SQL-ІН'ЄКЦІЇ ЯК ЗАГРОЗА БЕЗПЕЦІ ДАНИХ

Іващенко М.Д., Петренко О.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

SQL-ін'єкція, також відома як SQLI, є поширеним вектором атаки, який використовує зловмисний код SQL для маніпулювання серверною базою даних для доступу до інформації, яка не призначена для відображення [1]. Ця інформація може включати будь-яку кількість елементів, включаючи конфіденційні дані компанії, списки користувачів або приватні дані клієнтів.

Метою доповіді є узагальнення та систематизація інформації про SQL-ін'єкцію, що представляє собою серйозну загрозу безпеці та полягає у використанні вразливостей веб-застосунку для несанкціонованого доступу до бази даних. В доповіді зазначено, що у процесі SQL-ін'єкції шкідливий код вставляється або «впроваджується» в текстові поля введення, такі як форми на веб-сторінках. Цей код потім виконується безпосередньо в системі бази даних, що дозволяє атакуючим отримати доступ до конфіденційної інформації, модифікувати дані або навіть знищити їх [2].

SQL-ін'єкції зазвичай поділяються на три категорії: In-band SQLi, Inferential SQLi, Out-of-band SQLi [3]. Розглядаючи можливі наслідки SQL-ін'єкцій, насамперед, важливо підкреслити ризик втрати довіри з боку клієнтів та користувачів. В разі несанкціонованого доступу до особистої інформації, такої як номери телефонів, адреси та конфіденційні дані кредитних карт, може виникнути серйозний злам довіри, що може сильно зашкодити репутації організації або платформи. Запобігання SQL-ін'єкціям та використання належних методів захисту даних є надзвичайно важливими завданнями для забезпечення безпеки веб-додатків та збереження довіри користувачів

Отже, SQL-ін'єкції є серйозною загрозою безпеці інформаційних систем, оскільки вони дозволяють зловмисникам несанкціоноване отримувати доступ до баз даних та впливати на дані. Ця атака може призвести до втрати конфіденційної інформації, порушення цілісності даних та впливу на доступність системи. Загроза SQL-ін'єкцій вимагає від розробників та адміністраторів систем надзвичайної обережності та впровадження ефективних заходів захисту, таких як санітаризація та валідація вхідних даних, використання параметризованих запитів та належна настройка систем безпеки. Розуміння різних видів SQL-ін'єкцій та їх можливих наслідків є важливим кроком для запобігання цим атакам і збереження безпеки інформаційних систем.

Список літератури

1. What is SQL Injection | SQLI Attack Example & Prevention Methods | Imperva. Imperva. URL: https://www.imperva.com/learn/application-security/sql-injection-sqli/ (accessed: 05.10.2023)

2. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. (2015). Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі. *Системи обробки інформації*, (9), 101-104.

3. SQL-ін'єкції - aCode. Acode. URL: https://acode.com.ua/sql-injection/