DELL Technologies

Prompt-/SQL-injectie: versterking van cyberbeveiliging en veerkracht met Dell Technologies

De toenemende dreiging van prompt-/SQL-injectieaanvallen

Prompt- en SQL-injectieaanvallen hebben herhaaldelijk bewezen tot de schadelijkste en meest wijdverbreide methoden van cyberaanvallen te behoren die door cybercriminelen worden gebruikt. Deze aanvallen maken misbruik van beveiligingslekken in gebruikersquery- of databasesystemen, waardoor kwaadwillenden servers kunnen manipuleren, data kunnen stelen en workflows kunnen verstoren. De toenemende afhankelijkheid van applicaties op basis van data heeft het aanvalsoppervlak vergroot, waardoor technieken voor prompt- en SQL-injectie een grotere dreiging vormen in alle sectoren.

Aanvallers maken gebruik van deze mazen bij onder meer e-commerceplatforms en financiële instellingen om onbevoegde toegang te krijgen tot gevoelige data, wat de dringende behoefte aan geavanceerde tegenmaatregelen aantoont. Dell Technologies erkent de kritieke aard van deze uitdagingen en biedt innovatieve en schaalbare oplossingen om bedrijven te beschermen tegen prompt- en SQL-injectieaanvallen.

Prompt-/SQL-injectieaanvallen begrijpen

Wat zijn dit?

- **Prompt-injectieaanvallen** omvatten de manipulatie van AI- of automatiseringsprompts door schadelijke invoer. Deze aanvallen verwarren systemen zoals AI-chatbots, wat leidt tot onverwachte of schadelijke handelingen**.**
- **SQL-injectieaanvallen** zijn gericht op online databasesystemen. Aanvallers voegen schadelijke SQL-query's in invoervelden in (bijv. aanmeldings- of zoekformulieren) om backend-databases te manipuleren en te beheren.

Hoe ze werken

Prompt-injectieprocessen:

1. Aanvallers kunnen prompts manipuleren om schadelijke resultaten te genereren door gebruik te maken van dubbelzinnige of slecht ontworpen instructies.
2. Dit is vaak gericht op AI-systemen die worden gebruikt voor klantenservice, analyse of besluitvorming.

SQL-injectieprocessen:

1. Een schadelijke SQL-code wordt geïnjecteerd in invoervelden van een kwetsbare applicatie.
2. Het misbruikte systeem voert deze instructies uit, waardoor onbevoegde datatoegang, verwijdering of systeembeheer mogelijk wordt.

Veelvoorkomende technieken

- **Op Union gebaseerde SQL-injectie:** query's combineren om informatie uit de database te extraheren.
- **Op fouten gebaseerde technieken:** opzettelijk vervaardigde query's gebruiken om fouten te produceren die de databasestructuur onthullen.
- **Overbelasten of verwarren door middel van prompts:** kwaadwillende instructies indienen die op AI of regels gebaseerde uitvoer overschrijven.

De impact op bedrijven

De gevolgen van een prompt-/SQL-injectieaanval kunnen veel verder reiken dan het directe incident. Enkele van de meest schadelijke gevolgen zijn:

Financiële kosten

Direct verlies als gevolg van deze aanvallen zijn onder andere gestolen klantdata en transactiebestanden, wat vaak leidt tot boetes. Een SQL-injectieaanval op een financiële instelling kostte het bedrijf bijna $ 40 miljoen aan juridische procedures, vergoedingen en nieuwe beveiligingsmaatregelen.

Operationele storingen

SQL-injecties die gericht zijn op backend-databases kunnen systemen laten crashen, workflows platleggen en essentiële services beëindigen. De gemiddelde downtime voor getroffen bedrijven wordt geschat op 18 tot 24 uur, wat aanzienlijke productiviteitsverliezen veroorzaakt.

Reputatieschade

Prompt-injectieaanvallen op AI-platforms leiden vaak tot onjuiste informatie of onjuiste besluitvorming. Gestolen bedrijfsgeheimen of gecompromitteerde diensten kunnen het vertrouwen van klanten ondermijnen en relaties beschadigen.

Praktijkvoorbeeld

Een retailbedrijf kreeg te maken met een SQL-injectie op het betalingsplatform, waardoor de kaartinformatie van klanten in gevaar kwamen en de dienstverlening dagenlang werd verstoord. Het opschonen van het incident vereiste wettelijke rapportage, bijna **$ 3 miljoen** aan klantencompensatie en juridische kosten.

Alarmerende statistieken

Volgens het rapport 'State of the Internet' van Akamai (over 2017-2019) vertegenwoordigt SQL-injectie bijna **twee derde (~65%)** van alle aanvallen op webapplicaties.

OWASP zag prompt-injectie als het **nr. 1 LLM**-beveiligingsrisico in de top 10 van 2025

Bron: 2025: OWASP Top Security Risks

Oplossingen van Dell Technologies voor prompt-/SQL-injectieverdediging

Dell Technologies voorziet bedrijven van een ecosysteem van tools en beschermingsmechanismen die specifiek zijn ontworpen om geavanceerde aanvallen zoals prompt- en SQL-injectie tegen te gaan.

Eindpuntbeveiliging met Dell Trusted Devices

Eindpunten zijn de gateways naar bedrijfsnetwerken. Dell Trusted Devices bieden beveiliging op hardwareniveau voor solide, compromisloze bescherming.

- **Dell SafeID** beveiligt gebruikersreferenties met verbeterde op hardware gebaseerde verificatie.
- **SafeData** versleutelt gevoelige data, zowel tijdens overdracht als in rust, en beschermt tegen inbreuk tijdens SQL-injectieaanvallen.

Proactieve bedreigingsdetectie met CrowdStrike

De proactieve detectietools van Dell, aangedreven door CrowdStrike, maken gebruik van AI om abnormaal gedrag te identificeren en te neutraliseren.

- **Realtime monitoring:** zorgt ervoor dat prompt- of SQL-afwijkingen onmiddellijk worden gesignaleerd in hybride omgevingen.
- **Beheersing van dreigingen:** op AI gebaseerde algoritmen isoleren getroffen knooppunten op het netwerk om volledige compromissen te voorkomen.

Een productiemultinational die proactieve dreigingsdetectie gebruikte, stopte preventief pogingen tot SQL-injectiequery's die gericht waren op hun industriële databases, waardoor miljoenen aan potentiële downtime werden bespaard.

Server- en storagebeveiliging van Dell

- **Vertrouwde servers:** bescherm databaseapplicaties door servers te versterken tegen pogingen tot inbreuk.
- **Adaptieve workloadbeveiliging:** voorkomt ongeautoriseerde uitvoering van schadelijke code of injecties.

Dell PowerProtect voor data-integriteit

- **Onveranderlijke back-ups:** verbeterde veerkracht zorgt voor herstel, zelfs als databases of prompts beschadigd zijn.
- **Air-gapped storage:** isoleert herstelpunten op fysieke en logische wijze, en beperkt zo terugvalmanipulatie van SQL-injecties.

Tijdens een ransomware-aanval op basis van SQL-injectie herstelde een telecommunicatieprovider de activiteiten in minder dan 48 uur met behulp van de back-upisolaties van Dell PowerProtect, waardoor kritieke verliezen werden voorkomen.

Geavanceerde netwerkbeveiliging en microsegmentatie met Dell PowerSwitch Networking en SmartFabric OS

Versterkt de bescherming tegen zero-day-aanvallen door geavanceerde netwerksegmentatie, strikte toegangscontroles en realtime verkeersanalyse te leveren in uw hele infrastructuur.

Strategische partnerschappen

- **Microsoft:** geïntegreerde bescherming tegen op query gebaseerde injecties op veelgebruikte platforms zoals Azure en SQL Server**.**
- **CrowdStrike en Secureworks:** geavanceerde bedreigingsinformatie en op maat gemaakte incidentrespons versterken de algehele veerkracht in combinatie met de infrastructuur van Dell.

Een meerlaagse beveiligingsstrategie ontwikkelen

Belangrijke acties die bedrijven moeten ondernemen

- **Zero Trust-framework:** implementeer uitgebreide validatie voor alle gebruikers en systeemopdrachten.
- **Beveiligde programmeringspraktijken:** ontwikkelaars moeten gebruikersinvoer opschonen en codebestendige SQL-injecties implementeren.
- **Versleutelingsprotocollen:** bescherm datatransmissie en -storage met geavanceerde versleutelingsalgoritmen.
- **Training voor werknemers:** train medewerkers in het herkennen van afwijkende invoer, phishingpogingen en kwaadwillende promptmanipulatie.
- **Systeemaudits en -tests:** routinematige controles op kwetsbaarheden zorgen ervoor dat de bescherming voor prompt- en SQL-injecties up-to-date blijft.

De architectuur van Dell past al deze principes tegelijkertijd toe, waardoor unieke beveiligde platforms voor haar klanten worden gecreëerd.

Dell Professional Services benutten

Van incidentrespons tot dagelijkse monitoring, Dell Professional Services helpt bedrijven met een gepersonaliseerde aanpak. Deskundige teams beoordelen risico's, implementeren solide verdediging en bieden snel herstel bij bedreigingen.

Beschermen wat er echt toe doet met Dell Technologies

Om de geraffineerde aard van cyberaanvallen met prompt- en SQL-injectie te bestrijden, is een proactieve aanpak nodig. Dell Technologies is uw partner en biedt geavanceerde tools, strategische partnerschappen en deskundige diensten.

De toekomst van operationele integriteit en het vertrouwen van de klant begint met preventieve oplossingen. Neem vandaag nog contact op met Dell Technologies om uw data te beveiligen, veerkracht op te bouwen en te groeien in de digitale wereld.

Samen beschermen we wat er echt toe doet.

Ontdek op **Dell.com/SecuritySolutions** hoe u enkele van de grootste uitdagingen op het gebied van cyberbeveiliging van dit moment kunt aanpakken

Meer informatie over Dell oplossingen

Neem contact op met een Dell Technologies expert

Bekijk meer informatiebronnen

Neem deel aan het gesprek via #HashTag

DELL Technologies