php代码审计基础篇

第10课 变量覆盖

php代码审计变量覆盖漏洞

漏洞介绍

变量覆盖是指变量未被初始化，我们自定义的参数值可以替换程序原有的变量值

通常来说，单独的变量覆盖漏洞很难有利用价值，需要和其他漏洞结合起来或者结合其他程序的功能才能完成攻击

但在某些情况下，可通过变量覆盖漏洞直接获取getshell,所以这个漏洞发挥空间是很大的通常结合程序的其他漏洞实现完整的攻击，比如文件上传页面，覆盖掉原来白名单的列表，导致任意文件上传；用户注册页面控制没覆盖的未初始化变量导致SQL。

比如我们上传的地方有变量覆盖漏洞，就可以覆盖原理的白名单后缀，实现任意文件上传

php代码审计变量覆盖漏洞

漏洞挖掘思路

常见危险函数:

|$$使用不当

extract()函数使用不当

parse_str()使用不当

import_request_variables()开启了全局变量注册等

php代码审计变量覆盖漏洞

漏洞防范

变量覆盖漏洞都是因为开发在进行变量注册的时候不严谨导致的所以解决变量覆盖的问题，最简单的方法就是不进行变量注册直接去使用原生的数组变量，比如$_GET,$_POST来进行操作

如果需要注册变量的话，可以直接在代码中定义变量，然后通过赋值进行操作

还可以在注册变量之前，先去验证变量是否存在，最重要的就是要控制变量，变量是否可控也是导致这个漏洞的一大因素

针对函数

extract()函数第二个参数修改为extr_skip

parse_str()函数的防范

添加判断语句import_request_variables()函数防御

在PHP5.5之后已被官方删除

php代码审计变量覆盖漏洞

实例代码分析

多米cms变量覆盖

谢谢观赏