Certified Ethical Hacker (CEH): SQL Injection

SQL 注入

今日议题

- SQL注入概述
-
- SQL注入工具和逃避方法
- SQL注入防御

SQL注入概述

- 什么是SQL注入

  - SQL注入攻击指的是通过构建特殊的输入作为参数传入Web应用程序，而这些输入大都是SQL语法里的一些组合，通过执行SQL语句进而执行攻击者所要的操作，其主要原因是程序没有细致地过滤用户输入的数据，致使非法数据侵入系统。
  - 获取　　验证的数据库访问权限或直接从数据库检索信息。

SQL注入概述

- SQL注入原理

  由于程序没有过滤用户的输入，攻击者通过响服务器提交恶意的SQL查询语句，应用程序接收后错误的将攻击者的输入作为原始SQL查询语句的一部分执行，导致改变了程序原始的SQL查询逻辑，额外的执行了攻击者构造的SQL查询语句。

  - SQL注入是最常见的网站漏洞
  - Web应用程序中的缺陷，不是数据库和web服务器的问题
  - 许多程序员并没有意识到这个威胁

SQL注入概述

- SQL注入类型
  - 简单SQL注入
    - ✓联合SQL注入
    - ✓基于错误的SQL注入
  - SQL盲注入