<<SQL注入攻击与防御>>

图书基本信息

书名：<<SQL注入攻击与防御>>

13位ISBN编号：9787302224136

10位ISBN编号：7302224137

出版时间：2010-6

出版时间：清华大学出版社

作者：克拉克

页数：339

字数：589000

前言

十几年前，基于数据库的Web应用刚流行时，几乎所有开发商都忽略了SQL注入漏洞，导致当时大多数网站的登录入口形同虚设。
时至今日，Web应用已愈加成熟，安全性也不断得到加强。
遗憾的是，针对SQL注入漏洞的各种攻击工具也在推陈出新，不断地向安全管理人员发出新的挑战。
如何最大程度地降低SQL注入风险，从根本上实施SQL注入防御，成为网络管理人员和开发人员亟需解决的“烫手山芋”。

现在网络上关于SQL注入方面的教程比较零散，大多针对某一类具体应用，难以作为预防SQL注入的完整解决方案。
本书弥补了这一缺憾！
本书作者均是专门研究SQL注入的安全专家，他们集众家之长，对应用程序的基本编码和升级维护进行全程跟踪，详细讲解可能引发SQL，注入的行为以及攻击者的利用要素，并结合长期实践经验提出了相应的解决方案。
SOL注入利用的是正常的HTTP服务端口，表面上和正常的Web访问没有差别，隐蔽性极强。
针对这种情况，书中重点讲解了SQL注入的排查方法和可以借助的工具，总结了常见的利用SQL注入漏洞的方法。
开发人员和系统管理人员在SQL注入防御中扮演着重要角色，因此，书中专门从代码层和系统层角度介绍了避免SQL注入的各种策略和需要考虑的问题。

全书共l0章，分别介绍了SOL注入的基本概念，如何发现、确认并利用SQL注入和SQL盲注，利用操作系统防御SQL注入，SQL注入的一些高级话题，代码层和平台层防御等知识，书中主要针对的是Microsoft SQL Server、My SQL和Oracle这三大主流数据库。
本书注重于实践，涉及的内容也比较前沿，另外，还包含了大量翔实的案例，它们都具有很好的现实指导作用，读者可从中学到最新的攻击和防御技术。

本书主要由黄晓磊和李化翻译完成，全书由李化统稿。
由于本书内容较新、知识面广且译者水平有限，译文中难免存在错误之处，敬请读者批评指正。

<<SQL注入攻击与防御>>

内容概要

SQL注入是Internet上最危险、最有名的安全漏洞之一，本书是目前唯一一本专门致力于讲解SQL威胁的图书。
本书作者均是专门研究SQL注入的安全专家，他们集众家之长，对应用程序的基本编码和升级维护进行全面跟踪，详细讲解可能引发SQL注入的行为以及攻击者的利用要素，并结合长期实践经验提出了相应的解决方案。
针对SQL注入隐蔽性极强的特点，本书重点讲解了SQL注入的排查方法和可以借助的工具，总结了常见的利用SQL漏洞的方法。
另外，本书还专门从代码层和系统层的角度介绍了避免SQL注入的各种策略和需要考虑的问题。
本书主要内容 SQL注入一直长期存在，但最近有所增强。
本书包含所有与SQL注入攻击相关的、当前已知的信息，凝聚了由本书作者组成的、无私奉献的SQL注入专家团队的所有深刻见解。
什么是SQL注入?理解它是什么以及它的基本原理 查找、确认和自动发现SQL注入 查找代码中SQL注入时的提示和技巧 使用SQL注入创建利用 通过设计来避免由SQL攻击所带来的危险

作者简介

凭借这本《SQL注入攻击与防御》，测试人员现在有了一把弥补Internet上各种分散式教程不足的利器。
阅读本书您可以学会识别并利用各种平台上不同种类的SQL注入缺陷。

——Devon Kearna，安全分析师

<<SQL注入攻击与防御>>

书籍目录

章节摘录

8.9 常见问题解答　　问题：为什么不能使用参数化语句来提供表名或列名？
解答：不能在参数化语句中提供SQL标识符，是因为在数据库中它们会被编译并且之后会被提供的数据填充。
这要求SQL标识符在提供数据之前的编译期间出现。
问题：为什么不能拥有参数化的ORDERBY子句？
解答：这个问题的答案与上一问题相同，因为ORDERBY包含一个SQL标识符，也就是要进行排序的列。
问题：如何在x技术中对Y数据库使用参数化语句？
解答：大多数现代编程语言和数据库均支持参数化语句。
请查看当前使用的数据库访问API的文档。
请记住，有时也将这些语句称为预处理语句。
问题：怎样参数化一个存储过程调用？
解答：在大多数编程语言中，这与使用参数化语句非常类似或者完全相同。
请查询当前使用的数据库访问API的文档。
请记住，有时也将这些语句称为可调用语句。
问题：从哪里获取良好的用于验证x的黑名单？
解答：非常不幸，向黑名单中放入什么内容取决于应用的语境。
如果可能的话，请尽量不要使用黑名单，因为我们无法列举出所有的潜在攻击或恶意输入。
如果必须使用黑名单，则请确保您要么使用输出编码，要么将黑名单输入验证作为唯一的验证方法。
问题：使用白名单输入验证是安全的吗？
解答：不是。
这取决于您允许通过的内容。
例如，可能允许输入单引号，当在动态SQL中包含这样的输入时就会产生问题。
问题：哪些场合比较适合使用白名单输入验证？
哪些场合适合使用黑名单输入验证？
解答：应该在应用中接收输入的地方使用白名单输入验证，以便对敏感内容应用验证。
在Web应用防火墙或类似的位置适合将黑名单验证作为附加的控制，以此来检测明显的SQL注入攻击企图。
问题：需要对发送给数据库和从数据库获取的输入都进行编码吗？
为什么？
解答：不管在哪里使用动态SQL，都需要确保提交给数据库的内容不会引发SQL注入问题。
这并不意味着恶意内容已经变得安全。
当从数据库查询这些内容并在其他地方的动态SOL中使用时，还是会存在危险。
问题：应该在哪些位置进行编码？
解答：应该在使用信息的位置附近进行编码。
如果在数据未到达数据库之前向数据库提交数据，那么就应该对数据进行编码。
应该在有可能使用数据的位置附近（例如，将数据展示给用户之前针对跨站脚本编码）或者在动态SQL中使用数据之前（针对SQL注入编码）对来自数据库的数据进行编码。

<<SQL注入攻击与防御>>

编辑推荐

唯一一本关于SQL注入攻击与防御的专业书籍　　理解，发现、利用和防御SQL注入的最佳指导
见解精辟，丰富、精彩的SQL注入示例及防御策略　　作者多年长期实践经验的总结

版权说明