DELL Technologies

프롬프트/SQL 삽입: Dell Technologies를 통한 사이버 보안 및 회복탄력성 강화

증가하는 프롬프트/SQL 삽입 공격 위협

프롬프트 및 SQL 삽입 공격은 사이버 범죄자가 이용하는 가장 위험하고 보편적인 사이버 공격 방법 중 하나임이 반복적으로 입증되었습니다. 이러한 공격은 사용자 쿼리 또는 데이터베이스 시스템의 취약성을 악용하여 악의적인 행위자가 서버를 조작하거나 데이터를 탈취하거나 워크플로를 중단시킬 수 있도록 합니다. 데이터 기반 애플리케이션에 대한 의존도가 높아짐에 따라 공격 노출 지점이 확대되면서 프롬프트 및 SQL 삽입 기법은 모든 산업 분야에서 더욱 심각한 위협이 되었습니다.

전자 상거래 플랫폼에서 금융 기관에 이르기까지 공격자는 이러한 허점을 악용하여 기밀 데이터에 무단으로 액세스함으로써 고급 대응책이 시급히 필요하다는 것을 보여줍니다. Dell Technologies는 이러한 당면 과제의 중요한 특성을 인식하며 혁신적이고 확장 가능한 솔루션을 제공하여 프롬프트 및 SQL 삽입 공격으로부터 비즈니스를 보호합니다.

프롬프트/SQL 삽입 공격 이해

어떤 기능일까요?

- **프롬프트 삽입 공격**은 악의적인 입력을 통해 AI 또는 자동화 프롬프트 조작을 감행합니다. 이러한 공격은 AI 챗봇과 같은 시스템에 혼란을 야기하여 예기치 않은 동작이나 유해한 동작을 초래합니다.
- **SQL 삽입 공격**은 온라인 데이터베이스 시스템을 대상으로 합니다. 공격자는 악성 SQL 쿼리를 입력 필드(예: 로그인 또는 검색 양식)에 삽입하여 백엔드 데이터베이스를 조작하고 제어합니다.

작동 방식

프롬프트 삽입 프로세스:

1. 공격자가 모호하거나 부실하게 설계된 명령을 악용하여 유해한 출력을 생성하기 위해 프롬프트를 조작합니다.
2. 이는 고객 서비스, 분석 또는 의사 결정에 사용되는 AI 시스템을 대상으로 하는 경우가 많습니다.

SQL 삽입 프로세스:

1. 악성 SQL 코드가 취약한 애플리케이션의 입력 필드에 삽입됩니다.
2. 악용된 시스템은 이러한 명령을 실행하여 무단 데이터 액세스, 삭제 또는 시스템 제어를 활성화합니다.

일반적인 기법

- **통합 기반 SQL 삽입:** 쿼리를 결합하여 데이터베이스에서 정보를 추출합니다.
- **오류 기반 기법:** 의도적으로 작성된 쿼리를 사용하여 데이터베이스 구조를 드러내는 오류를 발생시킵니다.
- **프롬프트 과부하 또는 혼란:** AI 또는 규칙 기반 출력을 무력화하는 악성 명령을 제시합니다.

© 2025 Dell Inc. or its subsidiaries.

비즈니스에 미치는 영향

프롬프트/SQL 삽입 공격의 파급 효과는 당장의 인시던트에만 국한되지 않습니다. 가장 유해한 결과 중 일부는 다음과 같습니다.

재무 비용

이러한 공격으로 인한 직접적인 손실에는 고객 데이터 및 거래 기록 도난이 포함되며, 이로 인해 규제 벌금이 부과되는 경우가 많습니다. 금융 기관에 대한 SQL 삽입 공격으로 인해 회사는 소송, 보상, 새로운 보안 조치에 거의 4천만 달러를 지출합니다.

운영 중단

백엔드 데이터베이스를 대상으로 하는 SQL 삽입은 시스템을 충돌시키고 워크플로를 마비시키며 필수 서비스를 중단시킬 수 있습니다. 영향을 받는 비즈니스의 평균 다운타임은 18~24시간으로 추정되며, 이로 인해 상당한 생산성 손실이 발생합니다.

평판 훼손

AI 플랫폼에 대한 프롬프트 삽입 공격은 잘못된 정보나 부적절한 의사 결정으로 이어지는 경우가 많습니다. 영업 비밀 도난 또는 서비스 침해는 고객 신뢰를 저해하고 관계를 손상시킵니다.

실제 업무 환경의 예

한 소매업체는 결제 플랫폼에 SQL 삽입 공격을 받아서 고객 카드 세부 정보가 유출되었고 며칠 동안 서비스가 중단되었습니다. 이 인시던트를 해결하는 과정에서 규제 당국에 보고를 해야 했고, 고객 보상 및 소송 비용으로 약 **300만 달러**가 들었습니다.

경각심을 불러일으키는 통계

Akamai의 "인터넷 현황" 보고서(2017~2019년)에 따르면 SQL 삽입은 모든 웹 애플리케이션 공격의 거의 **2/3(약 65%)**를 차지합니다.

OWASP는 2025년도 상위 10개 목록에서 프롬프트 삽입을

#1 LLM

보안 위험으로 선정

출처: 2025년: OWASP 주요 보안 위험

프롬프트/SQL 삽입 방어를 위한 Dell Technologies 솔루션

Dell Technologies는 프롬프트 및 SQL 삽입과 같은 정교한 공격에 대응하도록 맞춤화된 툴과 보호 메커니즘의 생태계를 기업에 제공합니다.

Dell Trusted Devices를 통한 엔드포인트 보안

엔드포인트는 회사 네트워크의 게이트웨이입니다. Dell Trusted Device는 하드웨어 수준에서 보안을 내장하여 강력하고 타협 없는 보호를 제공합니다.

- **Dell SafeID**는 향상된 하드웨어 기반 인증을 통해 사용자 자격 증명을 보호합니다.
- **SafeData**는 전송 중이거나 저장 상태인 기밀 데이터를 모두 암호화하여 SQL 삽입 악용 시 손상을 방지합니다.

CrowdStrike를 통한 사전 예방적 위협 탐지

CrowdStrike 기반의 Dell 사전 예방적 탐지 툴은 AI를 활용하여 비정상적인 동작을 식별하고 무력화합니다.

- **실시간 모니터링:** 하이브리드 환경에서 프롬프트나 SQL 이상 징후가 발견되면 즉시 플래그를 지정합니다.
- **위협 억제:** AI 기반 알고리듬은 네트워크에서 영향을 받는 노드를 격리하여 본격적인 침해를 방지합니다.

사전 예방적 위협 탐지를 사용하고 있던 한 다국적 제조업체는 자사 산업 데이터베이스를 대상으로 하는 SQL 삽입 쿼리를 시도를 선제적으로 차단하여 잠재적 다운타임으로 인한 수백만 달러의 손실을 절감했습니다.

© 2025 Dell Inc. or its subsidiaries.

Dell의 서버 및 스토리지 보안

- **신뢰할 수 있는 서버:** 침해 시도로부터 서버를 강화하여 데이터베이스 애플리케이션을 보호합니다.
- **적응형 워크로드 보안:** 악성 코드 또는 삽입의 무단 실행을 방지합니다.

데이터 무결성을 위한 Dell PowerProtect

- **변경 불가능한 백업:** 향상된 회복탄력성으로 데이터베이스 또는 프롬프트가 손상된 경우에도 복구를 보장합니다.
- **에어 갭 스토리지:** 복구 지점을 물리적, 논리적으로 격리하여 SQL 삽입 대체 조작을 완화합니다 방지합니다.

예를 들어, SQL 삽입 기반 랜섬웨어 공격 발생 시, 한 통신사는 Dell PowerProtect의 백업 격리를 사용해 48시간 이내에 운영을 복원하여 심각한 손실을 피했습니다.

Dell PowerSwitch 네트워킹 및 SmartFabric OS를 통한 고급 네트워크 보안 및 마이크로 세분화

인프라스트럭처 전반에 걸쳐 고급 네트워크 세분화, 엄격한 액세스 제어, 실시간 트래픽 분석을 제공하여 제로데이 공격에 대한 방어를 강화합니다.

전략적 파트너십 활용

- **Microsoft:** Azure 및 SQL Server와 같이 널리 사용되는 플랫폼에서 쿼리 기반 삽입에 대한 통합 방어
- **CrowdStrike 및 Secureworks:** 고급 위협 인텔리전스와 맞춤형 인시던트 대응은 Dell의 인프라스트럭처와 결합되어 전반적인 회복탄력성을 강화합니다.

다중 계층 보안 전략 구축

기업이 취해야 할 주요 조치

- **제로 트러스트 프레임워크:** 모든 사용자 및 시스템 명령에 대한 포괄적인 검증을 구현합니다.
- **안전한 코딩 관행:** 개발자는 사용자 입력값을 정제하고 코드에 강한 SQL 삽입을 배포해야 합니다.
- **암호화 프로토콜:** 고급 암호화 알고리듬으로 데이터 전송 및 스토리지를 보호합니다.
- **직원 교육:** 직원들이 입력 이상, 피싱 시도, 악의적인 프롬프트 조작을 인식하도록 교육합니다.
- **시스템 감사 및 테스트:** 정기적인 취약성 점검을 통해 프롬프트 및 SQL 삽입 방어를 최신 상태로 유지합니다.

Dell의 아키텍처는 이러한 모든 원칙을 동시에 적용하여 고객을 위한 독보적이고 안전한 플랫폼을 구축합니다.

© 2025 Dell Inc. or its subsidiaries.

Dell Professional Services 활용

인시던트 대응부터 일상적인 모니터링까지, Dell의 전문 서비스는 맞춤형 접근 방식으로 기업을 지원합니다. 숙련된 팀이 위험을 평가하고, 강력한 방어 체계를 구현하며, 위협 발생 시 신속한 문제 해결을 제공합니다.

Dell Technologies를 통해 가장 중요한 데이터를 보호

프롬프트 및 SQL 삽입 사이버 보안 공격의 정교한 특성에 대처하려면 사전 예방적인 접근 방식이 필요합니다. Dell Technologies는 최첨단 툴, 전략적 파트너십, 전문가 서비스를 제공하는 파트너로서 함께합니다.

운영 무결성과 고객 신뢰의 미래는 예방적 솔루션에서 시작됩니다. 지금 바로 Dell Technologies에 문의하여 데이터를 보호하고, 회복탄력성을 구축하고, 디지털 세상에서 성공을 거두십시오.

다 함께 가장 중요한 것을 보호합니다.

Dell.com/SecuritySolutions에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.

Dell 솔루션에 대한 자세한 정보

Dell Technologies 전문가에게 문의

추가 리소스 보기

#HashTag로 대화에 참여하기

© 2025 Dell Inc. 또는 자회사. All Rights Reserved. Dell 및 기타 상표는 Dell Inc. 또는 해당 자회사의 상표입니다. 기타 모든 상표는 해당 소유주의 상표일 수 있습니다.

DELL Technologies