RISCURILE ASOCIATE CU UTILIZAREA SQL. SQL INJECTION

Cristian DICOL

Departamentul Ingineria Software și Automatică, grupa TI-191 F/R, Facultatea Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei, Chișinău, Republica Moldova

Autorul corespondent: Cristian DICOL, e-mail: dicol.cristian@isa.utm.md

Coordonator științific: Dorian SARANCIUC, lector universitar, FCIM, DISA

Rezumat. *În acest articol se spune despre atacurile cibernetice prin injectare SQL. Articolul explică modalitatea în care acest tip de atac este realizat și de ce sunt atacurile prin injectare SQL o amenințare majoră pentru organizațiile de toate dimensiunile. De asemenea, sunt oferite sfaturi pentru organizațiile care doresc să se protejeze împotriva acestor atacuri, precum utilizarea interogărilor parametrizate, validarea și igienizarea intrărilor în aplicații, implementarea măsurilor de protecție la nivel de aplicație și de rețea și antrenarea personalului pentru a recunoaște semnele unui atac posibil.*

Cuvinte cheie: *atac cibernetic, coduri, declarație sql, bază de date, formular web, url, interogări parametrizate, validare, igienizare*

Introducere

Un atac cibernetic cunoscut sub numele de injecție SQL implică inserarea de cod rău intenționat într-o instrucțiune SQL, de obicei prin câmpuri de introducere a utilizatorului, pentru a manipula sau a fura date dintr-o bază de date. Acest lucru se poate face prin completarea unui formular web cu informații eronate sau prin crearea unei adrese URL rău intenționate care conține o instrucțiune SQL rău intenționată [1].

Un script SQL (Structured Query Language) este inserat într-o anumită aplicație printr-o casetă de introducere în acest tip de atac. Altfel spus, un hacker va încerca să insereze o comandă SQL care poate citi datele din baza de date într-un formular de înregistrare dacă găsește unul pe un site web [2].

Un atac reușit va putea insera, actualiza și șterge date din baza de date. Poate îndeplini sarcini administrative.

Cât de dese sunt SQL injections?

Datorită faptului că aceste atacuri trec frecvent neobservate, este dificil să spunem cu certitudine cât de răspândite sunt. Deși sunt un tip de atac bine-cunoscut și folosit frecvent, ele reprezintă totuși o amenințare serioasă pentru afaceri de toate tipurile. Organizațiile trebuie să ia măsuri de precauție pentru a se apăra împotriva aceste amenințări prin protejarea adecvată a bazelor de date și prin implementarea controalelor de validare și dezinfectare a intrărilor în aplicațiile lor [3].

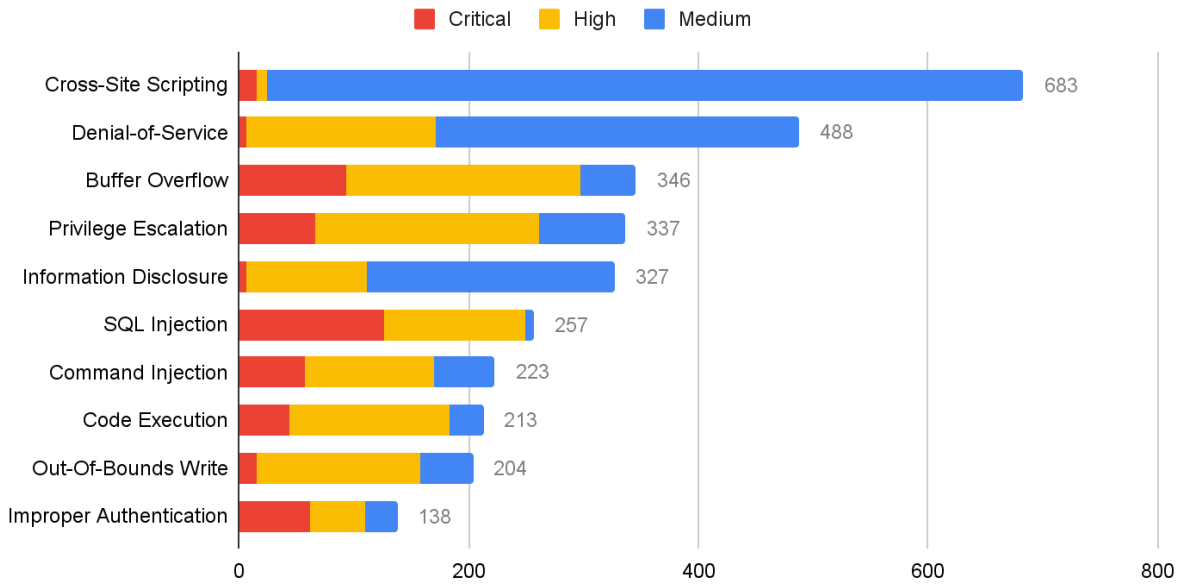

Figura 1 – Tendințe privind securitatea rețelei: noiembrie 2021 până în ianuarie 2022

Cum organizațiile trebuie să se protejeze împotriva lor?

Sunt mai mulți pași pe care organizațiile pot întreprinde pentru a se proteja împotriva atacurilor prin injectare SQL: [4]

a. Utilizați interogări parametrizate: interogările parametrizate sunt o modalitate sigură și eficientă de a preveni atacurile prin injecție SQL. Acestea vă permit să specificați substituenți pentru introducerea utilizatorului în instrucțiunile dvs. SQL, care sunt apoi igienizate și validate automat de serverul bazei de date.
b. Validarea și igienizarea intrărilor: este important să validați și să igienizați toate intrările de utilizator înainte de a le utiliza într-o instrucțiune SQL. Aceasta poate include verificarea caracterelor ilegale, aplicarea limitelor de lungime de intrare și conversia caracterelor speciale în omologii lor escape.
c. Utilizați cel mai mic privilegiu: acordarea utilizatorilor doar a permisiunilor minime de care au nevoie pentru a-și face treaba poate ajuta la prevenirea accesului neautorizat la datele sensibile.
d. Actualizați și corecționați în mod regulat: menținerea la zi a serverului de baze de date și a aplicațiilor cu cele mai recente corecții de securitate poate ajuta la prevenirea exploatării vulnerabilităților de către atacatori
e. Utilizați un paravan de protecție pentru aplicații web (WAF- web application firewall): un WAF este un instrument de securitate care vă poate ajuta să vă protejați site-ul web de atacurile web obișnuite, inclusiv atacurile de injecție SQL.
f. Testați și monitorizați în mod regulat: testarea regulată a aplicațiilor pentru vulnerabilități și monitorizarea activităților suspecte vă poate ajuta să identificați și să răspundeți la potențialele atacuri de injecție SQL în timp util.
g. Prin implementarea acestor și a altor măsuri de securitate, organizațiile își pot reduce semnificativ riscul de a deveni victime ale atacurilor cu injecție SQL.

Exemplul unui atac

De exemplu, să presupunem că există un formular de autentificare pe un site web care cere un nume de utilizator și o parolă. Site-ul web ar putea utiliza o interogare SQL de genul acesta pentru a verifica dacă numele de utilizator și parola introduse sunt valide:

```
SELECT * FROM users WHERE username='$username' AND password='$password';
```

Figura 2 – Valorile introduse de utilizator

Unde, $username și $password sunt variabile ce conțin valorile introduse de utilizator. În cazul în care un atacator introduce un nume de utilizator de ' OR '1'='1 și o parolă de ' OR '1'='1, interogarea SQL rezultată va arăta astfel:

```
SELECT * FROM users WHERE username='' OR '1'='1' AND password='' OR '1'='1';
```

Figura 3 – Declarație evaluată ca adevărată

Deoarece „1"="1" este întotdeauna adevărat, această interogare va fi întotdeauna evaluată drept adevărat, permițând atacatorului să se conecteze fără să cunoască numele de utilizator și parola adecvate.

Deoarece oferă unui atacator acces la date sensibile, capacitatea de a modifica sau elimina date sau chiar de a prelua întreaga bază de date, atacurile cu injecție SQL pot fi extrem de periculoase. Pentru a opri atacurile cu injecție SQL, este esențial să validați și să igienizați corect intrarea utilizatorului.

Figura 4 – SQL injection pe numerele unui automobil

Cele mai importante domenii pentru cercetările privind atacurile cu injecție SQL

Există diverse arii de cercetare care ar putea fi considerate cruciale pentru a aborda atacurile prin injectare SQL în viitor:[5]

a. Tehnici avansate de detectare și prevenire: Experții lucrează în mod constant la dezvoltarea de metode noi și îmbunătățite de detectare și prevenire a atacurilor prin injectare SQL. Acestea ar putea include dezvoltarea de noi algoritmi, modele de învățare automată sau alte tehnologii care pot identifica și bloca mai bine acest tip de atacuri.

b. Sanitizare eficientă a datelor: Pe măsură ce hackerii continuă să găsească noi modalități de a ocoli măsurile de sanitizare existente, cercetarea în metode mai eficiente de sanitizare a intrărilor utilizatorilor ar putea fi un domeniu important de concentrare.

c. Îmbunătățirea educației în securitate: În timp ce soluțiile tehnice sunt importante, este crucial ca organizațiile să înțeleagă în profunzime cum să se protejeze împotriva atacurilor prin injectare SQL. Cercetările viitoare ar putea concentra dezvoltarea de metode mai eficiente de educare și formare a angajaților în ceea ce privește modul de a preveni și de a răspunde acestui tip de atacuri.

d. Înțelegerea mai profundă a motivațiilor și tacticilor atacatorilor: Prin înțelegerea motivațiilor pentru care atacatorii vizează anumite organizații și a tacticilor pe care le folosesc pentru a efectua atacuri prin injectare SQL, cercetătorii pot informa mai bine dezvoltarea de strategii de prevenire și răspuns.

Concluzii

Injectarea SQL este un tip de atac cibernetic prin care un atacator introduce coduri cu intenții rele într-o declarație SQL pentru a manipula sau a fura date dintr-o bază de date. Acest lucru poate fi realizat prin intermediul formularelor web sau prin URL-uri malițioase care conțin declarații SQL cu intenții rele. Atacurile cu injectare SQL sunt frecvente și pot rămâne adesea nedetectate, fiind o amenințare majoră pentru organizațiile de toate dimensiunile. Organizațiile pot lua măsuri pentru a se proteja împotriva acestor atacuri prin securizarea bazelor de date, utilizarea interogărilor parametrizate, validarea și igienizarea intrărilor în aplicații, implementarea măsurilor de protecție la nivel de aplicație și de rețea și antrenarea personalului pentru a recunoaște semnele unui atac posibil.

În general, este nevoie de cercetări continue pentru a ține pasul cu amenințarea crescândă a atacurilor prin injectare SQL și pentru a proteja mai bine organizațiile și indivizii de acest tip

Referințe

1. SQL Injection - Ghidul celei mai utilizate metode de atac. [online]. [accesat 20.12.2022]– Disponibil: httpswww.link-academy.comblogsql-injection-ghidul-celei-mai-utilizate-metode-de-atac#~text=Ce%20este%20SQL%20Injection%3F,intermediul%20unei%20căsuțe%20de%20input.
2. SQL Injection [online]. [accesat 20.12.2022]– Disponibil: https://owasp.org/www-community/attacks/SQL_Injection
3. How to prevent SQL injection with prepared statements [online]. [accesat 20.12.2022]– Disponibil: https://searchsecurity.techtarget.com/definition/SQL-injection
4. What is SQL Injection (SQLi) and How to Prevent It [online]. [accesat 20.12.2022]– Disponibil: https://www.acunetix.com/websitesecurity/sql-injection/
5. SQL Injection: Vulnerabilities & SQL Injection Prevention [online]. [accesat 20.12.2022]– Disponibil: https://www.veracode.com/security/sql-injection