超菜鸟级ctf5

原创

恋物语战场原 于 2019-05-18 23:11:13 发布 2056 收藏 2

分类专栏： CTF 文章标签： ctf 菜鸟级别

本文链接：https://blog.csdn.net/qq_26406447/article/details/90321995

超菜鸟级ctf5

前言

这次的题整体也比较简单，感觉密码题可能多了点

题目

门太低了

这道题前面也做过类似，考查xss，查看源码也能看到提示xss，这里script必须小写，大写还不行…没什么意思的题啊

New Swan Stone Castle

这中sql注入已经做了很多了，sqlmap都是可以直接跑出来的

这里手工注入的话要闭合括号和双引号。能用sqlmap直接不调参就跑出来，意义也不大啊

可以参考超菜鸟级ctf4

the Great Wall

这道题也是sqlmap直接跑出来，—level 3跑出来的，（2没试）

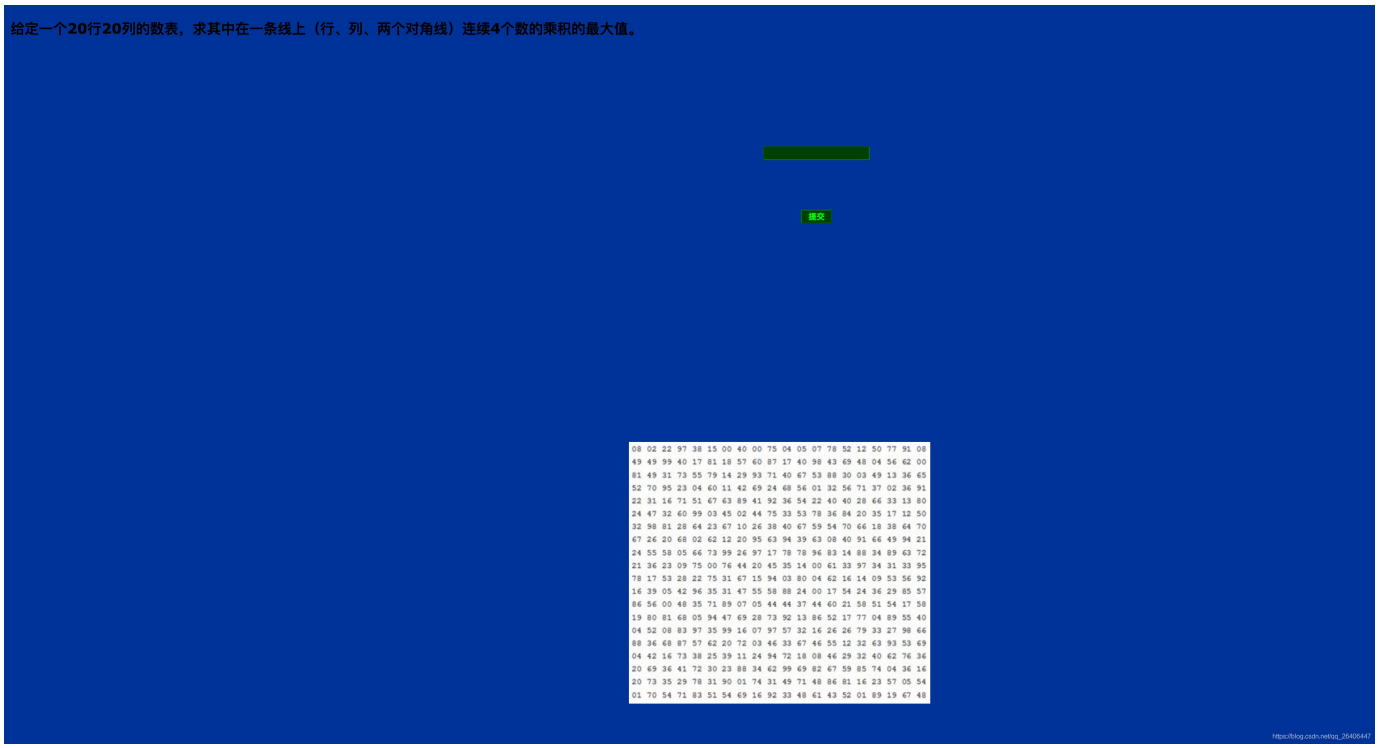
手工的话也是要闭合双引号和括号，手工的话可以尝试万能密码

门加锁了

这道题就是禁用了右键

f12检查元素或者ctrl+u查看源码就OK了

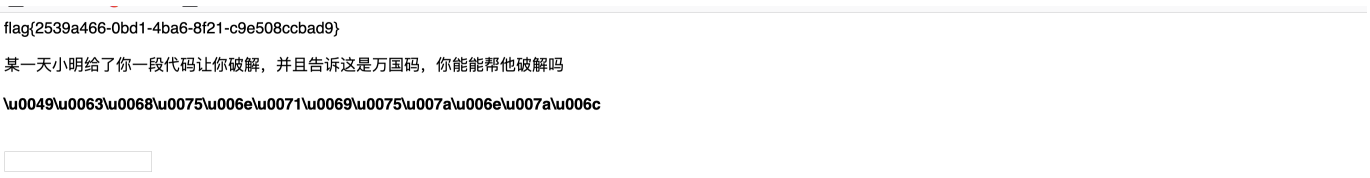
乘积最大值比较算法



这道题和前面做过的题类似主要考查写脚本能力吧

万国码

很明显的unicode编码，解码后输入，就如下图出flag很没意思



致敬经典

这道题当时猜出是凯撒密码了，简单做了一个脚本跑了下发现不对就放弃了...

lrua{1uy3yj9l-yw9u-48j2-uuj8-36h03706y7u7}

这张图片在网上进行识别可以发现是凯撒

这里双数字母向左偏移6位，单数字母向右偏移6位…当时没想到要这样分类…

藏宝图

这里是有一张没能成功显示的图片，这里直接对其进行下载，打开文件可以发现是一串base64加密的字符串解码后得到flag

藏宝图

小明和小军，得到一张藏宝图。勇士，请根据他们的藏宝图找到宝藏吧

逆向解密

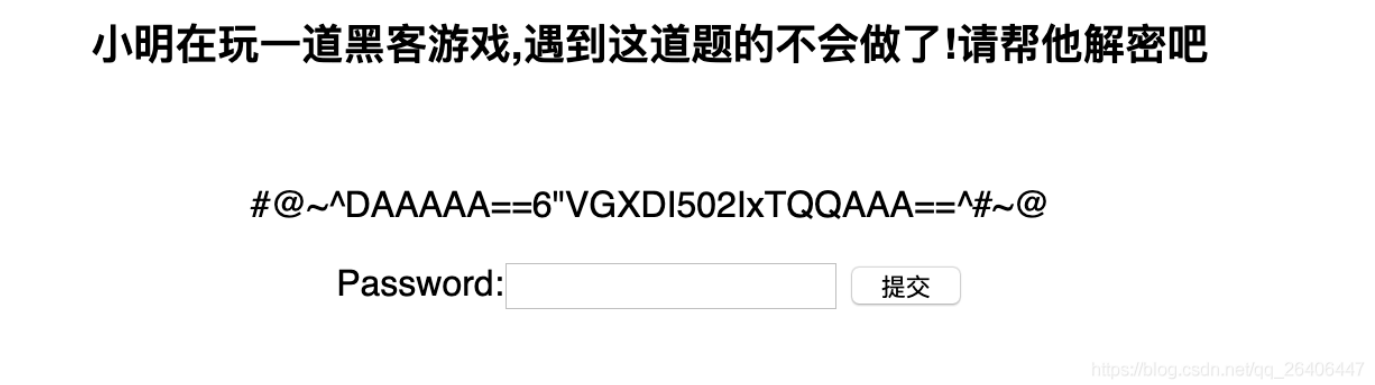
查看源码会提示psw.php，访问得到php源码

```php
<?php
    highlight_file( __FILE__ );
    function encode($string,$option='encode'){
        if ($option=='encode') {

            $lenght=strlen($string);

            for ($x=0;$x<$lenght;$x++) {

             @$tmp=substr($string,$x,1);

             $ord=ord($tmp)+10;

             @$result=$result.chr($ord);
        }
        echo $result.'</br>';


    }elseif($option=='decode'){

        }
    }
    encode('_Y^kdg_k','decode');
?>
```

我没看到这里的意思，答案的意思是下面的encode里的参数是加密过的，然后需要我们来完善decode部分的代码来实现逆向解密…做题的时候确实是没有理解到题的意思…当然php自己也不熟…

神秘代码

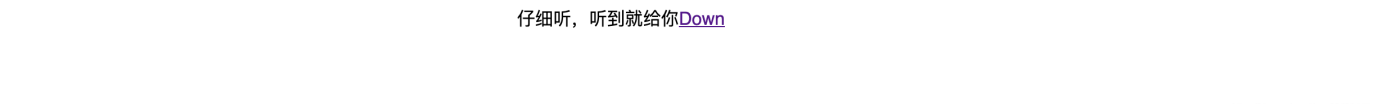
确实是对密码这块不是很熟，看到后以为是base64…



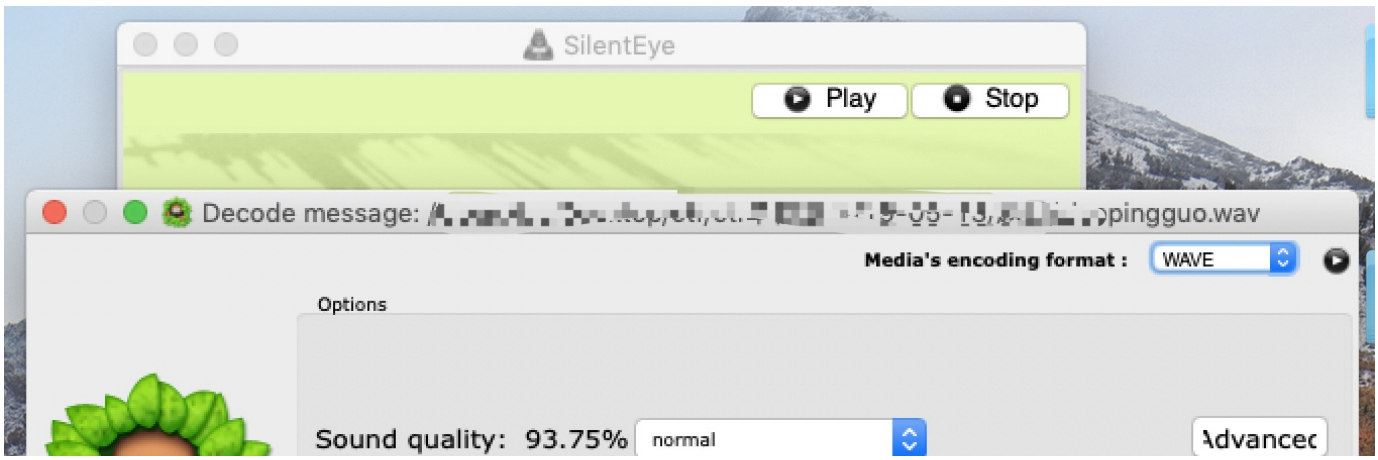
答案说是VBScript编码，在线解码后提交就能得到flag

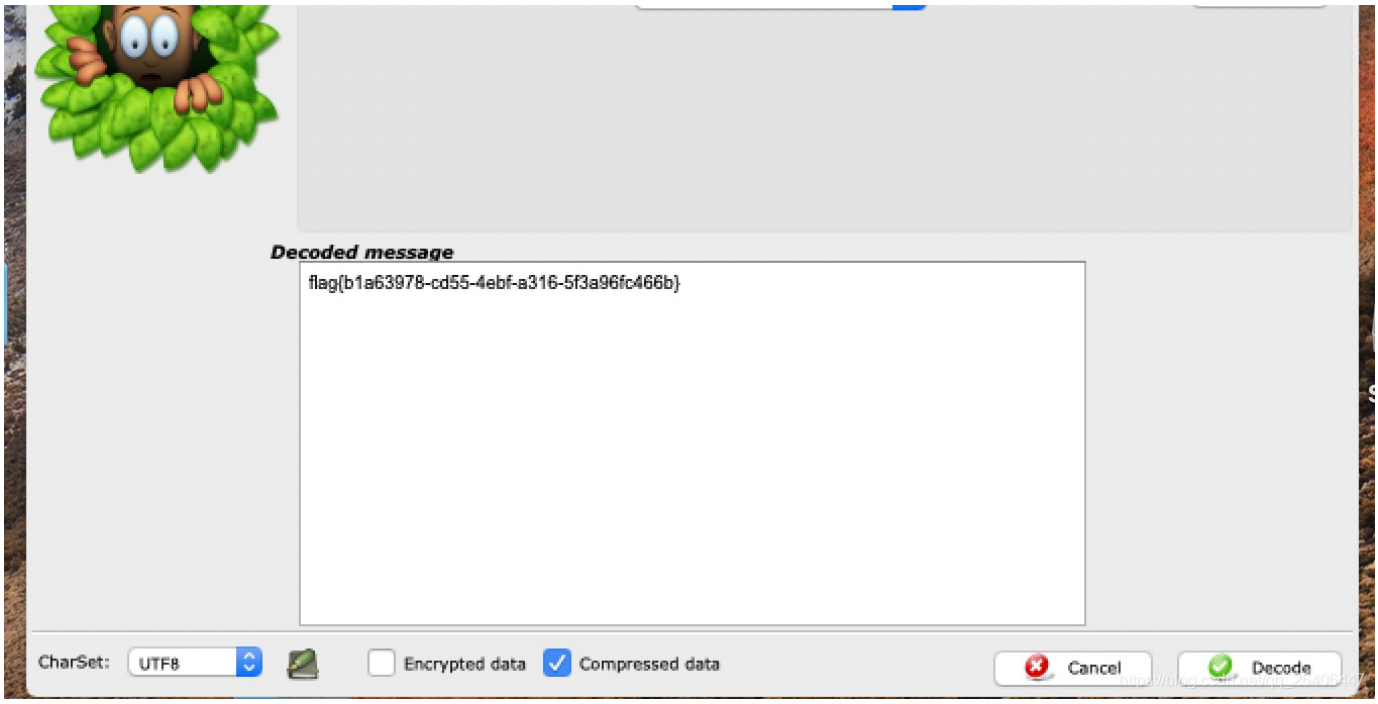
小苹果

音频隐写题，给了一首小苹果…不会，隐写是真的不会…



答案说用silenteye来分析，下好只后直接打开文件，点击decode就能获得flag值

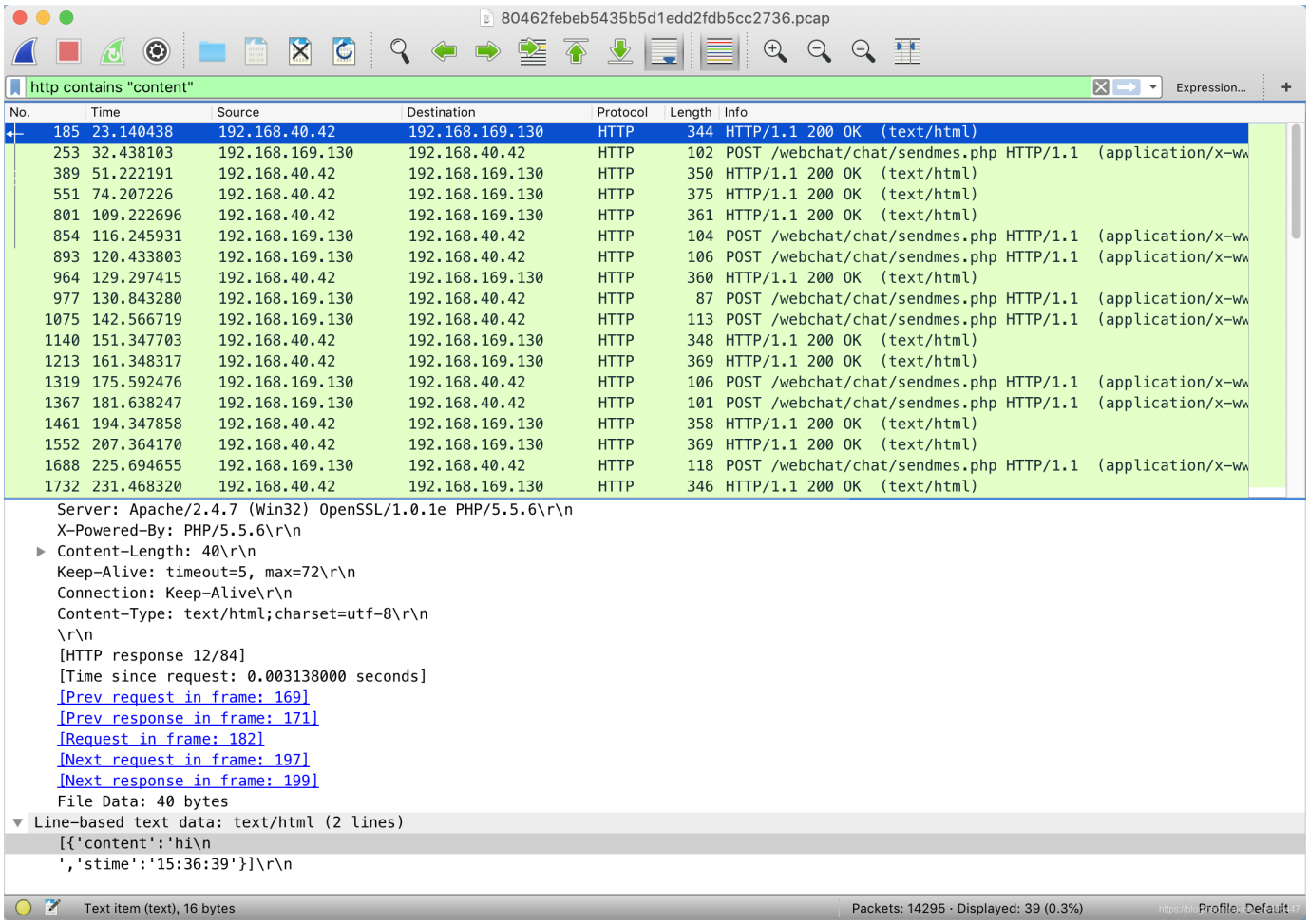




大黑阔的数据包

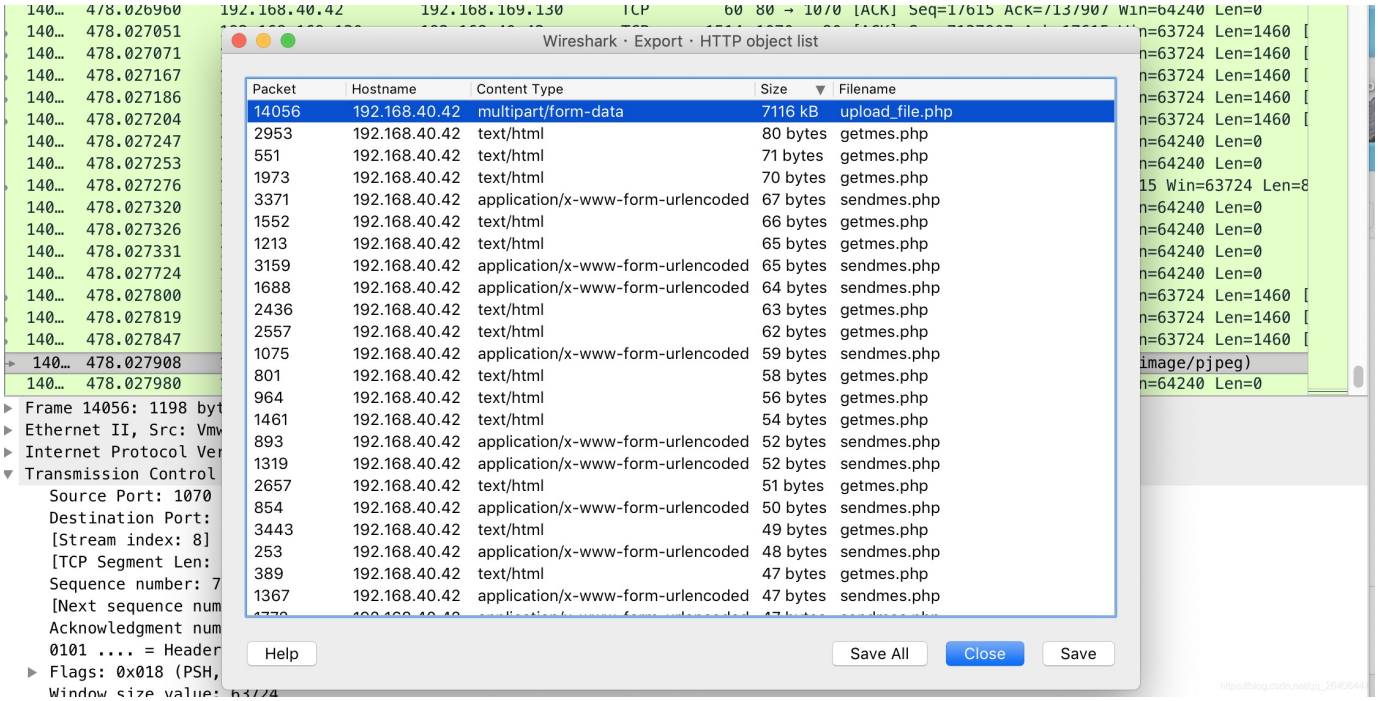
这里给了一个pcap的数据包

按照writeup搜http contains “content”

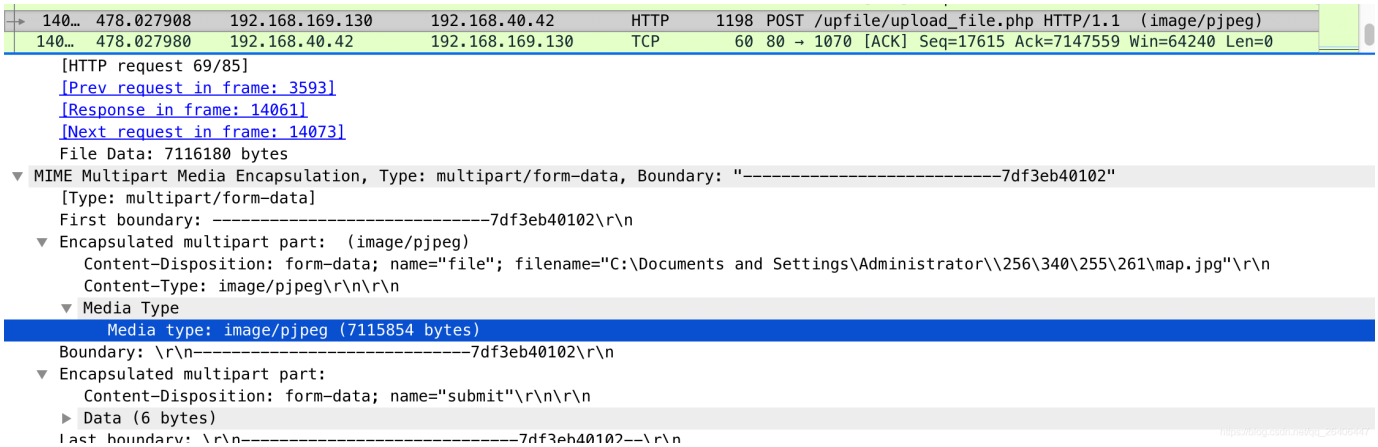


可以发现一段对话

大佬说可以通过文件大小来找图片的包



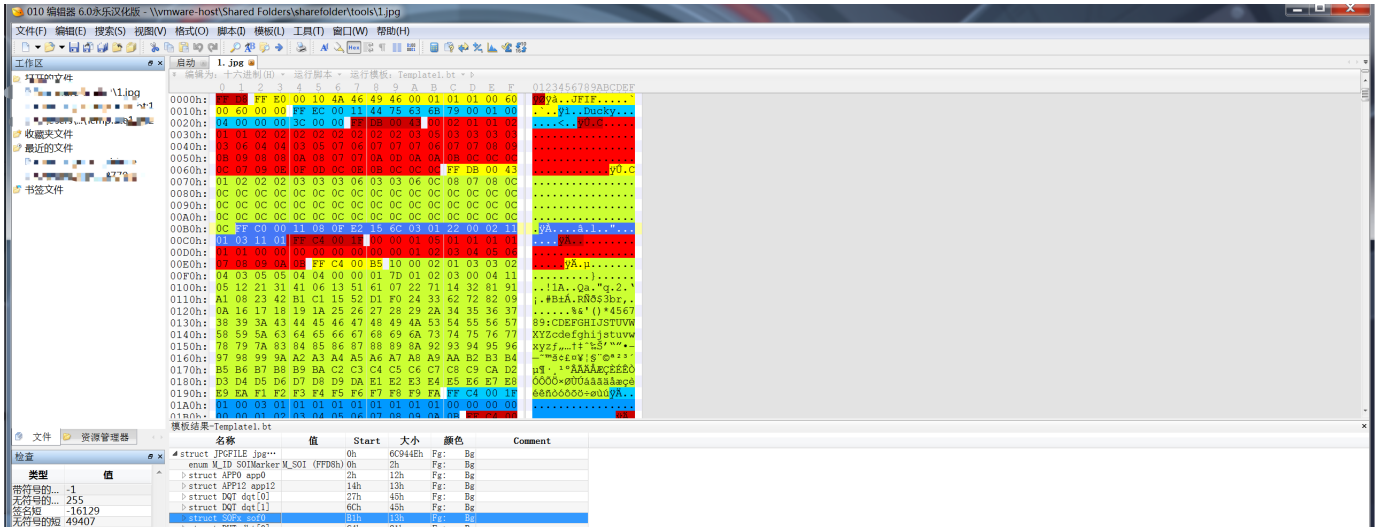
我们找到包，然后导出里面的图片

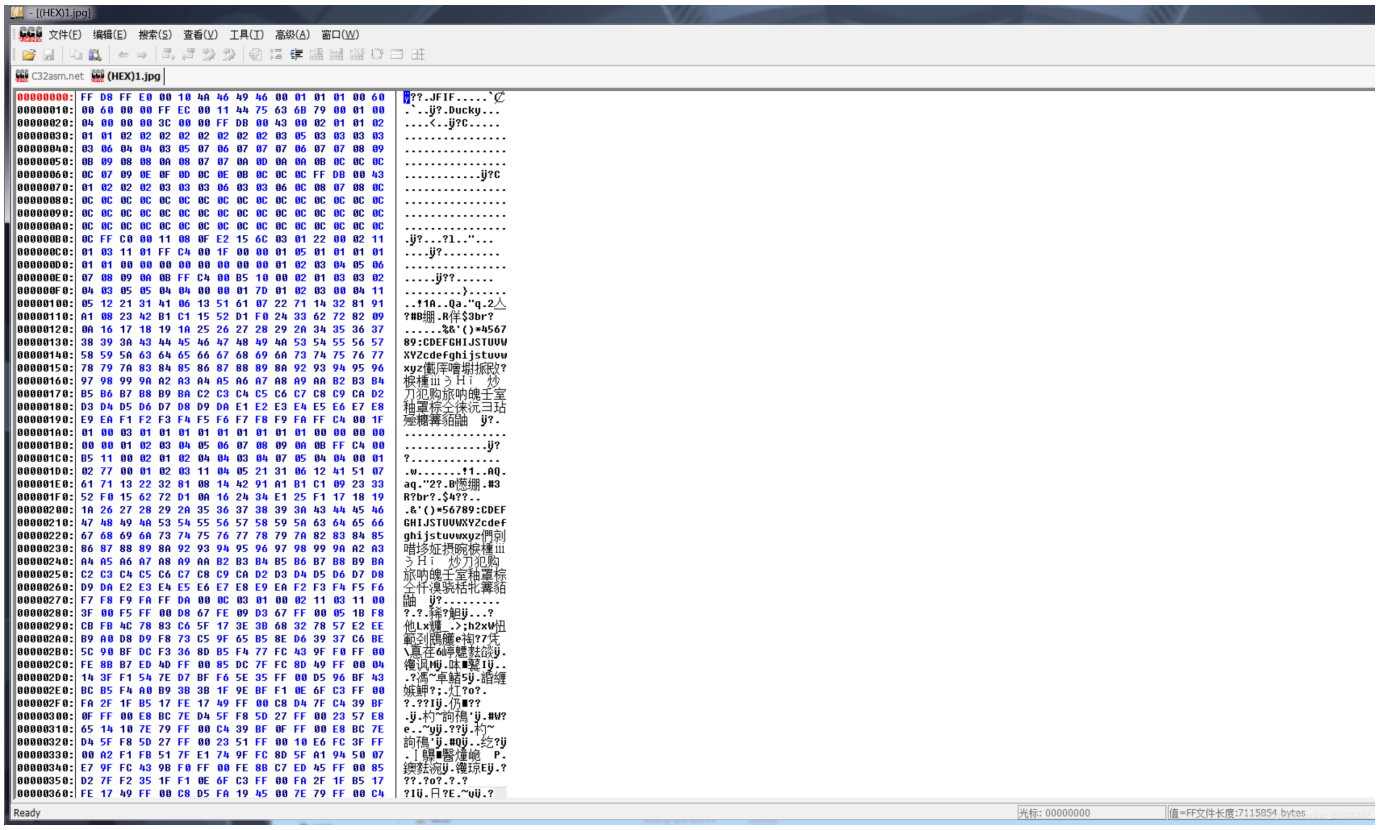


然后可以发现是一张地图

（图片太大上传不了...）

题解说是用c32asm来查看图片删除多余的部分，大佬是用010editor主要有个模版功能挺方便的





然后说前面的部分有部分是多余的部分。将其删除掉

好的用了模版我还是不太懂要删哪…菜鸡流泪…

后面就是删除多余部分ps打开得到flag…

小心猪圈

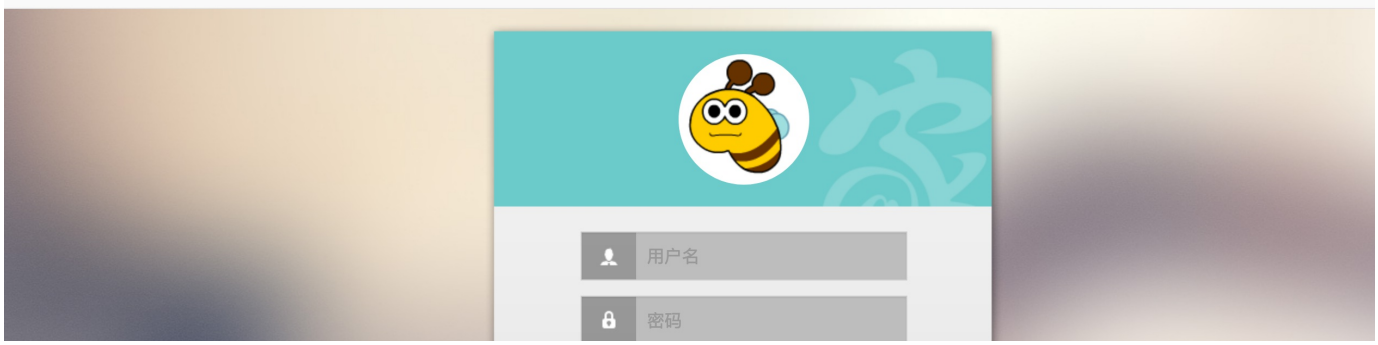
加密题…

小心猪圈

R29klGpvYjo1NzY1NkM2QzIwNjQ2RjZFNjUzQTRBMzU1ODQ3NTkzNjRBNDE0RTM1NTg0NzRCNDk0NDU0NEY1MjUzNTg0MTQ5NDQ0MjRGMzU1MTU4NTM0RjUzNTI0NzQ5MzQ1ODRCNTc1MjU0NEE0QTU1NDc0OTUzNDM1NzRGNEU0RDU2NTE1NT

先base64解码，再16进制解码，再base64解码，最后是猪圈密码解密（题解16到64解码中说还用到了python解码，但没有说怎么解的，不会密码的菜鸡…）

跳来跳去

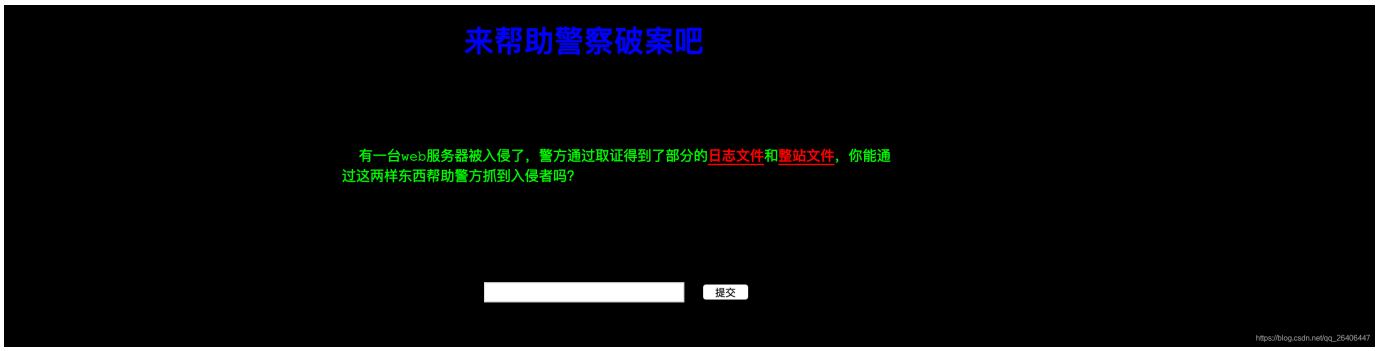


这里用它给的用户名密码登陆会显示权限不足

抓包发现cookie中有个token，token的值进行md5解码后发现是test2…（没想到md5）

然后替换成admin1的md5值就能成功登陆拿到flag（为什么有个1呢…）

Daily_日志源码分析



这里提供了日志文件和整站文件

大佬说有整站文件肯定先看配置文件，找到my.cnf，搜索password

```
# The following options will be passed to all MySQL clients
[client]
password        = YouGotIt!@#$  // KEY
port            = 3306
socket          = /opt/lampp/var/mysql/mysql.sock

# Here follows entries for some specific programs
```


直接找到了密码，输入得到flag…

这里的日志主要告诉你它用的xampp方便找配置文件吧…

总结

这次的web的考查点也不是很多

主要就感受到了配置文件的重要性…