php代码审计基础篇

第3课 sql注入

php代码审计之sql注入漏洞

漏洞介绍

SQL注入即是指web应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在web应用程序中事先定义好的查询语句的结尾上添加额外的SQL语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

代码审计中的sql注入

其实就是开发者在编写代码操作数据库的时候，直接将外部可控的参数拼接到sql语句中然后这个语句没有经过任何过滤就直接放入到数据引擎执行

分类

普通注入：由于代码层面过滤不严或无过滤，用户可以直接控制输入。分为整数型和字符型注入编码注入程序在进行操作前会进行一些编码处理，而编码处理的函数也是存在问题

宽字节注入set character_set_client =gbk

二次urldecode注入

php代码审计之sql注入漏洞

常见防护函数

intval()函数用于获取变量的整数值。

addslashes()

函数返回在预定义字符之前添加反斜杠的字符串

预定义字符单引号(')双引号(")反斜杠(\)NULL

mysql_escape_string()转义一个字符串用于mysql_query

mysql_query()函数执行一条MySQL查询

preg_replace—执行一个正则表达式的搜索和替换

str_replace()函数以其他字符替换字符串中的一些字符(区分大小写)

mysql_escape_string和mysqLreale3.scape string函数都是对字符串进行过滤，在PHP4.0.3以上版本才有

漏洞挖掘思路

用户可控输入，拼接了用户输入的代码

数据库操作存在一些关键字，比如select from、mysql connect、mysql query、mysql fetch_row等，数据库的查询方式还有update、insert、delete我们在做白盒审计时，只需要查找这些关键字，即可定向挖掘SQL注入漏洞

php代码审计之sql注入漏洞

实例代码分析

经典bluecms sql注入

semcms某文件存在注入漏洞

X_FORWARDED_FOR注入

谢谢观赏