php代码审计基础篇

第8课 文件操作（一）

php代码审计

漏洞介绍

文件操作类漏洞

文件操作包括文件包含、文件读取(下载、文件删除，文件的修改以及文件上传，这几种文件操作的漏洞有部分的相似点，但是每种漏洞都有各自的漏洞函数以及利用方式。

文件包含漏洞：

服务器执行PHP文件时，可以通过文件包含函数加载另一个文件中的PHP代码，并且当PHP来执行，这会为开发者节省大量的时间。这意味着您可以创建供所有网页引用的标准页眉或菜单文件。当页眉需要更新时，您只更新一个包含文件就可以了，或者当您向网站添加一张新页面时，仅仅需要修改一下菜单文件(而不是更新所有网页中的链接)

文件包含(远程文件，本地文件包含)

include和require区别主要是，include在包含的过程中如果出现错误，会抛出一个警告，程序继续正常运行；而require函数出现错误的时候，会直接报错并退出程序的执行。

而include_once(),require_once()这两个函数，与前两个的不同之处在于这两个函数只包含一次，适用于在脚本执行期间同一个文件有可能被包括超过一次的情况下，你想确保它只被包括一次以避免函数重定义，变量重新赋值等问题

漏洞介绍

文件操作类漏洞

文件操作包括文件包含、文件读取、文件删除、文件修改以及文件上传，这几种文件操作的漏洞有部分的相似点，但是每种漏洞都有各自的漏洞函数以及利用方式。文件读取和下载漏洞：

文件下载操作中，文件名及路径由客户端传入的参数控制，并且未进行有效的过滤，导致用户可恶意下载任意文件。

文件读取是属于文件操作漏洞的一种，一般任意文件读取漏洞可以读取的配置信息甚至系统重要文件。

```php
<?php
    $filename = $_GET['filename'];
    echo file_get_contents($filename);
    header('Content-Type: image/jpeg');
    header('Content-Disposition: attachment; filename='.$filename);
    header('Content-Lengh: '.filesize($filename));
?>
```

漏洞防范

要操作更多文件需要跳转目录。

大多都是直接在请求中传入文件名。或者过滤不严谨导致绕过

有的文件操作是不需要直接传入文件名的，比如下载文件的时候，下载的文件是已知的，则我们可以用更安全的方法来替代直接以文件名为参数下载操作，比如把文件名、文件路径、文件ID(随机MD5形式)

要避免目录跳转的问题，

需要传人件路径的，可以在后台固定文件操作目录，然后禁止参数中有“.”两个点和反斜杠以及斜杠来跳转目录，怎么禁止呢?检查到传人的参数有这些字符，之间提示禁止操作并停止程序继续往下执行即可。

漏洞挖掘思路

挖掘经验：

文件包含搜索include()、include_once()、require()和require__once()这四个函数来回溯看看有没有可控的变量，它们的写法可以在括号里面写要包含的路径，也可以直接用空格再跟路径。

文件下载和读取：

一种方式是可以先黑盒看看功能点对应的文件，再去读文件，这样找起来会比较快。另外一种方式就是去搜索文件读取的函数，看看有没有可以直接或者间接控制的变量，文件读取(下载)函数列表如下：

file_get_contents()、highlight file()、fopen().readfile()、fread()、fgetss()、fgets()、parse_ini_file(),show_sourc()、file()下载也是类似

实例代码分析

齐博cms文件包含

MetInfo CMS任意文件读取

Ear Music任意文件下载漏洞

Pluck CMS 4.7.2文件包含

谢谢观赏