DELL Technologies

Prompt/SQL-injektion: Stärk cybersäkerheten och motståndskraften med Dell Technologies

Det ökande hotet från prompt-/SQL-injektionsattacker

Prompt-och SQL-injektionsattacker har upprepade gånger visat sig vara bland de skadligaste och mest genomgripande metoderna för cyberattacker som används av cyberbrottslingar. Dessa attacker utnyttjar sårbarheter i användarfråge- eller databassystem och gör det möjligt för skadliga aktörer att manipulera servrar, stjäla data eller störa arbetsflöden. Ökat beroende av datadrivna program har utökat angreppsytan, något som gör promptattacker och SQL-injektionstekniker till större hot i alla branscher.

Angripare utnyttjar dessa kryphål för att få obehörig åtkomst till känsliga data: från e-handelsplattformar till finansinstitut. Det här visar det brådskande behovet av avancerade motåtgärder. Dell Technologies inser att dessa utmaningar är viktiga och erbjuder innovativa och skalbara lösningar för att skydda företag mot Prompt- och SQL-injiceringsattacker.

Vad är prompt-och SQL-injektionsattacker?

Vilka är de?

- **Prompt-injektionsattacker** innebär manipulering av AI eller automatiseringsuppmaningar från skadliga inmatningar. Dessa attacker förvirrar system som AI-chattrobotar och leder till oväntade eller skadliga åtgärder**.**
- **SQL-injektionsattacker** riktar sig mot databassystem online. Angripare infogar skadliga SQL-frågor i inmatningsfält (exempelvis inloggnings- eller sökformulär) för att manipulera och kontrollera backend-databaser.

Så fungerar de

Prompt-injektionsprocesser:

1. Angripare manipulerar uppmaningar för att generera skadliga utdata genom att utnyttja tvetydiga eller dåligt utformade instruktioner.
2. Detta riktar sig ofta till AI-system som används för kundservice, analys eller beslutsfattande.

SQL-injektionsprocesser:

1. En skadlig SQL-kod sprutas in i inmatningsfälten i ett sårbart program.
2. Det utnyttjade systemet utför dessa instruktioner och möjliggör obehörig dataåtkomst, radering eller systemkontroll.

Vanliga tekniker

- **Union-Based SQL-injektion:** Kombinerar frågor för att extrahera information från databasen.
- **Felbaserade tekniker:** Använder avsiktligt skapade frågor för att skapa fel som avslöjar databasstrukturen.
- **Överbelastning eller förvirring:** Matar in skadliga instruktioner som kringgår AI eller regelbaserade utdata.

Påverkan på företag

Dominoeffekterna av en prompt-/SQL-injektionsattack sträcker sig långt bortom den omedelbara incidenten. Några av de mest skadliga konsekvenserna är:

Finansiella kostnader

Direkta förluster från dessa attacker inkluderar stulna kunddata och transaktionsregister, något som ofta leder till böter. En SQL-injektionsattack på ett finansinstitut kostade företaget nästan 40 miljoner USD i rättstvister, återbetalningar och nya säkerhetsåtgärder.

Driftstörningar

SQL-injektioner som riktar sig till backend-databaser kan krascha system, förlama arbetsflöden och stoppa viktiga tjänster. Den genomsnittliga driftavbrotten för berörda företag uppskattas till mellan 18 och 24 timmar, vilket orsakar betydande produktivitetsförluster.

Anseendeskada

Prompt-injektionsattacker på AI-plattformar leder ofta till felaktig information eller felaktigt beslutsfattande. Stulna företagshemligheter eller komprometterade tjänster urholkar kundernas förtroende och skadar relationer.

Verkliga exempel

Ett detaljhandelsföretag drabbades av en SQL-injektion på sin betalningsplattform. Resultatet var komprometterade kundkortuppgifter och stoppade tjänster i flera dagar. För att åtgärda incidenten krävdes myndighetsrapportering och nästan **3 miljoner USD** i kompensation till kunder och rättegångskostnader.

Skrämmande statistik

SQL-injektioner representerar nästan **två tredjedelar (~65 %)** av alla webbprogramattacker enligt Akamais rapport ”State of the Internet” (som täcker 2017–2019).

OWASP identifierade prompt-injektioner som

nummer 1

på LLM-säkerhetsrisken i sin Top 10-lista 2025

Källa: 2025: OWASP Top Security Risks

Dell Technologies-lösningar för försvar mot Prompt-/SQL-injektion

Dell Technologies utrustar företag med ett ekosystem av verktyg och skyddsmekanismer som är skräddarsydda för att motverka sofistikerade attacker som prompt- och SQL-injektioner.

Slutpunktssäkerhet med Dell Trusted Devices

Slutpunkter är gatewayer till företagsnätverk. Dell Trusted Devices bäddar in säkerhet på hårdvarunivå för robust och kompromisslöst skydd.

- **Dell SafeID** skyddar användaruppgifter med förbättrad hårdvarubaserad autentisering.
- **SafeData** krypterar känsliga data både under transport och vila, och skyddar mot intrång under SQL-injektion.

Proaktiv hotdetektering med CrowdStrike

Dells proaktiva detekteringsverktyg som drivs av CrowdStrike använder AI för att identifiera och neutralisera onormala beteenden.

- **Realtidsövervakning:** Säkerställer att prompt- eller SQL-avvikelser flaggas omedelbart i hybridmiljöer.
- **Hotbegränsning:** AI-baserade algoritmer isolerar berörda noder i nätverket för att förhindra fullständiga kompromisser.

Ett multinationellt tillverkningsföretag som använde proaktiv hotdetektering stoppade försök till SQL-injicering med inriktning på sina industriella databaser, och sparade miljoner i potentiella driftavbrott.

Server- och lagringssäkerhet från Dell

- **Betrodda servrar:** Skydda databasprogram genom att stärka servrar mot intrångsförsök.
- **Adaptiv arbetsbelastningssäkerhet:** Förhindrar obehörig körning av skadlig kod eller injektioner.

Dell PowerProtect för dataintegritet

- **Oföränderliga säkerhetskopieringar:** Förbättrad tålighet säkerställer återställning även om databaser eller uppmaningar är skadade.
- **Lagring med luftgap:** Fysiskt och logiskt isolerar återställningspunkter, vilket minskar risken för manipulation av SQL-injektioner.

Under en SQL-injektionsbaserad utpressningsvirusattack återställde en telekommunikationsleverantör driften på mindre än 48 timmar med hjälp av Dell PowerProtects säkerhetskopieringsisoleringar, för att undvika kritiska förluster.

Avancerad nätverkssäkerhet och mikrosegmentering med Dell PowerSwitch Networking och SmartFabric OS

Stärker försvaret mot nolldagsattacker genom att leverera avancerad nätverkssegmentering, strikta åtkomstkontroller och trafikanalys i realtid i hela infrastrukturen.

Strategisk användning av partnerskap

- **Microsoft:** Integrerat försvar mot frågebaserade injektioner på allmänt använda plattformar som Azure och SQL Server**.**
- **CrowdStrike och Secureworks:** Avancerad hotinformation och skräddarsydda incidentsvar stärker den övergripande motståndskraften i kombination med Dells infrastruktur.

Bygga en säkerhetsstrategi i flera lager

Viktiga åtgärder som företag bör vidta

- **Ramverk för nollförtroende:** Implementera omfattande validering för alla användare och systemkommandon.
- **Säkra kodningsrutiner:** Utvecklare bör rensa data som användare matar in och distribuera kodbeständiga SQL-injektioner.
- **Krypteringsprotokoll:** Skydda dataöverföringar och lagring med avancerade krypteringsalgoritmer.
- **Medarbetarutbildning:** Utbilda personalen i att känna igen inmatningsavvikelser, nätfiskeförsök och manipulering av skadliga meddelanden.
- **Systemrevisioner och tester:** Rutinmässiga sårbarhetskontroller säkerställer att försvaret mot prompt- och SQL-injektioner förblir uppdaterat.

Dells arkitektur tillämpar alla dessa principer samtidigt och skapar unikt säkra plattformar för sina kunder.

Dra nytta av Dell Professional Services

Dells professionella tjänster hjälper företag med ett personligt tillvägagångssätt, från incidentåtgärder till daglig övervakning. Skickliga team bedömer risker, implementerar robusta försvar och erbjuder snabba åtgärder vid hot.

Skydda det som är viktigast med Dell Technologies

Det krävs en proaktiv strategi för att bekämpa den sofistikerade karaktären hos prompt- och SQL-injektionsattacker. Dell Technologies är din partner och erbjuder banbrytande verktyg, strategiska partnerskap och experttjänster.

Framtiden för operativ integritet och kundförtroende börjar med förebyggande lösningar. Kontakta Dell Technologies idag för att skydda dina data, bygga motståndskraft och lyckas i den digitala världen.

Tillsammans skyddar vi det som är viktigast.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **Dell.com/SecuritySolutions**

Mer information om Dells lösningar

Kontakta en av Dell Technologies experter

Visa fler resurser

Delta i samtalet med #HashTag

DELL Technologies