Секція 1

ДОСЛІДЖЕННЯ БЕЗПЕКИ СУЧАСНИХ ORM ФРЕЙМВОРКІВ .NET

Чишкала С.А.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Орєхов О. О.

Актуальність. При розробці сучасних додатків часто виникає питання як додаток буде працювати з даними. З одного боку простішим для програмістів та дешевшим для власника продукту рішенням є використання сучасних ORM фреймворків, з іншого боку не все так однозначно, адже є багато «але» [1]. На етапі обговорення замовник та бізнес аналітик визначають список задач та всі вимоги до проекту. Все залежить від розмірів плануємого проєкту. Тема ORM завжди була і буде актуальною в розробці сучасних додатків, адже майже кожен додаток має свою базу даних і з цього постає питання, як цей додаток буде спілкуватися з базою і на скільки це безпечно [2].

Метою даної роботи є дослідження безпеки сучасних ORM бібліотек для .NET.

Основні положення. SQL-ін'єкція – це метод використання даних користувача через поле введення веб-сторінок [3]. Шкідливі дані, коли вони приймаються сервером або програмою, можуть використовуватися для маніпулювання даними користувача та компанії. Це одна з найпростіших і водночас найруйнівніших атакуючих ідей. Тисячі веб-серверів страждають щодня, завдаючи мільйони доларів збитків.

SQL-ін'єкція, залежно від типу використовуваної СУБД та умов впровадження, може дати 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, що атакується. Атака типу ін'єкції SQL може бути можлива через некоректну обробку вхідних даних, що використовуються в SQL-запитах [4]. Зловмисники можуть використовувати цю вразливість для отримання облікових даних користувачів з бази даних. Після чого вони можуть видавати себе за реальних користувачів та красти їхні гроші чи дані.

Зловмисники можуть отримати права адміністратора у базі даних, щоб стерти, скопіювати чи пошкодити всі дані на сервері. У деяких випадках SQL ін'єкція також дозволяє зловмисникам отримати доступ до операційної системи. Це призводить до атаки на внутрішню мережу вашого бізнесу. Розробники сайтів та додатків, що працюють з реляційними базами даних, повинні знати про такі вразливості та вживати заходів протидії. В роботі були розглянуті способи захисту впроваджені в ORM бібліотеках від подібного роду атак.

Висновки. Entity Framework дуже популярна бібліотека в розробці сучасних комерційних додатків. Однак, багато розробників навіть не підозрюють про те на скільки потужний функціонал бібліотека пропонує. Багато хто ігнорує безпечні підходи при використанні фрейморку, або не підозрює про їх існування. На практиці, це відбувається через брак знань розробників. Використання ORM недостатньо, щоб запобігти атакам, таким як ін'єкції SQL [5]. Розробники повинні коректно використовувати фреймворк, щоб уникати небезпечний коду.

Список літератури

1. Security Considerations. *Microsoft*. URL – https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/ef/security-considerations (дата звернення: 18.11.2021);
2. Secure Data Access. *Microsoft*. URL – https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/secure-data-access (дата звернення: 18.11.2021);
3. SQL injection. *Wikipedia*. URL – https://en.wikipedia.org/wiki/SQL_injection (дата звернення: 19.11.2021);
4. SQL Injection attacks in Entity Framework Core. *Adrientorris*. URL – https://adrientorris.github.io/entity-framework-core/SQL-Injection-attacks-in-Entity-Framework-Core-2-0.html (дата звернення: 19.11.2021);
5. Fixing SQL Injection: ORM is not enough. *Snyk*. URL – https://snyk.io/blog/sql-injection-orm-vulnerabilities/ (дата звернення: 20.11.2021).

Відомості про авторів

Чишкала Сергій Андрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 066-237-33-39, s.chyshkala@student.csn.khai.edu

Орєхов Олександр Олександрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н., професор, a.orehov@csn.khai.edu