УДК 004.02

О.А. Саган, К.Б. Швирло
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ SQL-ІН'ЄКЦІЙ:ТИПИ АТАК ТА МЕТОДИ ЗАХИСТУ

O.A. Sahan; K.B. Shvyrlo

ANALYSIS OF SQL INJECTIONS: TYPES OF ATTACKS AND DEFENSE METHODS

У сучасних інформаційних системах безпека баз даних є ключовим аспектом, адже там зберігається велика кількість конфіденційно інформації, яка може мати цінність для користувачів та для самої системи, а її витік є неприпустимим. Вразливості, такі як SQL-ін'єкції, можуть призвести до витоку конфіденційної інформації, порушення функціонування системи та значних збитків для організації. SQL-ін'єкції належать до найнебезпечніших атак на веб-додатки, оскільки вони дозволяють зловмисникам виконувати довільні SQL-запити, змінювати дані або навіть отримувати контроль над сервером бази даних.

Виділяють декілька типів загроз, кожен з яких характеризується способом здійснення. Через користувацькі поля можна виконувати запити, додаючи метасимволи до введених даних і цим змінюючи структуру запиту.

Аналогічні дії зловмисники можуть виконувати, використовуючи cookie-файли. Для цього змінюються значення, що передаються додатку. Також виконання ін'єкцій може відбуватись через серверні змінні, наприклад, HTTP-заголовки, що використовуються у запитах. Атака може відбуватися не одразу, а під час обробки збережених даних у майбутніх запитах [1]. Метою всіх видів цієї атаки є викрадення конфіденційної інформації, зловмисна зміна даних у базі, запуск шкідливого коду або процедур, отримання прав адміністратора.

Для захисту системи від SQL-ін'єкцій слід перевіряти отримані від користувача дані, наприклад, за допомогою регулярних виразів. Застосовувати підготовлені запити, які дозволять уникнути негативного ефекту за рахунок чіткого визначення параметрів запиту. Використовувати екранування користувацьких даних [2-3].

Отже, SQL-ін'єкції є серйозною загрозою для веб-додатків, особливо у випадку необхідності обробки великої кількості даних користувача. Причиною появи таких вразливостей є неналежна обробка даних, отриманих від користувача.

Успішні атаки можуть мати ряд негативних наслідків для об'єкта атаки, а саме: компрометація даних, збої в роботі системи, фінансові та репутаційні втрати. Тому важливим аспектом безпеки є захист даних та протидія різним видам атак.

Ефективний захист потребує комплексного підходу до проблеми, а саме: чітко розуміти природу SQL-ін'єкцій, використовувати інструменти, що запобігають виконанню шкідливого коду, навчати розробників для підвищення рівня безпеки коду, регулярний аудит коду та застосування систем автоматизованого виявлення вразливостей та розробка нових засобів протидії атакам.

Література.

1. SQL Injection. HackTricks. URL: https://book.hacktricks.xyz/pentesting-web/sql-injection.
2. How To Protect Against SQL Injection Attacks. Information Security Office. URL: https://security.berkeley.edu/educationawareness/how-protect-against-sql-injection-attacks.
3. How To Prevent SQL Injection Attacks? Best Practices. GlobalDots.. URL: https://www.globaldots.com/resources/blog/how-to-prevent-sql-injection-attacks/.