БЕЗПЕКА ДАНИХ В ВЕБ-ДОДАТКАХ: ЯК ЗАХИСТИТИ ВІД UNION-BASED SQL INJECTION

Ляшко М.С., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Метою доповіді є розгляд однієї з найпоширеніших форм SQL ін'єкцій - "Union-based SQL Injection," та методів виявлення та запобігання цій загрозі. "Union-based SQL Injection" відноситься до технічних вразливостей, які дозволяють зловмисникам об'єднувати дані з різних таблиць бази даних через SQL-запити [1]. Зловмисники включають операцію UNION у SQL-запит, щоб об'єднати результати свого запиту з результатами легітимного запиту до бази даних. Це може призвести до витоку конфіденційних даних, такі як імена користувачів, паролі, номери кредитних карт, а також іншу конфіденційну інформацію з бази даних. Зловмисники можуть використовувати цю загрозу для незаконного доступу до системи та зміни її функціональності [2, 3].

Для запобігання "Union-based SQL Injection" необхідно вживати низку конкретних заходів безпеки:

– обмеження прав доступу. Користувачі повинні мати доступ лише до даних та функцій, які є необхідними для їхньої роботи, і ні в якому разі не повинні виконувати SQL-запити, які необхідні лише адміністраторам;

– моніторинг безпеки та аудит подій. Система повинна слідкувати за всіма SQL-запитами, що виконуються, та реагувати на незвичайну активність;

– вимкніть виведення помилок – у більшості випадків атакувальники використовують помилки, що відображаються програмою, для перегляду результатів бази даних;

– використання параметризованих запитів – ніколи не долучайте введені користувачем дані у вигляді рядків до SQL-запиту. Замість цього створюйте запит у коді і потім додаєте користувацькі дані як параметри;

– обмеження довжини введення – обмеження довжини полів вводу може запобігти атакам SQL-ін'єкції UNION;

– білий список символів – дані користувачів, які використовуються в SQL-запитах, повинні бути обмежені лише безпечними символами;

– чорний список символів – забороняйте загально вживані символи, які використовуються в SQL-ін'єкційних векторах;

– налаштування аудиту бази даних і встановлення системи виявлення/запобігання вторгнення (IDS/IPS).

Список літератури

1. What is SQL Injection UNION Attacks? GeeksforGeeks.com – URL: https://www.geeksforgeeks.org/what-is-sql-injection-union-attacks/

2. Union SQL Injection: How It Works and 6 Tips for Prevention. Bright – URL: https://brightsec.com/blog/union-sql-injection/

3. SQL injection UNION attacks. PortSwigger.net URL: https://portswigger.net/web-security/sql-injection/union-attacks