DELL Technologies

Szybkie wstrzyknięcie poleceń/ kodu SQL: Wzmacnianie cyberbezpieczeństwa i odporności dzięki Dell Technologies

Rosnące zagrożenie atakami polegającymi na szybkim wstrzyknięciu poleceń/kodu SQL:

Ataki polegające na szybkim wstrzyknięciu poleceń/kodu SQL wielokrotnie okazywały się jednymi z najbardziej szkodliwych i wszechobecnych metod cyberataku używanych przez cyberprzestępców. Ataki te wykorzystują luki w zabezpieczeniach systemów zapytań użytkowników lub baz danych, umożliwiając złośliwym podmiotom manipulowanie serwerami, kradzież danych lub zakłócanie przepływów pracy. Rosnące uzależnienie od aplikacji opartych na danych rozszerzyło powierzchnię ataku, dzięki czemu techniki wstrzyknięcia poleceń i kodu SQL stają się istotnymi zagrożeniami we wszystkich branżach.

Od platform handlu elektronicznego po instytucje finansowe — atakujący wykorzystują te luki w zabezpieczeniach, aby uzyskać nieautoryzowany dostęp do wrażliwych danych, co świadczy o pilnej potrzebie zastosowania zaawansowanych środków zaradczych. Firma Dell Technologies dostrzega krytyczny charakter tych wyzwań i zapewnia innowacyjne oraz skalowalne rozwiązania, które chronią firmy przed atakami polegającymi na szybkim wstrzyknięciu poleceń/kodu SQL.

Zrozumienie ataków polegających na szybkim wstrzyknięciu poleceń/kodu SQL

O jakie typy chodzi?

- **Ataki polegające na szybkim wstrzyknięciu poleceń** obejmują manipulację monitami sztucznej inteligencji lub automatyzacji przez złośliwe dane wejściowe. Ataki te mylą systemy, takie jak chatboty sztucznej inteligencji, co prowadzi do nieoczekiwanych lub szkodliwych działań**.**
- **Ataki polegającymi na szybkim wstrzyknięciu kodu SQL** celują w systemy baz danych online. Atakujący umieszczają złośliwe zapytania SQL w polach danych wejściowych (np. formularzach logowania lub wyszukiwania), aby manipulować i kontrolować bazy danych znajdujące się w tle.

Jak działają

Procesy wstrzyknięcia poleceń:

1. Atakujący manipulują poleceniami w celu generowania szkodliwych danych wyjściowych, wykorzystując niejednoznaczne lub źle zaprojektowane instrukcje.
2. Często dotyczy to systemów sztucznej inteligencji używanych do obsługi klienta, analizy lub podejmowania decyzji.

Procesy wstrzyknięcia kodu SQL:

1. Złośliwy kod SQL jest wstrzykiwany do pól danych wejściowych podatnej aplikacji.
2. Wykorzystany system wykonuje te instrukcje, umożliwiając nieautoryzowany dostęp do danych, ich usuwanie lub kontrolę nad systemem.

Typowe techniki

- **Wstrzykiwanie kodu SQL oparte na operatorze Union:** Łączenie zapytań w celu wyodrębnienia informacji z bazy danych.
- **Techniki oparte na błędach:** Używanie celowo spreparowanych zapytań do generowania błędów ujawniających strukturę bazy danych.
- **Przeciążenie lub dezorientacja polecenia:** przesyłanie złośliwych instrukcji, które nadpisują odpowiedzi AI lub wynik działania reguł.

© 2025 Dell Inc. lub podmioty zależne firmy.

Konsekwencje dla firm

Skutki uboczne ataku polegającego na szybkim wstrzyknięciu poleceń/kodu SQL wykraczają daleko poza samo zdarzenie. Niektóre z najbardziej szkodliwych skutków obejmują:

Koszty finansowe

Bezpośrednie straty wynikające z tych ataków obejmują skradzione dane klientów i dane dotyczące transakcji, często prowadzące do nałożenia kar regulacyjnych. Atak polegającymi na szybkim wstrzyknięciu kodu SQL na instytucję finansową kosztował firmę prawie 40 milionów dolarów w postaci kosztów sądowych, odszkodowań oraz wdrożenia nowych środków bezpieczeństwa.

Zakłócenia operacyjne

Wstrzyknięcia kodu SQL ukierunkowane na bazy danych zaplecza mogą spowodować awarię systemów, sparaliżowanie przepływów pracy i zatrzymanie podstawowych usług. Średni czas przestoju w firmach, których dotyczy problem, wynosi od 18 do 24 godzin i powoduje znaczne straty produktywności.

Uszczerbek na reputacji

Szybkie ataki na platformy sztucznej inteligencji często prowadzą do dezinformacji lub podejmowania niewłaściwych decyzji. Skradzione tajemnice handlowe lub naruszone usługi podważają zaufanie klientów i powodują szkody w relacjach.

Przykład z życia

Firma zajmująca się sprzedażą detaliczną padła ofiarą ataku za pomocą wstrzyknięcia kodu SQL na swoją platformę płatniczą, co spowodowało wyciek danych kart klientów i wstrzymanie usług na kilka dni. Usunięcie skutków incydentu wymagało zgłoszenia do organów regulacyjnych, wypłacenia prawie **3 milionów** dolarów odszkodowania klientom i poniesienia kosztów postępowania sądowego.

Organizacja OWASP uznała wstrzyknięcie poleceń za **największe** zagrożenie bezpieczeństwa związane z dużymi modelami językowymi (LLM), umieszczając je na pierwszym miejscu w zestawieniu Top 10 na rok 2025

Źródło: 2025: OWASP Top Security Risks

Alarmujące statystyki

Wstrzyknięcie kodu SQL stanowi prawie **dwie trzecie (~65%)** wszystkich ataków na aplikacje internetowe, zgodnie z raportem „State of the Internet" firmy Akamai (obejmującym lata 2017–2019).

Rozwiązania Dell Technologies do obrony przed atakami polegającymi na szybkim wstrzyknięciu poleceń/kodu SQL

Firma Dell Technologies wyposaża firmy w ekosystem narzędzi i mechanizmów ochrony dostosowanych do przeciwdziałania zaawansowanym atakom, takim jak wstrzyknięcia poleceń/kodu SQL.

Bezpieczeństwo punktów końcowych dzięki Dell Trusted Devices

Punkty końcowe to bramki do sieci firmowych. Dell Trusted Devices to wbudowane zabezpieczenia na poziomie sprzętowym, króre zapewnia solidną, bezkompromisową ochronę.

- **Dell SafeID** zabezpiecza poświadczenia użytkownika dzięki ulepszonemu uwierzytelnianiu sprzętowemu.
- **SafeData** szyfruje wrażliwe dane zarówno w ruchu, jak i w spoczynku, chroniąc przed naruszeniami bezpieczeństwa podczas ataków wstrzyknięcia SQL.

Proaktywne wykrywanie zagrożeń dzięki CrowdStrike

Narzędzia firmy Dell do proaktywnego wykrywania oparte na CrowdStrike wykorzystują sztuczną inteligencję do identyfikacji i neutralizowania nietypowych zachowań.

- **Monitorowanie w czasie rzeczywistym:** Zapewnia natychmiastowe oznaczanie monitów lub anomalii SQL w środowiskach hybrydowych.
- **Opanowywanie zagrożeń:** algorytmy oparte na sztucznej inteligencji izolują zainfekowane węzły w sieci, aby zapobiec pełnemu naruszeniu bezpieczeństwa.

Międzynarodowa firma produkcyjna, stosując proaktywne wykrywanie zagrożeń, z wyprzedzeniem zablokowała próby ataków wstrzyknięcia kodu SQL wymierzone w jej przemysłowe bazy danych, oszczędzając miliony dolarów potencjalnych strat związanych z przestojami.

© 2025 Dell Inc. lub podmioty zależne firmy.

Bezpieczeństwo serwerów i pamięci masowych od firmy Dell

- **Zaufane serwery:** Ochrona aplikacji baz danych poprzez wzmocnienie serwerów przed próbami naruszenia.
- **Adaptacyjne zabezpieczenie obciążeń roboczych:** Zapobiega nieautoryzowanemu wykonaniu lub wstrzyknięciu złośliwego kodu.

Dell PowerProtect dla integralności danych

- **Niezmienne kopie zapasowe:** Zwiększona odporność zapewnia odzyskiwanie nawet w przypadku uszkodzenia baz danych lub monitów.
- **Odizolowana pamięć masowa:** fizycznie i logicznie izoluje punkty odtwarzania, ograniczając ryzyko manipulacji w wyniku ataku wstrzyknięcia kodu SQL.

Na przykład podczas ataku ransomware opartego na wstrzyknięciu kodu SQL dostawca telekomunikacyjny przywrócił operacje w mniej niż 48 godziny przy użyciu izolacji kopii zapasowych Dell PowerProtect, unikając krytycznych strat.

Zaawansowane zabezpieczenia sieciowe i mikrosegmentacja dzięki rozwiązaniom Dell PowerSwitch Networking i SmartFabric OS

Wzmocnij ochronę przed atakami typu zero-day, zapewniając zaawansowaną segmentację sieci, ścisłą kontrolę dostępu i analizę ruchu w czasie rzeczywistym w całej infrastrukturze.

Strategiczne wykorzystanie partnerstw

- **Microsoft:** Zintegrowane mechanizmy obronne przed wstrzyknięciami opartymi na zapytaniach na powszechnie używanych platformach, takich jak Azure i SQL Server.
- **CrowdStrike i Secureworks:** Zaawansowana analiza zagrożeń i dostosowane do potrzeb reagowanie na incydenty zwiększają ogólną odporność w połączeniu z infrastrukturą firmy Dell.

Tworzenie wielowarstwowej strategii bezpieczeństwa

Kluczowe działania, które powinny podjąć firmy

- **Model „zero trust”:** Wdrożenie kompleksowej walidacji dla wszystkich użytkowników i poleceń systemowych.
- **Bezpieczne praktyki kodowania:** Programiści powinni oczyścić dane wejściowe użytkowników i wdrożyć odporne na kod wstrzyknięcia kodu SQL.
- **Protokoły szyfrowania:** Ochrona transmisji danych i pamięci masowej dzięki zaawansowanym algorytmom szyfrowania.
- **Szkolenie dla pracowników:** Edukowanie pracowników, aby rozpoznawali anomalie wejściowe, próby phishingu i złośliwe manipulacje poleceniami.
- **Audyty i testy systemu:** Rutynowe kontrole luk w zabezpieczeniach zapewniają aktualność zabezpieczeń przed wstrzyknięciami poleceń i kodu SQL.

Architektura firmy Dell stosuje wszystkie te zasady jednocześnie, tworząc specjalnie bezpieczne platformy dla swoich klientów.

© 2025 Dell Inc. lub podmioty zależne firmy.

Wykorzystanie Dell Professional Services

Usługi profesjonalne firmy Dell, od reagowania na incydenty po codzienne monitorowanie, pomagają firmom w spersonalizowanym podejściu. Wykwalifikowane zespoły oceniają ryzyko, wdrażają solidne zabezpieczenia i oferują szybkie działania naprawcze w obliczu zagrożeń.

Zabezpieczanie tego, co najważniejsze dzięki Dell Technologies

Zwalczanie zaawansowanych ataków typu wstrzyknięcie poleceń i kodu SQL wymaga proaktywnego podejścia. Firma Dell Technologies jest Twoim partnerem, oferującym najnowocześniejsze narzędzia, strategiczne partnerstwa i usługi specjalistyczne.

Przyszłość integralności operacyjnej i zaufania klientów zaczyna się od rozwiązań prewencyjnych. Skontaktuj się z firmą Dell Technologies już dziś, aby zabezpieczyć swoje dane, zbudować odporność i rozwijać się w cyfrowym świecie.

Razem chronimy to, co najważniejsze.

Więcej informacji o tym, jak radzić sobie z największymi wyzwaniami związanymi z cyberbezpieczeństwem, znajdziesz na stronie **Dell.com/SecuritySolutions**

Więcej informacji na temat rozwiązań Dell

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej zasobów

Dołącz do rozmowy, stosując #hasztag

© 2025 Dell Inc. lub podmioty zależne firmy. Wszelkie prawa zastrzeżone. Dell i inne znaki towarowe są znakami towarowymi firmy Dell Inc. lub jej podmiotów zależnych. Pozostałe znaki towarowe mogą należeć do ich odpowiednich właścicieli.

DELL Technologies