DELL Technologies

Injection d'invites/SQL : renforcer la cybersécurité et la résilience avec Dell Technologies

La menace grandissante des attaques par injection d'invites/SQL

Les attaques par injection d'invites et SQL comptent parmi les méthodes de cyberattaque les plus dommageables et les plus couramment utilisées par les cybercriminels. Ces attaques exploitent les failles de sécurité des systèmes de requêtes utilisateur ou de bases de données, et permettent à des acteurs malveillants de manipuler des serveurs, de voler des données ou de perturber des workflows. La dépendance croissante aux applications basées sur les données a élargi la surface d'attaque, faisant des techniques d'injection d'invites et SQL des menaces plus importantes dans tous les secteurs d'activité.

Visant des plateformes de commerce électronique comme des établissements financiers, les cyberattaquants exploitent ces failles pour accéder illégalement à des données sensibles. Les entreprises doivent donc se doter de manière urgente de mesures de protection avancées. Sachant l'importance de ces enjeux, Dell Technologies propose des solutions innovantes et évolutives pour protéger les entreprises contre les attaques par injection d'invites et SQL.

Présentation des attaques par injection d'invites/SQL

De quoi s'agit-il ?

- **Les attaques par injection d'invites** consistent à manipuler des invites d'IA ou d'automatisation à l'aide d'entrées malveillantes. Ces attaques perturbent des systèmes tels que les chatbots IA, provoquant des actions inattendues ou dommageables**.**
- **Les attaques par injection SQL** ciblent les systèmes de bases de données en ligne. Les cyberattaquants placent des requêtes SQL malveillantes dans des champs de saisie (formulaires de connexion ou de recherche, par exemple) afin de manipuler et de contrôler des bases de données back-end.

Fonctionnement

Injection d'invites :

1. Les cyberattaquants manipulent des invites pour générer des résultats dommageables en exploitant des instructions ambiguës ou mal formulées.
2. Ce type d'attaque cible souvent des systèmes d'IA utilisés dans le cadre du service client, de l'analytique ou de la prise de décisions.

Injection SQL :

1. Un code SQL malveillant est injecté dans les champs de saisie d'une application vulnérable.
2. Le système attaqué exécute ces instructions, permettant un accès non autorisé aux données, leur suppression ou la prise de contrôle du système.

Techniques courantes

- **Injection SQL basée sur UNION :** combinaison de requêtes visant à extraire des informations de la base de données.
- **Techniques basées sur les erreurs :** utilisation de requêtes créées dans le but de produire des erreurs révélant la structure de la base de données.
- **Surcharge d'invites ou confusion :** envoi d'instructions malveillantes qui remplacent les sorties basées sur l'IA ou des règles.

Répercussions pour les entreprises

Les effets d'une attaque par injection d'invites/SQL vont bien au-delà de l'incident immédiat. Voici certaines des conséquences les plus néfastes :

Coûts financiers

Ces attaques entraînent des pertes directes telles que le vol de données clients et d'enregistrements de transactions, ce qui peut donner lieu à des amendes réglementaires. Une attaque par injection SQL visant un établissement financier a coûté à cette société près de 40 millions de dollars en litiges, remboursements et nouvelles mesures de sécurité.

Interruptions des opérations

Les injections SQL ciblant les bases de données back-end peuvent provoquer des pannes système, paralyser les workflows et interrompre des services indispensables. On estime que les entreprises concernées connaissent une interruption de service moyenne de 18 à 24 heures, avec des pertes de productivité considérables.

Atteinte à la réputation

Les attaques par injection d'invites sur les plateformes d'IA provoquent souvent de la désinformation ou une mauvaise prise de décisions. Le vol de secrets commerciaux ou la compromission de services nuit à la confiance des clients et détériore les relations.

Exemple concret

Une entreprise de vente au détail a été confrontée à une injection SQL sur sa plateforme de paiement, avec une compromission des données de carte bancaire de ses clients et une interruption de ses services pendant plusieurs jours. La gestion de l'incident a nécessité des démarches réglementaires et lui a coûté près de **3 millions de dollars** en indemnisation des clients; ainsi que des frais de contentieux.

Statistiques alarmantes

L'injection SQL représente près des **deux tiers (environ 65 %)** des attaques d'applications Web, selon le rapport « État des lieux d'Internet » d'Akamai (couvrant la période 2017-2019).

L'OWASP a identifié l'injection d'invites comme le risque de sécurité **n° 1 pour les LLM** dans sa liste des 10 principaux risques de 2025.

Source : 2025: OWASP Top Security Risks

Les solutions de Dell Technologies pour lutter contre les injections d'invites/SQL

Dell Technologies propose aux entreprises un écosystème d'outils et de mécanismes de protection adaptés pour contrer les attaques sophistiquées telles que les injections d'invites et SQL.

Sécurité des points de terminaison avec Dell Trusted Devices

Les points de terminaison constituent les principaux accès aux réseaux de l'entreprise. Dell Trusted Devices intègre la sécurité au niveau matériel pour une protection robuste et sans faille.

- **Dell SafeID** sécurise les informations d'identification des utilisateurs grâce à une authentification matérielle renforcée.
- **SafeData** chiffre les données sensibles en transit et au repos, les protégeant contre toute compromission lors des attaques par injection SQL.

Détection proactive des menaces avec CrowdStrike

Les outils de détection proactive de Dell optimisés par CrowdStrike utilisent l'IA pour identifier et neutraliser les comportements anormaux.

- **Surveillance en temps réel :** garantit que les anomalies liées aux invites ou au code SQL sont immédiatement signalées dans les environnements hybrides.
- **Gestion des menaces :** des algorithmes basés sur l'IA isolent les nœuds concernés sur le réseau afin d'éviter toute extension de la compromission.

Une multinationale du secteur de la fabrication utilisant la détection proactive des menaces est parvenue à bloquer en amont des tentatives d'injection SQL ciblant ses bases de données industrielles, évitant ainsi des interruptions de service susceptibles d'engendrer plusieurs millions de dollars de pertes.

Sécurité des serveurs et du stockage proposée par Dell

- **Serveurs de confiance :** sécurisez vos applications de base de données en protégeant vos serveurs contre les tentatives de violation.
- **Sécurité adaptative des charges applicatives :** empêche l'exécution non autorisée de code malveillant ou les injections.

Dell PowerProtect pour l'intégrité des données

- **Sauvegardes immuables :** une résilience accrue garantit la récupération même en cas de corruption des bases de données ou des invites.
- **Stockage air-gapped :** isole physiquement et logiquement les points de récupération, ce qui limite la manipulation des mécanismes de secours par injection SQL.

Lors d'une attaque par rançongiciel reposant sur une injection SQL, un fournisseur de télécommunications a par exemple restauré ses opérations en moins de 48 heures grâce aux isolements de sauvegardes de Dell PowerProtect, évitant ainsi des pertes majeures.

Sécurité réseau avancée et microsegmentation avec Dell PowerSwitch Networking et SmartFabric OS

Protège contre les attaques « Zero-Day » en fournissant une segmentation avancée du réseau, des contrôles d'accès stricts et une analyse du trafic en temps réel sur l'ensemble de votre infrastructure.

Utilisation stratégique des partenariats

- **Microsoft :** mécanismes de défense intégrés contre les injections basées sur des requêtes sur des plateformes largement utilisées comme Azure et SQL Server**.**
- **CrowdStrike & Secureworks :** une cyber-intelligence avancée et des réponses sur mesure aux incidents renforcent la résilience globale, en complément de l'infrastructure Dell.

Mise en place d'une stratégie de sécurité multicouche

Mesures clés à mettre en œuvre par les entreprises

- **Cadre Zero-Trust :** mettez en place une validation complète pour tous les utilisateurs et toutes les commandes système.
- **Pratiques de codage sécurisé :** les développeurs doivent nettoyer les entrées utilisateur et déployer du code conçu pour résister aux injections SQL.
- **Protocoles de chiffrement :** protégez la transmission et le stockage des données grâce à des algorithmes de chiffrement avancés.
- **Formation des employés :** formez le personnel à reconnaître les entrées anormales, les tentatives d'hameçonnage et les manipulations malveillantes d'invites.
- **Tests et audits des systèmes :** des contrôles réguliers des failles de sécurité permettent de s'assurer que les mécanismes de défense contre les injections d'invites et SQL restent à jour.

L'architecture Dell applique tous ces principes simultanément, créant des plateformes sécurisées pour ses clients.

Tirer parti de Dell Professional Services

De la réponse aux incidents à la surveillance quotidienne, Dell Professional Services aide les entreprises grâce à une approche sur mesure. Des équipes qualifiées évaluent les risques, mettent en œuvre des mécanismes de défense robustes et proposent des mesures correctives rapides face aux menaces.

Sécuriser ce qui compte le plus avec Dell Technologies

Face à la sophistication des cyberattaques par injection d'invites et SQL, les entreprises doivent adopter une approche proactive. Dell Technologies vous accompagne en vous proposant des outils de pointe, des partenariats stratégiques et les services d'experts.

La pérennité des opérations et la confiance des clients passent par la mise en place de solutions préventives. Contactez Dell Technologies dès aujourd'hui pour sécuriser vos données, renforcer la résilience et prospérer à l'ère numérique.

Ensemble, nous protégeons ce qui compte le plus.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **Dell.com/SecuritySolutions**

En savoir plus sur les solutions Dell

Contacter un expert Dell Technologies

Consulter d'autres ressources

Prenez part à la discussion avec #hashtag

DELL Technologies