УДК 004.49

А. В. Шпикуляк

АВТОМАТИЗАЦІЯ ПРОЦЕСУ ВИЯВЛЕННЯ ТА ЗАХИСТУ ВІД SQL-ІН'ЄКЦІЙ ЗА ДОПОМОГОЮ СУЧАСНИХ ІНСТРУМЕНТІВ

Вінницький національний технічний університет

Анотація

Стаття розглядає методи виявлення та захисту від SQL-ін'єкцій, що є серйозною загрозою для безпеки веб-додатків. Вона описує традиційні підходи та їх обмеження, а також нові, автоматизовані методи та інструменти, які дозволяють підвищити ефективність захисту.

Ключові слова: SQL-ін'єкція, безпека даних, веб-застосунки, автоматизація, виявлення вразливостей, захист від атак.

Abstract

The article examines methods of detection and protection against SQL-injection, which is a serious threat to the security of web applications. It describes traditional approaches and their limitations, as well as new, automated methods and tools that can improve the effectiveness of protection.

Keywords: SQL-injection, data security, web applications, automation, vulnerability detection, attack protection.

Вступ

SQL-ін’єкція — це метод отримання несанкціонованого доступу до бази даних, при якому шкідливий код виконується прямо з поля вводу звичайної форми. Атака типу впровадження SQL-коду, в залежності від типу системи управління базами даних та умов впровадження, дає можливість атакуючому виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері.

Традиційні методи виявлення та захисту від SQL-ін'єкцій ґрунтуються на ручному аналізі коду та даних. Ці підходи можуть бути працездатні, але також вимагають багато часу і можуть бути вразливими перед новими типами атак. Завдяки сучасним інструментам є можливість автоматизувати багато аспектів виявлення та захисту від SQL-ін'єкцій. Це сприяє підвищенню безпеки веб-застосунків, зменшенню ризику помилок і звільненню часу розробників для інших завдань.

Результати дослідження

Існують різні типи інструментів, які можна використовувати для автоматизації виявлення та захисту від SQL-ін'єкцій:

- Сканери веб-застосунків (Web Application Scanners, WAS): ці інструменти автоматично сканують веб-застосунки на наявність вразливостей, включаючи SQL-ін'єкції. Вони можуть бути динамічними (сканують працюючий веб-застосунок) або статичними (аналізують код джерела).

- Аналізатори коду статичного аналізу (Static Application Security Testing, SAST): ці інструменти аналізують вихідний код веб-застосунка на наявність потенційних вразливостей, включаючи SQL-ін'єкції. Вони допомагають розробникам виявляти та виправляти проблеми на ранніх стадіях розробки.

- Системи запобігання вторгненням у веб-застосунки (Web Application Firewalls, WAF): ці інструменти розміщуються між веб-застосунком та інтернетом і моніторять весь трафік. WAF можуть блокувати запити, які вважаються шкідливими, включаючи ті, що містять SQL-ін'єкції.

Крім інструментів, існують методи, які розробники можуть використовувати для захисту від SQL-ін'єкцій:

- Використання параметризованих запитів: це дозволяє динамічно створювати SQL-запити на основі вхідних даних, що допомагає запобігти SQL-ін'єкціям.

- Використання бібліотек ORM: ці бібліотеки спрощують взаємодію з базами даних і часто мають функції захисту від SQL-ін'єкцій.

- Ретельна валідація вхідних даних: перед використанням вхідних даних у SQL-запитах слід ретельно їх перевіряти, щоб запобігти використанню шкідливого коду в атаках SQL-ін'єкцій.

Висновки

Захист від SQL-ін'єкцій стає все більш важливим у світі веб-розробки, де безпека даних відіграє ключову роль. Автоматизація виявлення та захисту від цих атак відкриває можливості для розробників, дозволяючи їм зосередитися на розвитку продукту, зберігаючи при цьому високий рівень безпеки. Використання сучасних інструментів протидії подібним атакам забезпечує захист від загроз та підвищує надійність веб-додатків у цифровому середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Dafydd Stuttard, Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2 edition Wiley. 2011. 912c.
2. SQL-injections: vulnerabilities and how to prevent attacks [Електронний ресурс]. - Режим доступу URL: https://www.veracode.com/security/sql-injection
3. Wassermann G. Static Checking of Dynamically Generated Queries in Database Applications / Wassermann, G; Gould, C; Su, Z, et al. // ACM Transactions on Software Engineering and Methodology. – 2017.

Шпикуляк Андрій Віталійович – студент групи 2СП-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: andrii.sk2003@gmail.com

Shpykuliak Andrii Vitaliiovych - student of group 2SP-21b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: andrii.sk2003@gmail.com