УДК 004.056

МЕТОДИКА ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В БАЗІ ДАНИХ ORACLE ВІД SQL-АТАК

METHODOLOGY FOR PROTECTING CONFIDENTIAL INFORMATION IN ORACLE DATABASES FROM SQL ATTACKS

Оксана Жигаревич, Анна Домбровська

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *This article explores safeguarding information confidentiality in Oracle databases from SQL attacks, stressing the need for effective protection measures amid increasing cyber threats.*

Захист інформації в базах даних є важливим аспектом інформаційної безпеки. Включає заходи, спрямовані на забезпечення конфіденційності, цілісності та доступності даних, запобігання несанкціонованому доступу, викраденню або модифікації інформації. Основні методи захисту включають шифрування, контроль доступу, аудит та моніторинг.

GDPR визначає вимоги до захисту персональних даних громадян ЄС, включаючи права суб'єктів даних та обов'язки організацій щодо захисту інформації. Відомі випадки значних штрафів включають штрафи для Google, British Airways за порушення вимог GDPR, що стало наслідком витоків даних та неналежного захисту інформації користувачів. База даних - це організована сукупність даних, що забезпечує зберігання, управління та доступ до інформації.

Oracle Database є однією з найпопулярніших СУБД завдяки своїй високій продуктивності, надійності та можливостям масштабування. Забезпечує широкі функціональні можливості для управління даними та їх захисту. SQL-ін’єкції є однією з найпоширеніших вразливостей веб-додатків, що дозволяють зловмисникам виконувати довільні SQL-запити, маніпулювати базами даних та отримувати несанкціонований доступ до конфіденційної інформації. Існує два основних типи SQL-ін’єкцій: Error-based SQLi та Blind SQLi.

Стандартні методи включають використання параметризованих запитів, перевірку введених даних, регулярний аудит безпеки. Використання placeholder’ів значно знижує ризик SQLi, дозволяє уникнути динамічної побудови запитів з неперевіреними даними. Захисту інформації в Oracle використовує складний метод шифрування, використання ролей та привілеїв, а також спеціалізовані функції для моніторингу та виявлення підозрілої активності.

Висновки: Аналізуючи аналітичні та базові поняття захисту інформації, було визначено, що конфіденційність, цілісність, доступність, аутентифікація та авторизація є ключовими аспектами безпеки. Досліджено основні характеристики бази даних Oracle, такі як архітектура та функції. Розглянуто типи SQL-ін’єкцій та їхні механізми реалізації, зокрема Error-based SQL injection та Blind SQL injection. Проаналізовано та запропоновано методи захисту баз даних Oracle від SQL-ін'єкцій, включаючи використання параметризованих запитів та методики захисту конфіденційності інформації.

Бібліографія

1. IDC: Oracle Autonomous Database [Електронний ресурс]. – Режим доступу: [https://www.oracle.com/a/ocom/docs/corporate/analystrelations/idc-oracle-autonomous-database.pdf]
2. MySQL 8.0 Reference Manual: Security Guidelines [Електронний ресурс]. – Режим доступу: [https://dev.mysql.com/doc/refman/8.0/en/security-guidelines.html]