MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Všeobecné informácie

SQL injection

VJ CSIRT

Čo je to SQL injection

Jedná sa o typ útoku, v rámci ktorého útočník využíva SQL dopyty vkladané napr. do vstupných polí webového formuláru na získanie informácií z databázy, ktoré by mu za normálnych okolností neboli prístupné, úpravu/odstránenie záznamov z databázy a pod. Dopad tohto útoku tak môže byť kritický, nakoľko si útočník môže takýmto spôsobom napr. eskalovať administrátorské práva, odstrániť celú databázu a pod.

Indikátory SQL injection útoku vo Vašej infraštruktúre

☐ použitie špeciálnych znakov v používateľských vstupoch (napr. ‘, “, ;, &, *)

☐ použitie booleovských operácií v používateľských vstupoch (napr. OR 1=1)

☐ použitie SQL dopytov v rámci URL adresy

☐ použitie slova *UNION* v používateľských vstupoch, na spustenie zložitejších SQL dopytov

☐ zvýšený počet vyplnených a odoslaných dát cez vstupné polia webu (prihlasovací formulár, vyhľadávacie polia a pod.)

Ochrana pred SQL injection

Existuje niekoľko spôsobov, akým zabrániť úspešnému útoku SQL injection. Patrí medzi ne:

☐ dôkladná sanácia používateľských vstupov

☐ použitie ORM (object relational mapping) namiesto štandardných SQL vstupov

☐ využitie parametrizovaných metód na tvorbu SQL dopytov (napr. prepared statements)

☐ implementácia WAF (web application firewall)