vuln07-PHP反序列化漏洞

无涯老师

课程大纲

1、PHP类与对象
2、PHP Magic函数
3、PHP序列化与反序列化
4、反序列化漏洞的出现
5、CTF题目分析
6、Typecho反序列化漏洞
7、PHP反序列化漏洞防御

01 PHP类与对象

类Class

一个共享相同结构和行为的对象的集合。

```php
<?php
class MyClass {
  var $var1;
  var $var2 = "constant string";

  function myfunc ($arg1, $arg2) {
      [..]
  }
  [..]
}
?>
```

对象Object

类的实例

```
$baidu = new Site;
$kitty = new Cat;
$benz = new Car;
```

02 Magic函数

Magic Methods

https://www.php.net/__sleep

__construct(), __destruct()
__call(), __callStatic(),
__get(), __set(),
__isset(), __unset()
__sleep(), __wakeup()
__serialize(), __unserialize()
__toString()
__invoke()
__set_state()
__clone()
__debugInfo()

函数作用

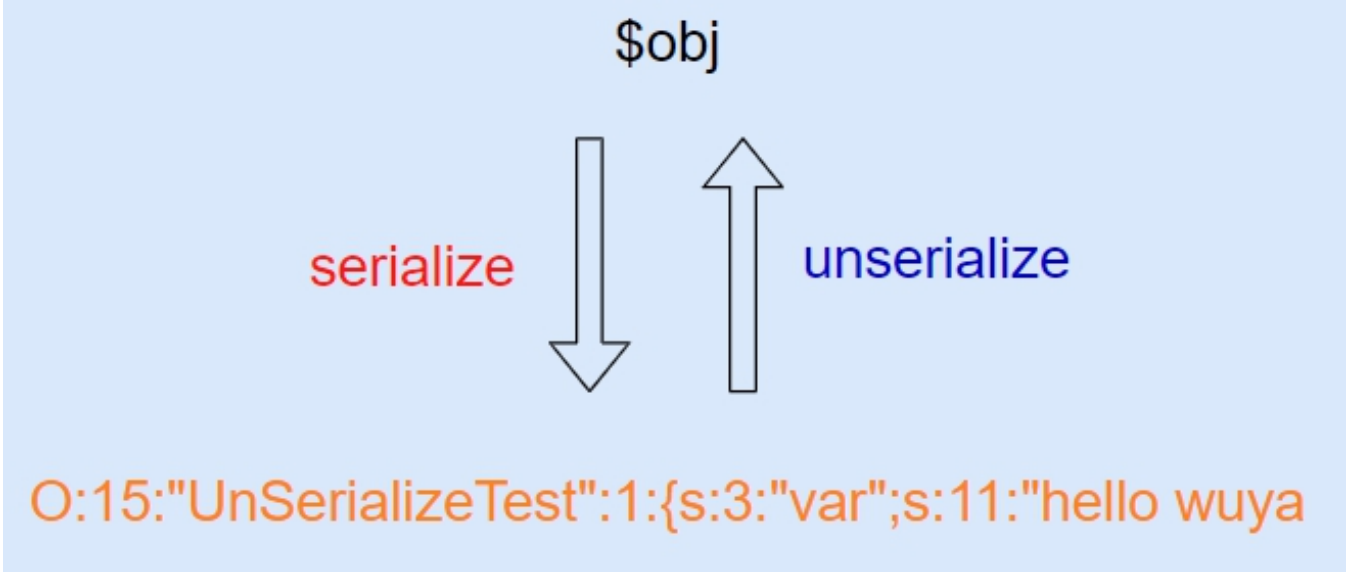
函数	作用
__construct	当一个对象创建时被调用
__destruct	当一个对象销毁时被调用
__toString	当一个对象被当作一个字符串使用
__sleep	在对象被序列化之前运行
__wakeup	在对象被反序列化之后被调用
__serialize()	对对象调用serialize()方法，PHP 7.4.0 起
__unserialize()	对对象调用unserialize()方法，PHP 7.4.0 起

函数作用

函数	作用
__call()	在对象上下文中调用不可访问的方法时触发
__callStatic()	在静态上下文中调用不可访问的方法时触发
__get()	用于从不可访问的属性读取数据
__set()	用于将数据写入不可访问的属性
__isset()	在不可访问的属性上调用isset()或empty()触发
__unset()	在不可访问的属性上使用unset()时触发
__invoke()	当脚本尝试将对象调用为函数时触发

03 PHP序列化和反序列化

序列化和反序列化


$obj
serialize
unserialize
O:15:"UnSerializeTest":1:{s:3:"var";s:11:"hello wuya

类型序列化

类型	格式
String	s:size:value;
Integer	i:value;
Boolean	b:value;(保存1或0)
Null	N;
Array	a:size:{key definition;value definition;(repeated per element)}
Object	O:strlen(object name):object name:object size:{s:strlen(property name):property name:property definition;(repeated per property)}

其他序列化格式

json字符串 json_encode
xml字符串 wddx_serialize_value
二进制格式
字节数组

反序列化：注意

1、如果传递的字符串不可以序列化，则返回 FALSE
2、如果对象没有预定义，反序列化得到的对象是 __PHP_Incomplete_Class

作用

1、传输对象
2、用作缓存（Cookie、Session）

反序列化与Maigc函数

__wakeup
__unserialize（7.4.0）

如果类中同时定义了 __unserialize() 和 __wakeup() 两个魔术方法，则只有 __unserialize() 方法会生效，__wakeup() 方法会被忽略。

04 反序列化的出现

反序列化漏洞

logfile.php

1、记录日志：file_put_contents()

2、类销毁的时候，删除这个日志文件：__destruct()、unlink()

3、日志文件的名字通过filename指定

反序列化漏洞

request.php 利用

1、unserialize通过GET传输反序列化字符串
2、替换了字符串的filename值，比如index.php
3、导致当前目录index.php被删除
4、可以删除任意文件

反序列化漏洞

1、unserialize函数的参数可控，比如通过GET请求传参（漏洞触发点）

2、脚本中定义了有Magic方法，方法里面有向php文件做读写数据或者执行命令的操作，比如__destruct()、unlink()

3、操作的内容需要有对象中的成员变量的值，比如filename

常见利用函数

类别	函数
命令执行	exec() passthru() popen() system() ……
文件操作	file_put_contents() file_get_contents() unlink() ……

利用方式

序列化一个对象，修改成员变量的值，达到操作其他文件或者执行命令的目的

05 CTF题目分析

题目地址

https://adworld.xctf.org.cn/task/answer?type=web&number=3&grade=1&id=4821&page=1

06 typecho反序列化漏洞分析

题目地址

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18753

下载地址：
https://github.com/typecho/typecho/releases/tag/v1.0-14.10.10-release

PHP版本：5.4.5nts （PHPStudy）

在数据库新建一个库，命名为typecho

07 反序列化漏洞修复和防御

防御

针对unserialize和Magic函数审计
对用户输入的内容过滤
白名单，限制反序列化的类；不能动态传参

Thank you for watching

无涯老师