УДК 004.056

Д.О. Козак

РОЗРОБКА ЗАХИЩЕНОГО ВЕБ-ДОДАТКУ ДЛЯ ОБРОБКИ ЗАПИТІВ КОРИСТУВАЧІВ

Вінницький національний технічний університет

Анотація

В роботі розглянуто теоретичну базу та здійснено аналіз необхідності створення захищеного веб-додатку для обробки запитів клієнтів. А саме: проаналізовано основні тенденції у розробці комерційних Інтернет-ресурсів з урахуванням усунення виявлених недоліків, створено алгоритми, що плануються бути використані при під час програмного реалізації захищеного веб-додатку.

Ключові слова: веб-додатки, запити клієнтів, дані, авторизація, реєстрація, база даних, клієнтський сервер, візуалізація.

Abstract

The paper considers the theoretical basis and analyzes the need to create a secure web application for processing customer requests. Namely: the main trends in the development of commercial Internet resources are analyzed, taking into account the elimination of identified shortcomings, created algorithms that are planned to be used during the software implementation of a secure web application.

Keywords: web applications, customer requests, data, authorization, registration, database, client server, visualization.

Вступ

Вразливість веб-додатків залишається одним з найбільш поширених недоліків забезпечення захисту інформації. Серед інших проблем, які часто зустрічаються, є низька обізнаність співробітників у питаннях інформаційної безпеки, слабка парольна політика або повсюдне її невиконання, недоліки в процесах управління оновленням програмного забезпечення, використання небезпечних конфігурацій, і, як це може здатися парадоксальним, неефективним міжмережевим розмежуванням доступу. Незважаючи на те, що вразливості веб-додатків неодноразово описані в сучасній науковій та спеціалізованій літературі, досить рідко зустрічаються превентивні захисні механізми, що знижують ризики ураження.

Метою даної роботи є аналіз та розробка захищеного веб-додатку для обробки запитів користувачів.

Принцип роботи веб-додатків та ризики

Вдалий веб-сайт – це надзвичайно ефективний інструмент зв’язку з клієнтами та ведення бізнесу – він здатний захоплювати увагу аудиторії. Як і будь-який інший маркетинговий інструмент, заснований на принципі безпосереднього відгуку, перш за все він повинен заінтригувати відвідувача, а потім спонукати його на певні дії [1]. Такі веб-сайти, хоча і містять іноді величезну кількість корисних статей, практично ніколи не досягають передбачуваного рівня відвідуваності. Веб-сайт, здатний привернути увагу і викликати цікавість, спонукає клієнтів не тільки переглянути сторінки і здійснити замовлення, але і знову відвідати його через деякий час, рекомендувати знайомим [2].

Проте, разом з цим зростає і необхідність розробки надійного захисту даних та захисту від НСД до таких веб-сайтів, враховуючи важливість даних, що обробляються на сайті, складність процесу їх передачі та можливі ризики витоку (рис. 1).

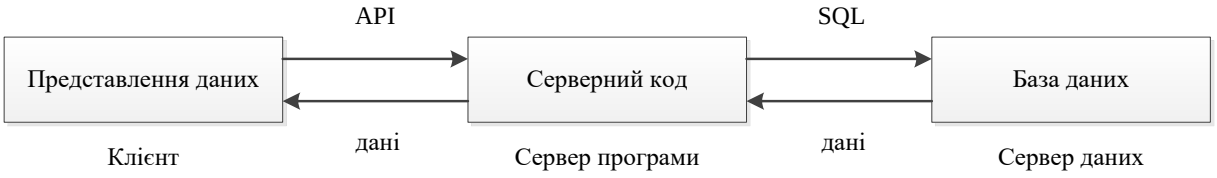

Рисунок 1 – Взаємодія частин програмного забезпечення веб-додатку (за [5])

Проблема захищеності веб-додатків посилюється тим, що при їх розробці не завжди враховуються проблеми, пов’язані з захистом цих систем від внутрішніх і зовнішніх небезпек або не достатньо уваги приділяється даному процесу. Це, в свою чергу може породжувати ситуацію, в якій проблеми інформаційної безпеки потрапляють у поле зору власника системи вже після завершення проекту, а усунути вразливість у вже створеному веб-додатку є більш витратною статтею бюджету, ніж при його розробці та впровадженні. Недостатня оцінка серйозності ризику загрози інформаційної безпеки з використанням веб-прикладних програм, доступних через Інтернет є основним фактором низького рівня захисту [3].

Структура та функціональні можливості захищеного веб-додатку

Аналізуючи поставлені задачі обраної теми, існує необхідність проектування програмного комплексу на основі веб-технологій. Головною перевагою веб-додатку перед іншими варіантами є його універсальність і можливість використання на будь-яких пристроях без портування на цільову операційну систему (браузер і його віртуальна машина виступає як цільова універсальна операційна система і комп’ютер). Для реалізації поставленої задачі було вирішено використовувати три ланкову архітектуру, яка складається з таких компонентів: клієнт, сервер і база даних. Схема даної архітектури зображена на рисунку 2.

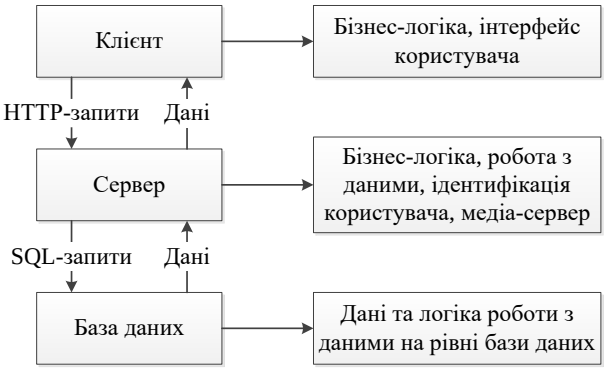

Рисунок 2 – Компоненти розроблюваного захищеного веб-додатку

При розробці веб-додатку важливо розуміти його першочергову мету, що вбачається у приверненні уваги клієнтів до ресурсу. Це означає, що розроблений веб-додаток повинен: відповідати базовим вимогам організації аналогічних веб-додатків; мати інтуїтивно-зрозумілий та компактний інтерфейс; забезпечувати функціонал пошуку сторінок, що є орієнтований на галузь до якої відноситься розроблюваний веб-додаток [4]. Враховуючи ряд функцій, що вимагають своєї реалізації для ефективної роботи веб-додатку, можна виділити такі основні елементи (рис. 3).

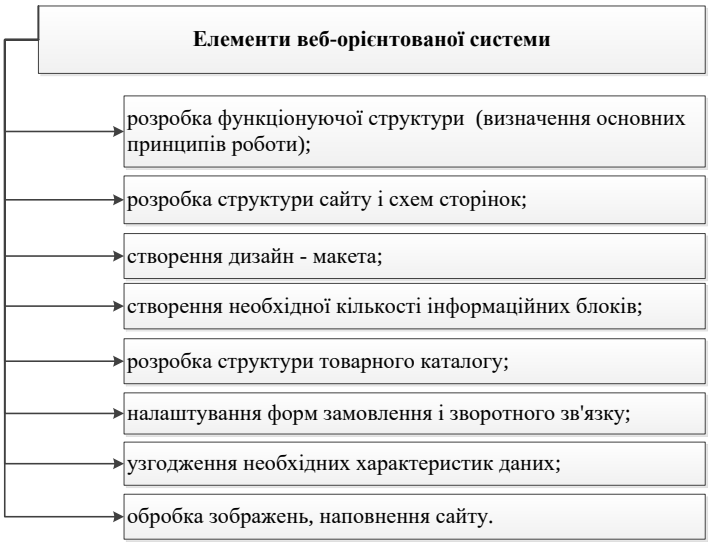

Рисунок 1.3 – Основні елементи веб-орієнтованої системи

Зворотною, невидимою для клієнта, стороною веб-додатку є система управління. Вхід в систему адміністрування здійснюється тільки після введення адміністратором логіна і пароля. Функціональні можливості адміністратора наведено на рисунку 4.

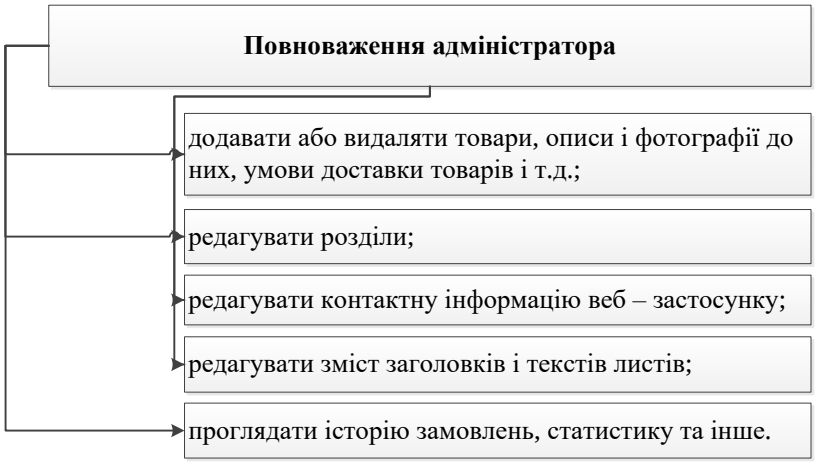

Рисунок 4 – Можливості адміністратора на захищеному веб-додатку

Для програмної розробки системи необхідно створити структурну схему алгоритму веб-додатку, відповідно до якої буде правильно функціонувати веб-орієнтована система. Структурну схему алгоритму веб-додатку можна представити у вигляді схеми (рис. 5).

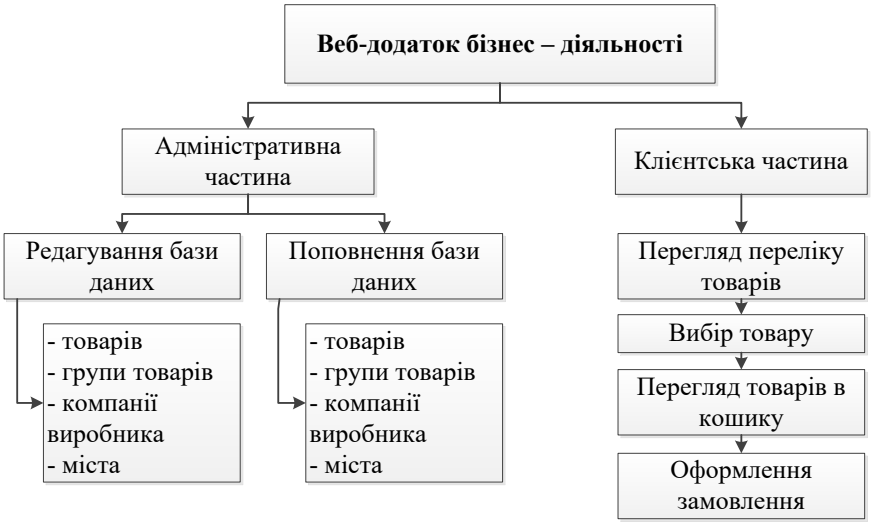

Рисунок 5 – Інформаційні розділи розроблюваного захищеного веб-додатку

Із структури можна побачити, що в веб-додатку пропонується дві робочих частини: адміністративна та клієнтська.

Після входження в систему управління, адміністративна частина дозволяє адміністратору редагувати бази даних та вносити в них додаткові елементи.

Клієнтська частина не має такої можливості, тобто доступ до ресурсів веб-додатку закритий для загального огляду. Разом з тим, клієнтська частина доступна всім користувачам і відвідувачам веб-додатку. Її функціонал дозволяє клієнтам здійснювати перегляд, пошук, вибір потрібного товару, який розміщений в різних групах. Це значно полегшує роботу користувача під час пошуку певної інформації. Клієнт має змогу знайти необхідну інформацію, оформити замовлення товару, вибрати тип оплати.

Розробка алгоритму роботи захищеного веб-додатку

Розроблюваний алгоритм роботи веб-додатку полягає у тому, що за допомогою браузера, клієнт звертається до сервера і потрапляє на головну сторінку веб-додатку. Сервер аналізує запит на

відповідний файл. Потім сервер передає файл на обробку інтерпретатору PHP. Далі інтерпретатор передає дані серверу, який передає html-розмітку клієнту. В загальному, орієнтовний послідовний алгоритм такого звернення представлений на рисунку 6.

Рисунок 6 – Алгоритм запиту та відповіді на захищеному веб-додатку

Алгоритм роботи користувача на розроблюваному веб-додатку, можна описати наступними кроками, при цьому враховуючи, що веб-додаток здійснює обробку всіх сторінок через файл index.php, а контент сторінки визначається змінною id.

Крок 1. Перехід користувачем за посиланням на веб-додаток (URL).

Крок 2. Перевірка доступності файлу. Якщо файл доступний, відбувається вивід файлу. Далі – перехід до кроку 5. Якщо файл недоступний, відбувається передача обробки в index. Далі – перехід до кроку 3.

Крок 3. Розбір URL, запит до бази даних про співпадіння URL і id_page.

Крок 4. Перевірка чи відбулось співпадіння. Якщо співпадіння відбулося, відбувається вивід id. Далі – перехід до кроку 5. Якщо співпадіння не відбулось, отримується на сторінці повідомлення про помилку (Error 404). Далі – перехід до кроку 5.

Крок 5. Завершення роботи з веб-додатком.

Схематично описаний алгоритм наведено на рисунку 7.

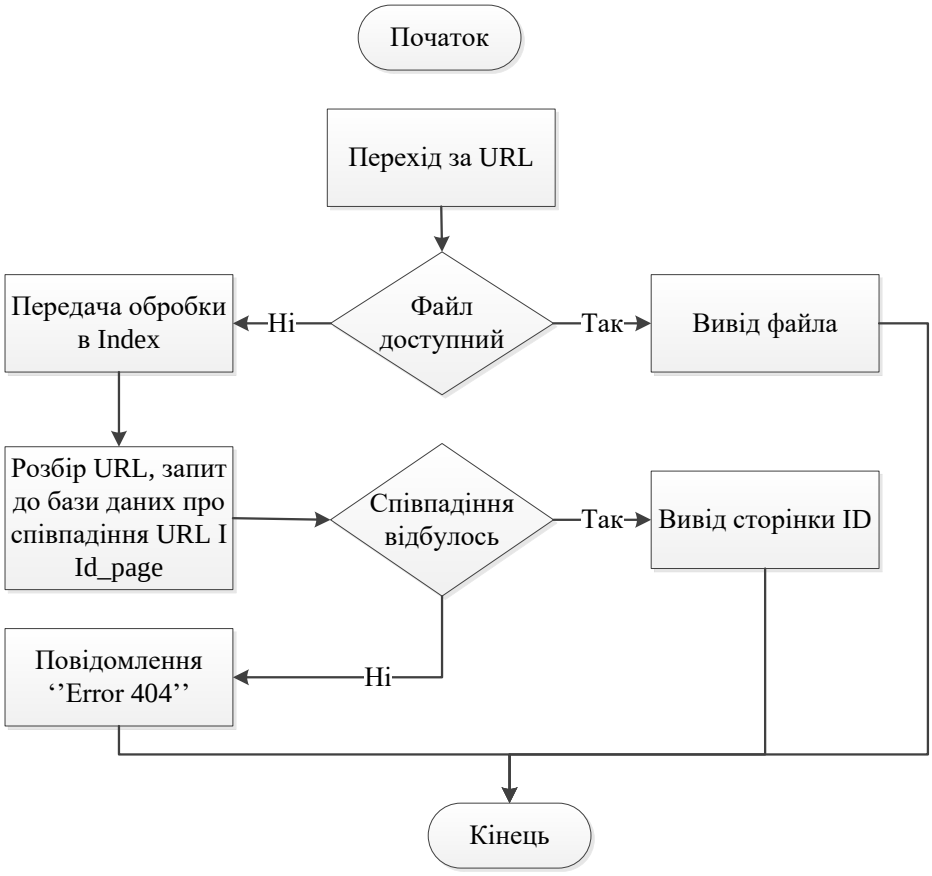

Рисунок 7 – Алгоритм роботи звернень до захищеного веб-додатку

Оскільки, сучасні загальнодоступні веб-додатки цікаві хакерам як ресурси або інструменти заробітку, а спектр застосування отриманої в результаті злому інформації широкий: платне надання

доступу до ресурсу, використання у бот-мережах і т. д. Особа власника не важлива, оскільки процес злому автоматизований і поставлений на потік. Вартість інформації пропорційна популярності і впливовості компанії. Доцільним є розробка модулів захисту веб-додатків.

Виходячи з поставлених цілей роботи, для захищеного веб-додатку були розроблені такі методи захисту як: захист на основі протоколу HTTPS та протоколу SSL; запобігання SQL-ін'єкції; перевірка і шифрування паролів; захищені плагіни послуг оплати та доставки; розподілення прав доступу до даних ресурсу (рис. 8).

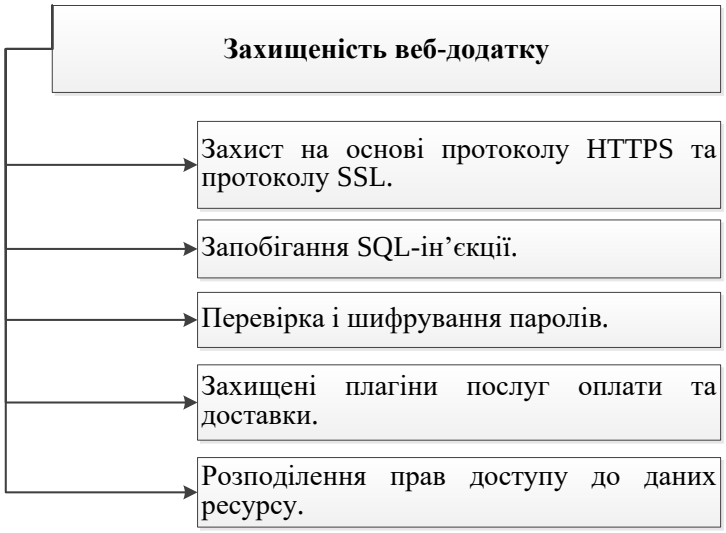

Рисунок 8 – Засоби захисту веб-додатку

Таким чином, на основі розроблених алгоритмів, наведених модулів веб-додатку, при подальшій роботі у даній галузі планується здійснити практичну реалізацію захищеного веб-додатку на основі наведених вище засобів.

Висновки

Отже, завдання надійного захисту веб-ресурсів від несанкціонованого доступу є однією з найпоширеніших і майже невирішених сьогодні проблем.

Тема роботи є актуальною, оскільки бурхливий розвиток IT-технологій суттєво впливає на необхідність створення і розробки програмного забезпечення для мережі Інтернет, а в комплексі з проблемою захищеності веб-додатків є важливою задачею, що потребує вирішення.

Враховуючи сучасні засоби розвитку та зумовлену ними необхідність втілення в життя постійних актуальних розробок для мережі Інтернет, в роботі значна надається увага розробці якісної платформи для введення бізнес-діяльності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Фролов А. В. Бази даних в Мережі інтернет. Практичний посібник по створенню Web-додатків з базами даних: посіб. Москва, 2000. 448 с.

2. Макарова М.В. Електронна комерція: Посібник для студентів. вищих навчальних закладів: навч. посіб. Київ: Видавничий центр «Академія», 2002. 272 с.

3. Richard Petersen, Linux Mint 17.2: Desktops and Administration, July 1, 2015. 455 c.

4. Charles Bell, Windows 10 for the Internet of Things, October 27, 2016. 467 c.

5. Sean D. Liming, John R. Malin, Professional's Guide to Windows Embedded Standard 7, August 30, 2012. C. 45–211.

Козак Діана Олегівна – студентка групи УБ-21м, факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: kdo99@ukr.net

Kozak Diana O. – student, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: kdo99@ukr.net