DELL Technologies

Injeção de prompt e SQL: Fortalecendo a resiliência e a segurança cibernética com a Dell Technologies

A crescente ameaça de ataques de Injeção de prompt e SQL

Ataques de injeção de prompt e SQL têm se mostrado repetidamente entre os métodos mais prejudiciais e difundidos de ataques cibernéticos usados por cibercriminosos. Esses ataques exploram vulnerabilidades em sistemas de banco de dados ou consulta do usuário, permitindo que agentes mal-intencionados manipulem servidores, roubem dados ou interrompam fluxos de trabalho. O aumento da dependência de aplicativos orientados por dados expandiu a superfície de ataque, tornando as técnicas de injeção de prompt e SQL ameaças mais significativas em todos os setores.

De plataformas de comércio eletrônico a instituições financeiras, os invasores exploram essas brechas para obter acesso não autorizado a dados confidenciais, demonstrando a necessidade urgente de contramedidas avançadas. A Dell Technologies reconhece a natureza crítica desses desafios e fornece soluções inovadoras e escaláveis para proteger as empresas contra ataques de injeção de prompt e SQL.

Compreendendo os ataques de injeção de prompt e SQL

O que são?

- **Ataques de injeção de prompt** consistem na manipulação de prompts de IA ou automação por entradas mal-intencionadas. Esses ataques confundem sistemas como chatbots de IA, levando a ações inesperadas ou prejudiciais**.**
- **Ataques de injeção de SQL** visam sistemas de banco de dados on-line. Os invasores inserem consultas SQL mal-intencionadas em campos de entrada (por exemplo, formulários de log-in ou pesquisa) para manipular e controlar bancos de dados de back-end.

Como eles funcionam

Processos de injeção de prompt:

1. Os invasores manipulam prompts para gerar resultados prejudiciais explorando instruções ambíguas ou mal elaboradas.
2. Isso geralmente tem como alvo os sistemas de IA usados para atendimento ao cliente, lógica analítica ou tomada de decisões.

Processos de injeção de SQL:

1. Um código SQL mal-intencionado é injetado em campos de entrada de um aplicativo vulnerável.
2. O sistema explorado executa essas instruções, permitindo acesso não autorizado a dados, exclusão ou controle do sistema.

Técnicas comuns

- **Injeção de SQL baseada em Union:** Combinando consultas para extrair informações do banco de dados.
- **Técnicas baseadas em erro:** Usando consultas criadas intencionalmente para produzir erros que revelam a estrutura do banco de dados.
- **Sobrecarga ou confusão de prompt:** Envio de instruções mal-intencionadas que substituem saídas baseadas em regras ou IA.

O impacto nos negócios

Os efeitos da propagação de um ataque de injeção de prompt e SQL vão muito além do incidente imediato. Algumas das consequências mais prejudiciais incluem:

Custos financeiros

As perdas diretas desses ataques incluem registros de transações e dados de clientes roubados, muitas vezes levando a multas regulatórias. Um ataque de injeção de SQL a uma instituição financeira custou à empresa cerca de US$ 40 milhões em litígios, reembolsos e novas medidas de segurança.

Disrupções operacionais

Injeções de SQL direcionadas a bancos de dados de back-end podem travar sistemas, paralisando fluxos de trabalho e interrompendo serviços essenciais. O tempo médio de inatividade das empresas afetadas é estimado entre 18 e 24 horas, causando perdas significativas de produtividade.

Danos à reputação

Ataques de injeção de prompt em plataformas de IA geralmente levam a informações erradas ou tomadas de decisão equivocadas. Segredos comerciais roubados ou serviços comprometidos desgastam a confiança do cliente e prejudicam relacionamentos.

Exemplo do mundo real

Uma empresa de varejo enfrentou uma injeção de SQL em sua plataforma de pagamento, comprometendo os detalhes dos cartões dos clientes e interrompendo os serviços por dias. A limpeza do incidente exigiu relatórios regulatórios, quase **US$ 3 milhões** em indenizações aos clientes e custos de litígio.

Estatísticas alarmantes

A injeção de SQL representa quase **dois terços (~65%)** de todos os ataques a aplicativos da Web, de acordo com o relatório "State of the Internet" da Akamai (abordando de 2017 a 2019).

O OWASP reconheceu a injeção de prompt como o **principal risco de segurança de LMM** em lista com as 10 principais vulnerabilidades de 2025

Fonte: 2025: OWASP Top Security Risks

Soluções da Dell Technologies para defesa de injeção de SQL/prompt

A Dell Technologies equipa as empresas com um ecossistema de ferramentas e mecanismos de proteção adaptados para combater ataques sofisticados, como injeções de prompt e SQL.

Segurança de endpoints com Dell Trusted Devices

Endpoints são os gateways para as redes da empresa. Os Dell Trusted Devices incorporam segurança no nível de hardware para proteção robusta e inflexível.

- **O Dell SafeID** protege as credenciais dos usuários com autenticação aprimorada baseada em hardware.
- **O SafeData** criptografa dados confidenciais em trânsito e em repouso, protegendo contra comprometimento durante explorações de injeção de SQL.

Detecção proativa de ameaças com a CrowdStrike

As ferramentas de detecção proativa da Dell, desenvolvidas pela CrowdStrike, utilizam a IA para identificar e neutralizar comportamentos anormais.

- **Monitoramento em tempo real:** Garante que anomalias de prompt ou SQL sejam sinalizadas imediatamente em ambientes híbridos.
- **Contenção de ameaças:** Algoritmos baseados em IA isolam os nós afetados na rede para evitar um comprometimento completo.

Uma empresa multinacional de manufatura que utiliza detecção proativa de ameaças interrompeu de forma preventiva tentativas de consultas de injeção de SQL direcionadas a seus bancos de dados industriais, economizando milhões em possíveis períodos de inatividade.

Segurança de servidor e armazenamento da Dell

- **Servidores confiáveis:** Proteja aplicativos de banco de dados, fortalecendo os servidores contra tentativas de violação.
- **Segurança adaptável de carga de trabalho:** Impede execução não autorizada de código mal-intencionado ou injeções.

Dell PowerProtect para integridade dos dados

- **Backups imutáveis:** A resiliência aprimorada garante a recuperação mesmo que bancos de dados ou prompts sejam corrompidos.
- **Armazenamento com air gap:** Isola física e logicamente os pontos de recuperação, evitando a manipulação de fallback de injeção de SQL.

Por exemplo, durante um ataque de ransomware baseado em injeção de SQL, um provedor de telecomunicações restaurou as operações em menos de 48 horas usando os isolamentos de backup do Dell PowerProtect, evitando perdas críticas.

Segurança de rede avançada e microssegmentação com o Dell PowerSwitch Networking e o SmartFabric OS

Fortalece as defesas contra ataques de dia zero, oferecendo segmentação de rede avançada, controles de acesso rígidos e análise de tráfego em tempo real em toda a sua infraestrutura.

Uso estratégico de parcerias

- **Microsoft:** Defesas integradas contra injeções baseadas em consultas em plataformas amplamente utilizadas, como Azure e SQL Server**.**
- **CrowdStrike e Secureworks:** Inteligência contra ameaças avançadas e respostas a incidentes personalizadas reforçam a resiliência geral combinadas com a infraestrutura da Dell.

Desenvolvendo uma estratégia de segurança multicamadas

Principais ações que as empresas devem tomar

- **Estrutura Zero Trust:** Implemente uma validação abrangente para todos os usuários e comandos do sistema.
- **Práticas de codificação segura:** Os desenvolvedores devem limpar as entradas de usuário e implementar o uso de código resistente a injeções de SQL.
- **Protocolos de criptografia:** Proteja o armazenamento e as transmissões de dados com algoritmos avançados de criptografia.
- **Treinamento de funcionários:** Capacite sua equipe para identificar anomalias de entrada, tentativas de phishing e manipulação de prompts mal-intencionados.
- **Auditorias e testes do sistema:** As verificações rotineiras de vulnerabilidades garantem que as defesas de injeção de prompt e SQL permaneçam atualizadas.

A arquitetura da Dell aplica todos esses princípios simultaneamente, criando plataformas singularmente seguras para seus clientes.

Aproveitando o Dell Professional Services

Da resposta a incidentes ao monitoramento diário, os Dell Professional Services auxiliam as empresas com uma abordagem personalizada. Equipes qualificadas avaliam riscos, implementam defesas robustas e oferecem correção rápida diante de ameaças.

Protegendo o que é mais importante com a Dell Technologies

O combate à natureza sofisticada de ataques de segurança cibernética de injeção de prompt e SQL requer uma abordagem proativa. A Dell Technologies é sua parceira, oferecendo ferramentas de ponta, parcerias estratégicas e serviços especializados.

O futuro da integridade operacional e da confiança do cliente começa com soluções preventivas. Entre em contato com a Dell Technologies hoje mesmo para proteger seus dados, desenvolver resiliência e prosperar no mundo digital.

Juntos, protegemos o que é mais importante.

Saiba como enfrentar alguns dos principais desafios atuais de segurança cibernética em **Dell.com/SecuritySolutions**

Saiba mais sobre as soluções Dell

Entre em contato com um especialista da Dell Technologies

Veja mais recursos

Participe da conversa com #HashTag

DELL Technologies