DELL Technologies

プロンプト/SQLインジェクション：デル・テクノロジーズでサイバーセキュリティとレジリエンスを強化

プロンプト/SQLインジェクション攻撃による脅威の増加

プロンプト インジェクション攻撃とSQLインジェクション攻撃は、サイバー犯罪者が使用するサイバー攻撃手法の中で、最も被害が大きく広範に及ぶことが幾度となく証明されてきました。これらの攻撃は、ユーザー クエリーやデータベース システムの脆弱性を悪用するもので、サイバー攻撃者にサーバーの操作、データの窃取、ワークフローの妨害を行う余地を与えます。データ主導型アプリケーションへの依存の高まりに伴い、攻撃対象領域が拡大し、あらゆる業界でSQLインジェクションの脅威が深刻化しています。

Eコマース プラットフォームから金融機関に至るまで、攻撃者はこうした抜け穴を悪用して機密データへの不正アクセスを試みており、高度な対策が緊急に必要であることは明白です。デル・テクノロジーズは、こうした課題の重要性を認識しており、プロンプト インジェクション攻撃やSQLインジェクション攻撃から企業を保護するための革新的で拡張性のあるソリューションを提供しています。

プロンプト/SQLインジェクション攻撃とは

概要

- **プロンプト インジェクション攻撃**とは、悪意のある入力によってAIや自動化プロンプトを操作するものです。このような攻撃はAIチャットボットなどのシステムを混乱させ、予期しないアクションや有害なアクションを引き起こします。
- **SQLインジェクション攻撃**は、オンライン データベース システムを標的にします。攻撃者は悪意のあるSQLクエリーを入力フィールド（ログイン フォームや検索フォームなど）に挿入して、バックエンド データベースの操作や制御を行います。

攻撃の仕組み

プロンプト インジェクションのプロセス：

1. 攻撃者は、あいまいな指示や不適切に設計された指示を悪用してプロンプトを操作し、有害な出力を生成します。
2. 多くの場合、カスタマー サービス、分析、意思決定に使用されるAIシステムが標的となります。

SQLインジェクションのプロセス：

1. 脆弱なアプリケーションの入力フィールドに悪意のあるSQLコードが挿入されます。
2. 侵害されたシステムでこれらの命令が実行され、不正なデータ アクセス、削除、システム制御が可能となります。

一般的な手法

- **ユニオンベースのSQLインジェクション：**クエリーを組み合わせて、データベースから情報を抽出します。
- **エラーベースの手法：**意図的に作成したクエリーを使用して、データベース構造を明らかにするエラーを生成します。
- **プロンプトによる過負荷（混乱）：**AIまたはルールベースの出力をオーバーライドする悪意のある指示を送信します。

ビジネスへの影響

プロンプト/SQLインジェクション攻撃の波及効果は、直接的に発生するインシデントをはるかに超えて広がります。最も有害な影響には次のようなものがあります。

財務コスト

こうした攻撃による直接的な損失には顧客データや取引記録の盗難などがあり、多くの場合、規制当局からの罰金が科せられます。SQLインジェクション攻撃により、ある金融機関は訴訟、補償、新たなセキュリティ対策のために約4000万ドルの損失を被りました。

業務の中断

バックエンド データベースを標的とするSQLインジェクションは、システムをクラッシュさせ、ワークフローを麻痺させ、重要なサービスを停止させる可能性があります。影響を受ける企業の平均ダウンタイムは18～24時間と推定され、生産性の大幅な低下を招きます。

風評被害

AIプラットフォームに対するプロンプト インジェクション攻撃が、誤った情報や不適切な意思決定につながることはよくあります。企業秘密の盗難やサービスの侵害は、お客様の信頼を失い、その関係を損なうことになります。

実例

ある小売店は、決済プラットフォームでSQLインジェクション攻撃を受け、顧客カードの詳細情報が漏えいし、サービスが数日停止しました。インシデントの処理には、規制当局への報告、約**300万ドル**の顧客補償費用、訴訟費用が必要となりました。

憂慮すべき統計

Akamaiの『インターネットの現状』レポート（2017～2019年を対象）によると、SQLインジェクションは、すべてのWebアプリケーション攻撃の約**3分の2（約65%）**を占めています。

OWASPは2025年のトップ10リストでプロンプト インジェクションを**最も深刻なLLM**セキュリティ リスクと認定

出典：OWASPのトップ セキュリティ リスク（2025年度版）

プロンプト/SQLインジェクション攻撃を防ぐデル・テクノロジーズのソリューション

デル・テクノロジーズは、プロンプト インジェクションやSQLインジェクションなどの高度な攻撃に対抗できるようカスタマイズされたツールと保護メカニズムのエコシステムを提供しています。

Dell Trusted Deviceによるエンドポイント セキュリティ

エンドポイントは、企業ネットワークへのゲートウェイです。Dell Trusted Deviceは、ハードウェア レベルでセキュリティを組み込んでおり、堅牢で妥協のない保護が可能です。

- **Dell SafeID**が、強化されたハードウェアベースの認証でユーザー資格情報を保護します。
- **SafeData**で、転送中と保存中の両方の機密データを暗号化して、SQLインジェクション攻撃による侵害から保護します。

CrowdStrikeによるプロアクティブな脅威検出

CrowdStrikeを搭載したDellのプロアクティブな検出ツールは、AIを活用して異常な行動を特定し、無力化します。

- **リアルタイム監視：**ハイブリッド環境全体でプロンプトまたはSQLの異常を即時にフラグ付けします。
- **脅威の封じ込め：**AIベースのアルゴリズムにより、ネットワーク上の影響を受けるノードを隔離し、本格的な侵害を防ぎます。

ある多国籍製造企業は、プロアクティブな脅威検出を使用し、産業用データベースを標的としたSQLインジェクション クエリーの試みを事前に阻止し、数百万ドル規模の潜在的なダウンタイムを回避しました。

Dellサーバーおよびストレージのセキュリティ

- **信頼できるサーバー：**侵害試行に対するサーバーの強化により、データベース アプリケーションを保護します。
- **適応型ワークロード セキュリティ：**悪意のあるコードやインジェクションの不正な実行を防止します。

データの整合性を確保するDell PowerProtect

- **不変バックアップ：**レジリエンスの強化により、データベースやプロンプトが破損している場合でもリカバリーが可能です。
- **エアギャップ型ストレージ：**リカバリー ポイントを物理的および論理的に分離し、SQLインジェクションによるフォールバック操作を軽減します。

例えば、ある通信事業者は、SQLインジェクション ベースのランサムウェア攻撃を受けた際、Dell PowerProtectのバックアップ分離機能を使用したことで、48時間以内に業務を復旧し、重大な損失を回避しました。

Dell PowerSwitch NetworkingとSmartFabric OSによる高度なネットワーク セキュリティとマイクロセグメンテーション

インフラストラクチャ全体で高度なネットワーク セグメンテーション、厳格なアクセス制御、リアルタイムのトラフィック分析を行うことで、ゼロデイ攻撃に対する防御を強化します。

パートナーシップの戦略的活用

- **Microsoft：**AzureやSQL Serverなど、広く使用されているプラットフォームでのクエリーベースのインジェクションに対する統合防御を提供します。
- **CrowdStrikeとSecureworks：**高度な脅威インテリジェンスとカスタマイズされたインシデント対応をDellのインフラストラクチャと組み合わせ、全体的なレジリエンスを強化します。

多層セキュリティ戦略の構築

企業が実施すべき主要アクション

- **ゼロトラスト フレームワーク：**すべてのユーザーとシステム コマンドの包括的な検証を実装します。
- **安全なコーディング プラクティス：**開発者は、ユーザー入力をサニタイズし、SQLインジェクション攻撃に耐性のあるコードを導入する必要があります。
- **暗号化プロトコル：**高度な暗号化アルゴリズムでデータ転送とストレージを保護します。
- **従業員トレーニング：**入力異常、フィッシング詐欺、悪意のあるプロンプト操作を認識するよう従業員を教育します。
- **システムの監査とテスト：**定期的な脆弱性チェックにより、プロンプト/SQLインジェクションの防御が最新の状態に保たれます。

Dellのアーキテクチャでは、これらすべての原則を同時に適用して、お客様のための極めて安全なプラットフォームを構築しています。

Dell Professional Servicesの活用

Dell Professional Servicesでは、インシデント対応から日常的なモニタリングまで、パーソナライズされたアプローチで企業を支援しています。熟練のチームがリスクを評価し、堅牢な防御を実装し、脅威発生時に迅速な修復を行います。

最も重要なものをデル・テクノロジーズで保護

プロンプト インジェクションやSQLインジェクションによる巧妙なサイバーセキュリティ攻撃に対抗するには、プロアクティブなアプローチが必要です。デル・テクノロジーズはパートナーとして、最先端のツール、戦略的パートナーシップ、エキスパート サービスを提供しています。

運用整合性とお客様の信頼が確保された未来は、予防的ソリューションから始まります。データの保護、レジリエンスの構築、デジタル世界での成功については、デル・テクノロジーズにお問い合わせください。

最も重要なものを協力して守りましょう。

今日のサイバーセキュリティの重要課題に対処する方法をご確認ください：**Dell.com/SecuritySolutions**

Dellのソリューションの詳細についてはこちら

デル・テクノロジーズのエキスパートへのお問い合わせ

他のリソースを表示

#HashTag で会話に参加

DELL Technologies