php代码审计基础篇

第9课 文件操作（二）

漏洞介绍

文件删除漏洞：

文件删除漏洞出现在有文件管理功能的应用上比较多，这些应用-一般也都有文件上传和读取等功能，它的漏洞原理跟文件读取漏洞是差不多的，不过是利用的丽数不一样而已，一般也是因为删除的文件名可以用./跳转，或者没有限制当前用户只能删除他该有权限删除的文件。常出现这个漏洞的丽数是unlink()文件修改漏洞：权限校验不严，函数过滤不严，导致可控拼接路径

文件上传漏洞：

文件上传漏洞是指用户上传了一个可执行的脚本文件，并通过此脚本文件获得了执行服务器端命令的能力。文件上传漏洞大多是没有限制上传的文件格式，导致可以直接上传危险文件，并且部分文件上传漏洞的利用技术门槛非常的低，对于攻击者来说很容易实施未进行文件类型和格式做合法性校验，任意文件上传

漏洞防范

文件上传漏洞虽然定位起来比较简单，但是修复起来要考虑的东西还是不少，主要是不同环境下的利用场景比较多，需要比较完善的策略去防止漏洞出现。

文件上传漏洞主要有两种利用方式，分为上传的文件类型验证不严谨和写入文件不规范。对应防范：

黑名单过滤，白名单过滤。

保存上传的文件时重命名文件，文件名命名规则采用时间戳的拼接随机数的

MD5值方式"md5(time()+rand(1,10000)"。

对权限的管理要合理

要避免目录跳转的问题

https://codeload.github.com/cOny1/upload-labs/zip/master

漏洞条件(文件上传)

Content-Length,即上传内容大小

MAX_FILE SIZE,即上传内容的最大长度

filename,即上传文件名

Content-Type,即上传文件类型

请求包中的乱码字段，即是所上传文件的内容

有可能存在请求包中的可控点还有上传路径，只是上面的示例中没有出现漏洞挖掘思路

文件删除：路径文件名可控，找unlink函数

文件可上传——知道文件上传路径——上传文件可以被访问——上传文件可以被执行

上传点都调用同一个上传类，直接全局搜索上传函数　　黑盒寻找上传点，代码定位

php代码审计

实例代码分析

Hongcms前台任意文件删除

易优cms任意文件上传漏洞

谢谢观赏