Вступ

Практикум “Безпека баз даних” присвячений питанням безпеки операцій із даними, а саме: цілісності й безпеці даних, гарантованій безпеці операцій у базах даних. Він побудований на принципах забезпечення конфіденційності, цілісності та доступності даних.

Курс практикуму починається з питань забезпечення цілісності даних і завершується темами вразливостей та розмежування доступу. Водночас розглядаються аномалії, що виникають у процесі спільної роботи, та проблеми продуктивності, які можуть бути спричинені, зокрема, діями зловмисника.

Перша лабораторна робота присвячена забезпеченню цілісності даних. Розглядаються різні види цілісності, закріплюються навички забезпечення цілісності та несуперечності даних. Окремо вивчаються недекларативні методи забезпечення цілісності.

Друга лабораторна робота спрямована на набуття навичок формування інтерфейсного рівня доступу до даних. Надання користувачеві безпосереднього доступу до базових відносин СУБД є невдалим рішенням як із погляду безпеки даних, так і подальшої еволюції схеми даних. Побудова проміжного рівня за допомогою представлень, процедур і функцій дає змогу приховати реальні дані та здійснювати рефакторинг бази даних без впливу на користувацькі інтерфейси додатків.

Третя лабораторна робота присвячена забезпеченню цілісності даних за багатокористувацького доступу та підтримання працездатності СУБД під навантаженням. Вона ілюструє різні рівні ізоляції транзакцій та аномалії, які виникають у багатокористувацькому режимі.

Четверта лабораторна робота розглядає питання оптимізації запитів і побудови індексів. Аналізуються плани запитів, оцінюється ефективність використання індексів. Також передбачається аналіз і можливість трансформації запитів для їх оптимізації відповідно до правил реляційної алгебри. Робота орієнтована на набуття навичок виявлення атак на продуктивність і методів їх запобігання.

П’ята лабораторна робота присвячена управлінню доступом у реляційних серверах. Особлива увага надається засобам управління з дрібною грануляцією доступу, зокрема на рівні окремих полів. Оскільки вбудовані механізми СУБД часто є недостатньо гнучкими, управління доступом реалізується як вбудованими засобами СУБД, так і додатковими механізмами, розробленими студентами. Також розглядається завдання маскування даних, що є критично важливим для сховищ із високим рівнем секретності, аби приховати не лише вміст конфіденційної інформації, а й сам факт існування відповідного рівня захисту.

Шоста лабораторна робота присвячена ознайомленню з типовими вразливостями реляційних серверів та методами їх усунення. Незважаючи на відмінності між СУБД та їхніми SQL-діалектами, реляційні сервери мають як специфічні, так і загальні вразливості. До проблем, характерних для різного програмного забезпечення (наприклад, вразливості алгоритмів шифрування або каналів доступу), додаються особливі загрози, пов'язані з моделлю зберігання даних і принципами обробки запитів. Деякі уразливості, зокрема переповнення буфера, можуть мати власну інтерпретацію та використання. У межах лабораторної роботи аналізуються основні загрози та виконуються практичні завдання з їх усунення.

Кожна лабораторна робота містить короткі теоретичні відомості, завдання на роботу, зміст звіту, варіанти виконання, контрольні запитання, список літератури та приклад виконання на PostgresSQL.

Загалом практикум створений для студентів, які знають основи побудови та адміністрування баз даних. Він має на меті розвиток практичних навичок і теоретичних знань із широкого спектра питань захищеності реляційних СУБД – від забезпечення цілісності та доступності даних до виявлення загроз.

Встановлення та налаштування серверів управління базами даних для MySQL, PostgreSQL та Oracle не розглядається, але надаються посилання на необхідні ресурси для самостійного опрацювання.

Автори вдячні випускниці кафедри безпеки інформаційних технологій Соломії Масник за надання прикладів виконання лабораторних робіт Практикуму.