php代码审计基础篇

第7课 命令执行

php代码审计

漏洞介绍

命令执行漏洞：

用户通过浏览器提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定绝对路径的情况下就执行命令，可能会允许使用者通过改变$PATH或程序执行环境的其他方面来执行一个恶意构造的代码

危害：

继承Web服务程序的权限去执行系统命令或读写文件

反弹shell 控制整个网站甚至控制服务器进一步内网渗透等等

命令管道符

直接执行后面的语句

|| 前面出错执行后面的前面为假

&前面的语句为假则直接执行后面的，前面可真可假

&&前面的语句为假则直接出错后面的也不执行...前面只能为真

漏洞防范

PHP在命令上

函数共有两个escapeshellcmd()和escapeshellarg()

escapeshellarg()将给字符串增加一个单引号并且能引用或者转码任何已经存在的单引号，这样以确保能够直接将一个字符串传入shell函数，并且还是确保安全的

escapeshellcmd()对字符串中可能会欺骗shell命令执行任意命令的字符进行转义。此函数保证用户输入的数据在传送到exec()或system()函数，或者执行操作符之前进行转义

尽量不要使用系统执行命令。

在执行命令函数、方法前，变量一定要做好过滤，对敏感字符进行转义。使用动态函数之前，确保使用的函数是指定的函数之一。对PHP语言来说，不能完全控制的危险函数最好不要使用

漏洞挖掘思路

应用调用执行系统命令的函数

将用户输入作为系统命令的参数拼接到了命令行中 没有对用户输入进行过滤或过滤不严常用函数

exec()、system()、popen()、passtOhru()、proc_open()、pcntlLexec()、shell_exec()、反引号`

了解执行方式

Web应用会有比较多的点之间使用system().

exec()、shell_exec()、passthru()、pcntl_exec()、popen)、proc_open()执行系统命令来调用这些脚本，用得多了难免就会出现纰漏导致漏洞，这类应用可以直接在代码里搜这几个函数，收获应该会不少。

除了这类应用，也有调用外部程序的功能，如数据库导出功能，曾经就出现过命令执行漏洞，因为特征比较明显，所以可以直接搜函数名即可进行漏洞挖掘。

实例代码分析

catfish存在命令执行漏洞

谢谢观赏