245821034	192.168.43.83	192.168.25.128	HTTP	475	HTTP/1.1 200 OK (text/html)
1150	50.147576455	192.168.43.83	192.168.25.128	HTTP	515	HTTP/1.1 200 OK (text/html)
1314	65.547155778	192.168.43.83	192.168.25.128	HTTP	515	HTTP/1.1 200 OK (text/html)
1320	65.582424279	192.168.43.83	192.168.25.128	HTTP	515	HTTP/1.1 200 OK (text/html)
1367	70.304861262	192.168.43.83	192.168.25.128	HTTP	524	HTTP/1.1 200 OK (text/html)

筛选出这些流量包，逐个右击选择跟踪TCP流，查看完整的数据流中数据包的信息

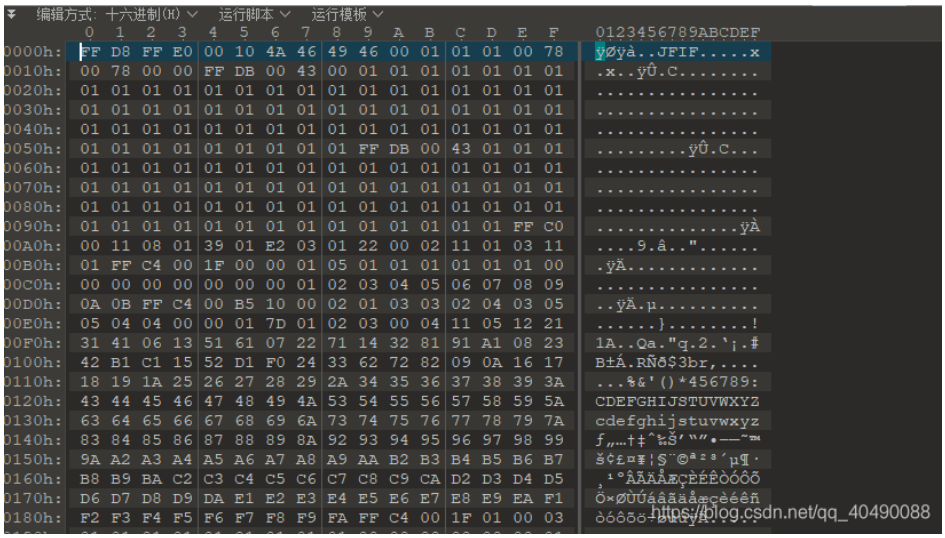
在第1150个包中发现巨长串十六进制编码，观察到结尾为FFD9，为jpg格式的文件结束标志

所以在前面的编码中寻找FFD8(jpg文件头标识)

```
aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTt
Ac2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskZj1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JGM9JF9Q
T1NUWyJ6MiJdOyRjPXN0cl9yZXBsYWNlKCJcciIsIiIsJGMpOyRjPXN0cl9yZXBsYWNlKCJcbiIsIiIsJGMpOyRidWY9IiI7Zm9yKCRpPTA
7JGk8c3RybGVuKCRjKTskaSs9MikkYnVmLj11cmxkZWNvZGUoIiUiLnN1YnN0cigkYywkaSwyKSk7ZWNobyhAZndyaXRlKGZvcGVuKCRmLC
J3IiksJGJ1Zik%2FIjEiOiIwIik7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc%3D&
z2=FFD8FFE000104A46494600010101007800780000FFDB00430001010101010101010101010101010101010101010101010101010101
0101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101FFDB00430101010101010101010101010
1010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101FF
C0001108013901E2030122000211010311 01FFC4001F0000010501010101010100000000000000000102030405060708090A0BFFC40
0B5100002010303020403050504040000017D01020300041105122131410613516107227114328191A108234281C11552D1F0243362
7282090A161718191A25262728292A3435363738393A4344454647484 94A535455565758595A6364656667686 96A737475767778797
```

将FFD8，FFD9之间的内容复制下来，保存在文本文件(txt)中

打开010Editor，选择导入十六进制文件



导入后，选择保存为jpg格式的文件。

查看该图片，看到图片中间有一串字符（理解为...This is password）

猜测为解压密码，尝试后，解压成功，得到一个flag.txt文件