DOI https://doi.org/10.30525/978-9934-26-506-8-103

SECURING WEB APPLICATIONS IN COMPUTERIZED MANAGEMENT SYSTEMS: MODERN THREATS AND EFFECTIVE PROTECTION METHODS

БЕЗПЕКА ВЕБ-ДОДАТКІВ У КОМП'ЮТЕРИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ: СУЧАСНІ ЗАГРОЗИ ТА ЕФЕКТИВНІ МЕТОДИ ЗАХИСТУ

Hurkovska S.S.,
PhD (Engineering), Associate Professor, LLC "Technical university "Metinvest polytechnic", Zaporizhzhia, Ukraine

Гурковська С.С.,
к.т.н., доцент, ТОВ «Технічний університет «Метінвест політехніка», м. Запоріжжя, Україна

Одним з найважливіших аспектів ведення сучасного бізнесу є інформаційна безпека. Все частіше бізнес використовує різноманітні веб-сервіси для заохочування користувачів, тобто бізнес-процеси активно інтегруються з інформаційними системами, це в свою чергу накладає певну відповідальність процес обробки та збереження великого обсягу чутливих даних. Тому постає задача постійного вдосконалення методів захисту.

Одна з найпоширеніших загроз витоку конфіденційної інформації це атака типу XSS (Cross-Site Scripting). Такий тип атаки дає можливість зловмисникам вбудовувати шкідливий код у веб-додаток. Такий код дає можливість підміняти особистість користувача. Це може призвести до витоку конфіденційної інформації, зміни важливих бізнес-даних або перенаправлення користувачів на сторонні сайти. Щоб захиститися від подібних атак є кілька способів, в тому числі впровадження Content Security Policy (CSP) дозволяє захиститися від таких атак, обмежуючи завантаження та виконання сторонніх ресурсів у веб-додатку.

Такий вид атаки як CSRF (Cross-Site Request Forgery) дає можливість зловмиснику використовувати сеанс авторизованого користувача для виконання непередбачених та небажаних операцій. Така атака також являє собою серйозний ризик для бізнес-систем, оскільки можливі несанкціоновані транзакції, зміна налаштувань або маніпуляція даними. Захист від CSRF передбачає використання CSRF-токенів, які генеруються на сервері та перевіряються під час кожного запиту, що надходить до бізнес-системи.

SQL-ін'єкції є ще однією поширеною загрозою, яка дозволяє зловмисникам маніпулювати запитами до бази даних, отримувати

доступ до чутливої інформації, видаляти або змінювати дані. Цей тип атака може порушити цілісність даних, що використовуються у процесах управління бізнесом. Використання параметризованих запитів та ORM-фреймворків дозволяє значно зменшити ризики SQL-ін'єкцій, оскільки ці підходи запобігають прямій маніпуляції SQL-кодом.

Комплексний підхід до захисту веб-додатків, які використовуються в бізнес-процесах, передбачає впровадження заходів безпеки на кожному етапі життєвого циклу розробки. Це означає, що тестування на вразливості, регулярні аудити коду та постійне оновлення компонентів повинні стати невід'ємною частиною розробки та підтримки додатків. Важливо також проводити моніторинг і швидко реагувати на нові загрози, адаптуючи систему захисту відповідно до змін у ландшафті кібербезпеки.

Безпека веб-додатків – це критичний аспект в системах інтерактивного управління бізнес-процесами, який вимагає постійного контролю та оновлення, а також введення певних інноваційних рішень. Запровадження сучасних методів захисту дозволяє не тільки захистити дані компанії, а й забезпечити стабільність бізнес-процесів, що є основою успішної діяльності у цифровому середовищі.

DOI https://doi.org/10.30525/978-9934-26-506-8-104

PROJECT CALENDAR IN MICROSOFT EXCEL: A FLEXIBLE, CONVENIENT, AND QUICK PLANNING METHOD

ПРОЄКТНИЙ КАЛЕНДАР В MICROSOFT EXCEL: ГНУЧКИЙ, ЗРУЧНИЙ ТА ШВИДКИЙ СПОСІБ ПЛАНУВАННЯ

Derzhevetska M.A.,
PhD (Economics),
LLC "Technical university "Metinvest polytechnic",
Zaporizhzhia, Ukraine

Держевецька М.А.,
к.е.н.,
ТОВ «Технічний університет «Метінвест політехніка»,
м. Запоріжжя, Україна

Календарне планування у бізнес-процесах відіграє ключову роль, оскільки є інструментом, що забезпечує структурованість і послідовність роботи на кожному етапі проєкту. Чіткий графік дозволяє не лише організувати процеси, а й значно підвищити ефективність управління ресурсами, зокрема людськими, матеріальними та технічними. Календар дозволяє уникнути простоїв та дублювання зусиль, адже кожен етап виконується в оптимальні терміни. Він стає важливим джерелом аналітики, оскільки дає змогу оцінити ефективність виконання проєкту після його завершення, виявити причини можливих затримок і скорегувати процеси для майбутніх проєктів. Таким чином,