链滴

SQL 注入

作者：Kun-ROC
原文链接：https://ld246.com/article/1622729429742
来源网站：链滴

<h1>SQL注入漏洞</h1>

1.基本介绍:

SQL Injection，即SQL注入，是指攻击者通过注入恶意的SQL命令，破坏SQL查询语句的结构，从而到执行恶意SQL语句的目的。SQL注入漏洞的危害是巨大的，常常会导致整个数据库被“脱裤”，尽如此，SQL注入仍是现在最常见的Web漏洞之一。

2.基本原理:

select * from user where username = '**username**'，加粗部分内容为用户可控的内容，如果我们试输入一个单引号（ ’）。Sql语句就变成了select * from user where username = ’ ’ ’ ，前面个单引号组成了一对，后面空出一个单引号不符合语法规则，所以产生报错。此时我们已经修改了原SQL语句的结构。输入$username参数的地方也叫做注入点，注入点可能存在于GET参数内、POST数内、HTTP头字段内等。

3.实战:

绕过登录:

select * from username = '**username**' and password = '$**password**'

方法:

(1).使用注释

(2).注意闭合单引号

如果我们输入' or '1'= '1' -- ，那么sql语句就会变成select * from username where username = 'username' or '1' = '1' [后边的内容全都被注释掉了]，此时该语句就等同于select * from user 。

4.SQL注入发生的原因

-攻击者可以对输入变量进行控制

-服务器对用户输入的变量没有进行安全处理（过滤、转义）

-不安全的数据库配置（最小用户权限、安全配置）

5. SQL注入漏洞的种类

-根据注入点输入类型分为字符串和数字型

-根据注入点的位置分为POST注入，GET注入，HTTP头注

-根据获取信息的方式分为基于报错的注入、基于布尔的盲注、基于时间的盲注、联合查询（union select）注入等

6.SQL注入一般流程

-判断是否存在注入，注入是字符型还是数字型

-猜解SQL查询语句的结构，并根据注入的类型来判断注入方法。

-获取当前数据库

-获取数据库中的表

-获取表中的字段名

-获取数据

明日更新SQL注入实战之联合查询(显错注入)

原文链接：SQL 注入