DOI: 10.59647/978-617-520-936-3/1

Безпека web-додатків: SQL-ін'єкції – один з найпопулярніших методів кібератак

Марія Балобольченкова, студент[1], (ORCID: 0009-0004-5732-1558), **Євгенія Шабала,** к.т.н., доцент кафедри кібербезпеки та комп'ютерної інженерії [1] ,(ORCID: 0000-0002-0428-9273)

[1] *Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна*

АНОТАЦІЯ

Теза зосереджена на досліджені такого поняття в кібербезпеці як SQL-ін'єкції. Даний вид кібератак розглядається з точки зору впливу на web-додатки та інформацію, що оброблюється за їх допомогою. Згадуються конкретні цілі поставлені перед зловмисником, їх вплив на додатки. Наведені приклади та статистика використання даного виду кібератак та можливості, що допоможуть попередити або мінімізувати атаки за допомогою SQL-ін'єкцій.

Ключові слова:SQL-ін'єкція, кібератака, цілі атак, інциденти, web-додатки, типи SQL-ін'єкцій.

1. ВСТУП

В сучасному цифровому світі, де web-додатки стали невід'ємною частиною нашого повсякденного життя та бізнес-процесів, питання безпеки цих додатків набуває критичного значення. Вони часто використовуються для обробки даних, що обов'язково потребують захисту: конфіденційна інформація, корпоративні записи тощо. Проте разом із новими засобами обробки інформації, з'являються і можливості, що допомагають зловмисникам модифікувати чи добувати цю інформацію. Одним з таких способів є SQL-ін'єкції.

2. ЩО ТАКЕ SQL-ІН'ЄКЦІЯ

Збереження та робота з інформацією, що подекуди є основним функціональним блоком web-додатків, відбувається за допомогою SQL (***S***tructured Query Language). Цим інструментом можна надсилати як корисні запити так і шкідливі.

SQL-ін'єкції (SQLi) – це вразливість веб-безпеки, яка дозволяє зловмиснику втручатися в запити, які програма робить до своєї бази даних, без відома інших користувачів.

2.1. Цілі атак та їх вплив на web-додатки.

На рисунку 1 можна розглянути цілі SQLi.

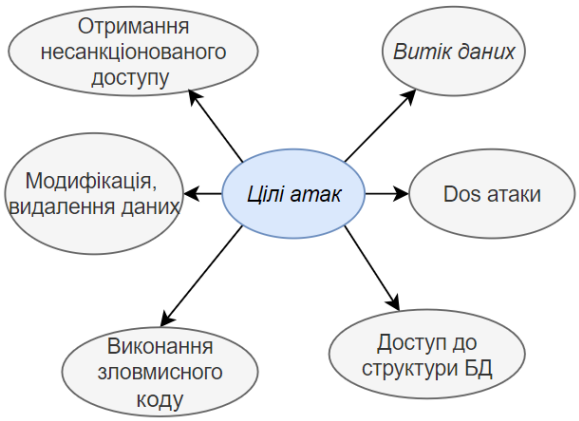

Рисунок 1. Цілі SQL-ін'єкцій

Як і в будь-яких зловмисних діях поставлені перед зловмисником цілі мають завдати шкоди. Виділяють декілька точок впливу такої діяльності на систему та людей/компанію:

- Витік конфіденційних даних;
- Втрата або пошкодження інформації;
- Фінансові та репутаційні втрати;
- Вплив на бізнес-процеси;
- Використання ресурсів;
- Порушення політики безпеки.

2.2. Типи SQL-ін'єкцій

Зазначивши які саме цілі мають на меті зловмисники, використовуючи мову запитів, важливо розглянути які типи застосування так званих ін'єкцій бувають.

Класичнана SQL-ін'єкція - це тип атаки, коли зловмисник використовує поля введення веб-програми, такі як форми входу, вікна пошуку або параметри URL-адреси, для виконання несанкціонованих команд SQL.

Сліпа SQL-ін'єкція — це тип SQL-ін'єкції, при якій зловмисник не отримує безпосередніх повідомлень про помилки з бази даних, але може використовувати логічні умови та затримки для визначення наявності уразливостей та отримання інформації. Вона є "сліпою", оскільки зловмисник не отримує чітких повідомлень про помилки або вивід даних, як у стандартній SQL-ін'єкції.

SQL-ін'єкція на основі помилок є технікою атаки, яка використовує інформацію, що надається базою даних у відповідь на помилкові SQL-запити, для отримання додаткових даних про структуру бази даних або для визначення вразливостей системи. Цей метод дозволяє зловмисникам витягувати інформацію, яка не повинна бути доступною, і може бути використана для підготовки більш складних атак.

SQL-ін'єкція на основі об'єднання є одним з методів атаки, який дозволяє зловмисникам об'єднувати результати декількох SQL-запитів в один, щоб отримати додаткову інформацію з бази даних. Цей метод дозволяє атакуючому витягувати дані з таблиць, до яких в іншому випадку не було б доступу. Такі SQLi використовують оператор UNION для об'єднання результатів кількох SELECT-запитів в один набір результатів. Оператор UNION дозволяє зливати дані з різних таблиць або запитів, що полегшує доступ до чутливої інформації.

SQL-ін'єкція на основі часу є технікою атаки, яка використовує затримки у відповіді сервера бази даних, щоб визначити наявність уразливостей у SQL-запитах або отримати інформацію про базу даних. Цей метод відноситься до сліпих SQL-ін'єкцій і дозволяє атакуючому

виконувати запити, які змушують базу даних затримувати відповіді на певний час. Хакер формує запити, які включають затримки або паузи і аналізує час відповіді сервера бази даних, щоб визначити результат запиту. Це дозволяє зловмиснику дізнатися про наявність уразливостей і отримати інформацію про структуру бази даних без безпосереднього виведення даних на екран.

3. ІНЦИДЕНТИ КІБЕРАТАК ТА ЗАСОБИ ЗАХИСТУ

3.1. Приклади кібератак за допомогою SQLi

Атака на базу даних MongoDB (2017-2018). В цьому випадку зловмисники використовували SQL-ін'єкції для атаки на бази даних NoSQL, MongoDB, які часто використовують SQL-подібні запити. Веб-додатки, які використовували MongoDB, мали вразливості, що дозволяли виконувати запити з небезпечними параметрами.

У 2019 році фінансовий холдинг Capital One постраждала від однієї з найбільших атак на бази даних за допомогою SQL-ін'єкцій. Зловмисник використав вразливість у веб-додатку для отримання доступу до конфіденційних даних більше ніж 100 мільйонів клієнтів. Атака включала не тільки SQL-ін'єкцію, але й інші техніки для витоку даних. [2]

В 2018 році зловмисники атакували міські системи в Джорджії, зашифрувавши дані і вимагавши викуп. Це була атака програм-вимагачів, а не SQL-ін'єкція, але вона підкреслює важливість захисту систем критичної інфраструктури.

Не зважаючи на обізнаність в даній сфері та досвід минулих років, SQLi все ще є одною з популярних загроз витоку даних та злому систем. 42% атак на загальнодоступні системи пов'язані з впровадженням SQL, що підкреслює популярність цієї техніки серед кіберзлочинців. [1]

У 2023 році 2159 уразливостей типу «SQL-ін'єкції» були прийняті як CVE. Тенденція є значною за 4 роки: + 460% і безперервна.

CVE	SQL Injection	Assesment on 12 months
2020	466	
2021	744	
2022	1790	
2023	2159	
2024 (January)	247	2964
source CVE.org		

Рисунок 2. Статистика застосування SQLi

3.2. Засоби запобігання атак

Відповідно до статистичних даних наведених вище, питання про засоби, що можуть запобігти SQLi є досі популярним.

Багато сучасних фреймворків та мов програмування мають вбудовані бібліотеки ORM, які автоматично управляють SQL-запитами через об'єктно-орієнтовані моделі даних. Це допомагає запобігти SQL-ін'єкціям, оскільки ORM не дозволяє прямий доступ до SQL-коду.

Перевірка та валідація всіх даних, що надходять від користувачів, перед їх використанням дозволить переконатись, що ввід відповідає очікуваним форматам та не пропускатиме приховані SQL-запити.

Також важливим є правильне надання доступу. Необхідно відслідковувати та надавати доступ на зміну бази даних додатком лише там де це має місце бути. Наприклад, якщо додаток не повинен змінювати структуру таблиць, не надавайте йому такі привілеї.

Регулярне оновлення програмного забезпечення і компонентів, включаючи сервери баз даних, веб-сервери та фреймворки. Ці дії допоможуть захиститися від відомих уразливостей, які можуть бути експлуатовані для SQL-ін'єкцій.

Також важливо проводити тестування. Зокрема можна виділити тестування на проникнення за для визначення слабких місць в web-додатках та своєчасної можливості вдосконалення системи. Тестування на доступ до інформації такої як помилки бази даних, що не потрібні звичайним користувачам має велике значення.

4. ВИСНОВКИ

SQL-ін'єкції залишаються однією з найпоширеніших і небезпечних форм кіберзагроз для web-додатків, що обробляють чутливу інформацію. Цей вид атаки дозволяє зловмисникам маніпулювати запитами до бази даних, що може призвести до витоку конфіденційних даних, втрати або пошкодження інформації, фінансових та репутаційних втрат, а також порушення бізнес-процесів.

Аналіз показує, що існують кілька основних типів SQL-ін'єкцій, кожен з яких має свою специфіку і наслідки. SQLi не втрачають популярності, не дивлячись на велику обізнаність фахівців. Тож треба бути готовими до такого типу кібератак і сьогодні.

Список літератури

1. The Growing Threats of Ransomware and SQL Injection Attacks. LinkedIn: вебсайт. URL: https://www.linkedin.com/pulse/growing-threats-ransomware-sql-injection-attacks-eric-petiot-3c6ie
2. What Capital One's Data Leak Tells Us About Firewall Exploits. SentinelOne: вебсайт. URL: https://www.sentinelone.com/blog/firewall-vulnerabilities-data-leaking-like-capital-one/
3. Securing web applications against XSS and SQLi attacks using a novel deep learning approach. Scientific Reports: вебсайт URL: https://www.nature.com/articles/s41598-023-48845-4