SQL 注入攻击与防护策略分析

郑智钊

（哈尔滨铁道职业技术学院）

摘　要：针对 WEB 应用安全问题中最常见到的 SQL 注入攻击，本文对攻击的原理、手段和过程做了介绍和剖析，并针对 SQL 注入的特点指出了对于提高网站安全的策略。

关键词：SQL 注入；WEB 安全；网站防护措施

引言

近年来，WEB 应用成为了人们日常生活、工作、学习中必不可少的工具和信息来源，随之而来的是信息安全问题层出不穷。2016 年国内某专业信息安全平台被发现存在 SQL 注入漏洞，导致大量用户信息被泄露。由于绝大多数当今网站都是通过数据库存储用户信息和网站数据，这导致 SQL 注入攻击成为网站最常见到的安全风险来源之一。

1. SQL 注入攻击原理

SQL 注入攻击是通过操作输入来修改 SQL 语句，用以达到执行代码对 WEB 服务器进行攻击的方法。简单的说就是在 post/get web 表单、输入域名或页面请求的查询字符串中插入 SQL 命令，最终使 web 服务器执行恶意命令的过程。可以通过一个例子简单说明 SQL 注入攻击。

假设某网站页面显示时 URL 为 http://www.example.com?test = 123，此时 URL 实际向服务器传递了值为 123 的变量 test，这表明当前页面是对数据库进行动态查询的结果。由此，我们可以在 URL 中插入恶意的 SQL 语句并进行执行。另外，在网站开发过程中，开发人员使用动态字符串构造 SQL 语句，用来创建所需的应用，这种情况下 SQL 语句在程序的执行过程中被动态的构造使用，可以根据不同的条件产生不同的 SQL 语句，比如需要根据不同的要求来查询数据库中的字段。这样的开发过程其实为 SQL 注入攻击留下了很多的可乘之机。

2. SQL 注入攻击常见方法和过程

2.1 寻找 SQL 注入漏洞

确定网站存在 SQL 注入漏洞的途径一般有两种，第一种是可以利用网站的错误提示，如果网站开启了错误显示，攻击者就可以通过在输入参数的地方反复调整发送的参数，通过页面出现的错误信息，推测出网站使用的数据库和开发语言信息。如果网站管理员关闭了错误信息提示，攻击者可以采用盲注的技巧来进行反复尝试。盲注是利用数据库查询的输入审查漏洞从数据库提取信息或提取与数据库查询相关的信息的技术。如在 URL 中输入 login.php?username =admin’ and 1 =1 和 login.php?user-name=admin’ and 1=2，如果前者能正常返回信息，而后者不能，基本上就可以认定网站存在 SQL 注入漏洞。这是因为 1=2 的表达式不成立，所以即使 username 传入了正确的数值也是无法通过，因此可以判读出该网站可以通过 usernamer 参数进行注入。

2.2 判断数据库

获得网站的数据库类型是 SQL 注入提取重要数据的前提条件之一，可以通过常见的技术架构进行判断，如 aps.net 常和 SQL Server 一起使用，而 PHP 往往使用 MySQL，JSP 会配合 Oracle 或 MySLQ。而 WEB 服务环境也可以提供线索，如运行 IIS 的服务环境往往采用 SQL Server 数据库，使用 TOMCAT 的更大的可能是 MySQL 或 Oracle。另外，还可以通过详细的错误信息判断数据库的版本，比如添加单引号作为注入参数，根据数据库产生的语法错误信息，就可以判断出数据库的种类。

2.3 攻击数据库系统

攻击数据库的目的是为了获得数据库中有价值的数据信息，进而可以为控制整个 WEB 系统做铺垫。获得数据库中数据可以遵循层次化的方法，首先提取数据库的名称，然后提取表、列，最后才是数据本身。通常，可以通过访问专门保存表示各种数据库结构的表，比如 MySQL 中，这些信息保存在 information_schema 数据库中。在该数据库中的 schemata 表中存储着数据库名，tables 表中存储着表名，columns 表中存储着字段名，通过以上的信息，再获得数据库表中的内容就轻而易举了。

2.4 控制 WEB 系统

在获得数据库中数据信息后，可以通过对具有管理权限的账号信息入手，通过登录帐号，使用网站后台上传功能上传木马程序，或添加恶意代码，最终甚至可以获得服务器的完全控制权限。

3. SQL 注入攻击防护策略

SQL 注入漏洞的产生，都是因为系统要接受来自客户端输入的变量或者 URL 传递的参数，为此，开发者一定要遵循“外部数据不可信”原则，对于用户输入的内容或传递的参数，要时刻保持警惕。因此对于 SQL 注入的防护策略通常要确保系统传递的变量符合开发者的设计要求。

3.1 变量检测

对于数据库中有固定数据类型的变量，在 SQL 语句执行前，应该对变量的类型进行严格的检查，确保变量是开发者预想的。比如系统中存在名为 id 的数字字段，那么系统在执行 SQL 语句前确保变量 id 的类型是 int 型的。

3.2 过滤特殊符号

当发生 SQL 注入攻击时，攻击者在提交的 SQL 语句会包含一些特殊的字符或字符串，如单引号、双引号、反斜杠、NULL 等。这样，可以通过使用数据库系统自带函数或编写相关验证程序对用户输入的这类符号进行转义或者过滤，从而达到限制 SQL 注入的目的。

3.3 合理使用预编译

预编译是吧一些格式固定的 SQL 编译后，存放在内存池中，当需要执行相同 SQL 语句时，就可以直接执行以及预编译的语句，不同的数据库系统都有预编译机制。因此，在当遇到类似 login.php?username=admin’ and 1=1 的注入攻击时，预编译 SQL 语句 WHERE username=?可以阻止攻击的成功。

3.4 对关键数据信息加密

对于数据库中诸如账号密码的信息应该避免使用明文存储，可以使用 AES、RSA、MD5 等算法对数据进行加密存储，这样即使系统被 SQL 注入成功，攻击者也无法轻易获得关键数据信息的内容。

4. 结语

SQL 注入一直是网站重要的安全风险来源，作为网站的开发者和运维人员应该意识到 SQL 注入攻击是一种综合的攻击手段。为了避免 SQL 注入带来的影响，开发者和运维人员应该从网站设计入手，并对服务器、数据库管理等多方面加以规范，确保网站可以安全可靠的运行。

参考文献：

[1]郑成兴.网络入侵防范的理论与实践[m].机械工业出版社，2012

[2]黄健.计算机信息安全技术及防护[J].信息安全与技术，2012,4.

[3] 阴国富. 基于 SQL 注人的安全防范检测技术研究 [J]. 河南科学，2009,27

[4]李虎军.浅谈网站 SQL 注入攻击防护策略研究[J].电脑知识与技术，2016,3

作者简介：

郑智钊，男，1983 年出生，工学学士，网络工程师，工作单位：哈尔滨铁道职业技术学院，主要研究方向：计算机科学与应用。