20200727信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/7/27 19:46	**更新时间:**	2020/7/27 22:39
作者:	820410740@qq.com		

文件包含

- 程序开发人员通常会把可重复使用的函数写到单个文件中，在使用某个函数的时候，直接调用此文件，无需再次编写，这种调用文件的过程通常称为包含

- 程序开发人员都希望代码更加灵活，所以通常会把被包含的文件设置为变量，来进行动态调用，但正是由于这种灵活性，从而导致客户端可以调用任意文件，造成文件包含漏洞。

- 几乎所有的脚本语言都会提供文件包含功能。文件包含漏洞在PHP Web Application中居多，在JSP/ASP/ASP.net程序中比较少。

漏洞产生的原因

1. Web应用实现了动态包含
2. 动态包含的文件路径参数，客户端可控

文件包含漏洞：攻击者利用包含的特性，加上应用本身对文件（包含）控制不严格，最终造成攻击者进行任意文件包含。（注：包含的文件会被当成脚本文件来解析）
（**文件包含并不属于漏洞，但是，由于对包含进来的文件不可控，导致了文件包含漏洞的产生**）
本地文件包含：包含服务器上的资源
远程文件包含：通过HTTP协议包含其他地方的资源
文件包含函数：

include()	文件包含失败时，会产生警告，脚本会继续执行
include_once()	与include()功能相同，文件只会被包含一次
require()	文件包含失败时，会产生错误，直接结束脚本运行
require_once()	与require()功能相同，文件只会被包含一次

文件包含特点：
文件包含危害：
1. 读取敏感信息
2. 木马文件执行，getshell。
防御策略：
1. 无需情况下设置allow_url_include和allow_url_fopen为关闭
2. 对可以包含的文件进行限制，可以使用白名单的方式，或者设置可以包含的目录，如open_basedir
3. 建议假定所有输入都是可疑的，尝试对所有输入提交可能可能包含的文件地址，包括服务器本地文件及远程文件，进行严格的检查，参数中不允许出现../之类的目录跳转符。
4. 严格检查include类的文件包含函数中的参数是否外界可控
文件包含漏洞无视文件格式
被包含的文件中有PHP代码，就会被执行。PHP 封装协议的使用

:// 处理交互式流

文件下载漏洞

1. burp 抓包获取文件下载URL链接
2. 可以传入想要下载的文件进行下载