php代码审计基础篇

第11课 反序列化

php代码审计

漏洞介绍

php允许保存一个对象方便以后重用，这个过程被称为序列化

序列化(Serialization)是将对象的状态信息转换为可以存储或传输的形式的过程。在序列化期间，对象将其当前状态写入到临时或持久性存储区。以后，可以通过从存储区中读取或反序列化对象的状态，重新创建该对象。 【将状态信息保存为字符串】

简单的理解：将PHP中对象、类、数组、变量、匿名函数等，转化为字符串，方便保存到数据库或者文件中

什么是反序列化?unserialize

序列化就是将对象的状态信息转为字符串储存起来，那么反序列化就是再将这个状态信息拿出来

使用。(重新再转化为对象或者其他的) 【将字符串转化为状态信息】

危害

就是在php反序列化的时候，反序列化的内容是用户可控，那么恶意用户就可以构造特定序列化内容的代码，通过unserialize()函数进行特定的反序列化操作，并且程序的某处存在一些敏感操作是写在类中的，那么就可以通过这段恶意代码，达到执行攻击者想要的操作。

魔术方法

php中有一类特殊的方法叫“Magic function”(魔术方法)

php类可能会包含一些特殊的函数叫magic函数，magic函数命名是以符号_开头的魔术方法：|

_construct()当一个对象创建时被调用，但在unserialize()时是不会自动调用的(构造函数)

_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()在对象在被序列化运行(清理缓存)

_wakeup在一个对象被反序列化的时候调用

_get()用于从不可访问的属性读取数据

漏洞挖掘思路

反序列化对象中存在魔术方法，而且魔术方法中的代码可以被控制，漏洞根据不同的代码可以导致各种攻击

在反序列化中，我们所能控制的数据就是对象中的各个属性值，

unserialize()函数的参数可控

php文件中存在可利用的类，类中有魔术方法

在各大流行的包中搜索_wakeup()和_destruct()函数.

追踪调用过程

实例代码分析

typecho1.1cms反序列化

谢谢观赏