DELL Technologies

提示/SQL 注入攻击防护：Dell Technologies 助力提高网络安全和弹性

提示/SQL 注入攻击的威胁不断增加

提示注入和 SQL 注入攻击已被反复证明是网络犯罪分子使用的极具破坏性和普遍性的网络攻击手段。这些攻击利用了用户查询或数据库系统中的漏洞，使恶意攻击者能够操纵服务器、窃取数据或中断工作流。随着数据驱动型应用程序的日益普及，攻击面也随之扩大，这使得提示注入和 SQL 注入技术对所有行业都构成了更为严峻的威胁。

无论是电子商务平台还是金融机构，攻击者都能利用这些漏洞在未经授权的情况下访问敏感数据，这凸显了开发先进防御手段的紧迫性。Dell Technologies 认识到这些挑战的严重性，并提供了创新且可扩展的解决方案，以保护企业免受提示注入和 SQL 注入攻击的威胁。

提示/SQL 注入攻击概览

它们是什么？

- **提示注入攻击**是指攻击者通过利用恶意输入来操纵 AI 或自动化提示。这些攻击会误导诸如 AI 聊天机器人之类的系统，进而导致出现意外或有害行为。
- **SQL 注入攻击**以在线数据库系统为目标。攻击者通过在输入字段（如登录或搜索表单）中注入恶意的 SQL 查询来操纵和控制后端数据库。

攻击原理

提示注入过程：

1. 攻击者通过利用含糊不清或设计拙劣的指令来操纵提示信息，从而生成有害的输出结果。
2. 这种攻击通常针对的是那些被用于客户服务、数据分析或辅助决策的 AI 系统。

SQL 注入过程：

1. 攻击者将恶意 SQL 代码注入易受攻击的应用程序的输入字段中。
2. 被攻击的系统将执行这些指令，从而给予攻击者未经授权地访问、删除数据或掌控系统的能力。

常见技术

- **基于联合查询的 SQL 注入：**通过联合查询从数据库中提取信息。
- **基于错误的注入技术：**通过构造特殊查询语句触发错误，从而获取数据库结构信息。
- **提示过载或混淆：**提交恶意指令，以覆盖 AI 或基于规则的输出。

对企业的影响

提示词/SQL 注入攻击产生的连锁效应远远超出了即时事件本身。一些最为严重的后果包括：

财务成本

这些攻击造成的直接损失包括客户数据和交易记录被盗，通常会导致监管部门罚款。一起针对金融机构的 SQL 注入攻击事件，导致涉事企业在诉讼费用、用户赔偿金以及新增安全措施方面损失近 4000 万美元。

运营中断

针对后端数据库的 SQL 注入攻击可能导致系统崩溃，造成工作流瘫痪及关键服务中断。受影响企业的平均停机时间估计在 18 到 24 小时之间，这会导致生产力显著下降。

名誉损害

针对 AI 平台的提示注入攻击常导致信息误导或决策失误。商业机密泄露或服务出现安全问题都会降低客户信任，损害合作关系。

现实案例

一家零售公司的支付平台遭遇 SQL 注入攻击，导致客户银行卡信息泄露，并造成服务中断数日。处理该事件需要进行监管报备、支付近 **300 万美元**的客户赔偿金以及承担诉讼费用。

警报统计信息

Akamai 发布的《互联网现状报告》（数据涵盖 2017-2019 年度）显示，SQL 注入攻击占所有 Web 应用程序攻击的比例达到近 **三分之二（约 65%）**。

在 OWASP 2025 年度十大安全风险榜单中，提示注入攻击被列为 **大语言模型 (LLM)** 的首要安全威胁

数据来源：2025 年 OWASP 十大安全风险榜单

针对提示/SQL 注入攻击的 Dell Technologies 防护解决方案

Dell Technologies 为企业提供了一整套工具与防护机制生态系统，专门用于抵御提示注入和 SQL 注入等复杂攻击。

戴尔可信设备赋能端点安全

端点是接入公司网络的门户。戴尔可信设备在硬件层面嵌入安全机制，以提供强大且不折不扣的防护保障。

- **Dell SafeID** 通过增强的基于硬件的身份验证来保护用户凭据。
- **SafeData** 会对静态和传输中的敏感数据进行加密，有效防范 SQL 注入攻击期间的数据泄露风险。

借助 CrowdStrike 实现主动威胁检测

由 CrowdStrike 提供支持的戴尔主动检测工具利用 AI 来识别和消除异常行为。

- **实时监视：**确保在混合环境中立即标记提示或 SQL 异常。
- **威胁遏制：**基于 AI 的算法可隔离网络上受影响的节点，以防止威胁大范围蔓延。

一家跨国制造公司通过使用主动威胁检测技术，先发制人地拦截了针对其工业数据库的 SQL 注入攻击企图，避免了可能高达数百万美元的停机损失。

戴尔服务器与存储安全解决方案

- **可信服务器：**通过强化服务器防入侵能力，为数据库应用程序提供安全保障。
- **自适应工作负载安全：**防止未经授权的恶意代码执行或注入违规行为。

Dell PowerProtect 数据完整性保障方案

- **不可变备份：**增强的弹性保障机制确保即使数据库或提示信息受损，仍能实现数据恢复。
- **物理隔离存储：**在物理和逻辑上隔离恢复点，有效缓解 SQL 注入攻击的回退操纵风险。

例如，某电信运营商在遭遇基于 SQL 注入的勒索软件攻击时，利用 Dell PowerProtect 的备份隔离功能，在 48 小时内恢复运营，避免了重大损失。

通过 Dell PowerSwitch Networking 与 SmartFabric OS 实现先进网络安全与微隔离解决方案

在整个基础架构中实现高级网络分段、严格的访问控制和实时流量分析，有效增强针对零日攻击的防御能力。

战略性地运用合作伙伴关系

- **Microsoft：**为 Azure 和 SQL Server 等广泛使用的平台提供针对查询式注入攻击的集成防御方案。
- **CrowdStrike 与 Secureworks：**通过高级威胁情报和定制化事件响应能力，结合戴尔基础架构协同增强整体防护弹性。

制定多层安全战略

企业应采取的关键行动

- **采用零信任框架：**对所有用户和系统命令进行全面验证。
- **安全编码实践：**开发人员应清理用户输入，并部署能抵御 SQL 注入的代码。
- **加密协议：**使用高级加密算法保护数据传输和存储内容。
- **员工培训：**对员工进行培训，使其能够识别输入异常、警惕网络钓鱼攻击，并防范恶意提示词的篡改。
- **系统审查与测试：**通过定期漏洞检查确保针对提示注入和 SQL 注入的防御措施持续保持更新。

戴尔的体系结构同时应用了上述所有原则，为客户打造了统一的安全平台。

利用 Dell Professional Services

从事件响应到日常监控，Dell Professional Services 可通过个性化方法为企业提供帮助。专业团队能够评估风险、实施稳健的防御措施，并在面临威胁时提供快速补救方案。

Dell Technologies 助力守护核心数据安全

应对提示注入与 SQL 注入等复杂网络攻击，需要采取主动防御策略。Dell Technologies 是您值得信赖的合作伙伴，致力于为您提供先进的工具、战略性的合作伙伴关系以及专业的服务。

要实现面向未来的稳健运营和赢得客户的信任，一切都始于预防性的解决方案。立即联系 Dell Technologies，守护数据安全、构建弹性体系，助您在数字时代蓬勃发展。

同心协力，守护核心价值。

如需了解如何应对当今重大的网络安全挑战，请访问 **Dell.com/SecuritySolutions**

详细了解
戴尔解决方案

联系 Dell Technologies
专家

查看更多资源

加入 #HashTag 对话

DELL Technologies