ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(повне найменування вищого навчального закладу)

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
(повне найменування інституту, назва факультету (відділення))

КАФЕДРА ПРОГРАМНИХ ЗАСОБІВ І ТЕХНОЛОГІЙ
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка
до магістерської кваліфікаційної роботи

другий (магістерський) рівень вищої освіти
(освітньо-кваліфікаційний рівень)

на тему: «Дослідження та застосування методів безпеки в інтернет-магазині, створеному на Laravel »

Виконав: студент 2 курсу, групи 6ПР
напряму підготовки
121 «Інженерія програмного забезпечення»
(шифр і назва напряму підготовки, спеціальності)

Мальченко О.В
(прізвище та ініціали)

Керівник: к. т. н., доцент Огнєва О.Є
(прізвище та ініціали)

Рецензент Вишемирська С.В
(прізвище та ініціали)

Хмельницький – 2023

Херсонський національний технічний університет

(повне найменування вищого навчального закладу)

Інститут,факультет,відділенняФакультетінформаційнихтехнологійта дизайну
Кафедра Програмних засобів і технологій
Освітньо-кваліфікаційний рівень другий (магістерський)
(шифр і назва)

Спеціальність 121 – Інженерія програмного забезпечення
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри ПЗіТ
к. т. н. доцент О.Є. Огнєва

“ “ 2023 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Мальченко Олександр Володимирович
(прізвище, ім’я, по батькові)

1. Тема проекту (роботи) «Дослідження та застосування методів безпеки в інтернет-магазині, створеному на Laravel»
керівник проекту (роботи) к. т. н., доцент Огнєва Оксана Євгенівна,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджена наказом вищого навчального закладу від “ ‘‘ 2023 р. № -с
2. Строк подання студентом проекту (роботи) 28.11.2023
3. Вихідні дані до проекту (роботи) ДСТУ з обробки інформації, літературні та періодичні джерела, матеріали походження практики. *
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз предметної області, постановка задачі;
2. Розробка моделі, структури даних та інтерфейсу кінцевого користувача;
3. Опис алгоритмів та розробка програмного забезпечення;
4. Аналіз отриманих результатів;
5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)
10 слайдів.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 17.09.2023

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної Роботи бакалавра	Строк виконання етапів проекту (роботи)	Примітка
1	Відбір та вивчення літературних джерел	18.09.2023	виконано
2	Складання технічного завдання.	22.09.2023	виконано
3	Огляд існуючих рішень, передумови до створення нового програмного засобу.	25.09.2023	виконано
4	Постановка завдання, точне формулювання з описом вхідної і вихідної інформації.	28.09.2023	виконано
5	Розробка концептуальної моделі, аналіз об'єктів і дій, інфологічне моделювання	01.10.2023	виконано
6	Математичне моделювання, опис математичної моделі і методів вирішення завдань, опис методики і способу здобуття рішення.	30.10.2023	виконано
7	Програмна реалізація, вибирання технічних і програмних засобів побудова призначеного для користувача інтерфейсу, програмування поставленого завдання.	19.11.2023	виконано
8	Складання програмної документації, оформлення пояснювальної записки, проходження норм контролю.	18.12.2023	виконано

Студент _____ Мальченко О.В
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ Огнєва О.Є
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

В даній магістерській кваліфікаційній роботі на тему "Дослідження та застосування методів безпеки в інтернет-магазині, створеному на Laravel" спрямована на вивчення та реалізацію ефективних заходів безпеки в інтернет-магазині, побудованому за допомогою фреймворку Laravel. Робота включає детальний аналіз існуючих методів захисту та їх впровадження в контекст Laravel для максимальної безпеки користувачів та даних.

Основні етапи роботи включають в себе вивчення поточних тенденцій в галузі кібербезпеки та аналіз вразливостей, що можуть виникнути в інтернет-магазині. На основі цього аналізу розробляються та імплементуються конкретні стратегії захисту, такі як використання Web Application Firewall (WAF), Content Security Policy (CSP), протоколу HTTPS тощо.

Кваліфікаційна робота також зосереджується на реалізації захисту від SQL-ін'єкцій, кросс-сайтових сценаріїв та інших атак, що можуть виникнути у веб-додатку. Окрема увага приділяється захисту персональних даних користувачів та забезпеченню конфіденційності інформації.

ANNOTATION

In this master's qualification work on the topic "Research and application of security methods in an online store created on Laravel" is aimed at studying and implementing effective security measures in an online store built using the Laravel framework. The work includes a detailed analysis of existing security methods and their implementation in the Laravel context for maximum user and data security.

The main stages of the work include the study of current trends in the field of cyber security and the analysis of vulnerabilities that may arise in the online store. Based on this analysis, specific protection strategies are developed and implemented, such as the use of Web Application Firewall (WAF), Content Security Policy (CSP), HTTPS protocol, etc.

Qualification work also focuses on implementing protection against SQL injections, cross-site scripting and other attacks that may occur in a web application. Special attention is paid to the protection of personal data of users and ensuring the confidentiality of information.

РЕФЕРАТ

Магістерська кваліфікаційна робота: 93 сторінки, 24 рисунка, 45 використаних джерел, 1 додаток.

Магістерська кваліфікаційна робота присвячена дослідженню та застосуванню методів безпеки в інтернет-магазині, розробленому з використанням фреймворку Laravel. Мета дослідження полягає в вивченні та впровадженні ефективних стратегій забезпечення безпеки, які забезпечують високий рівень захисту для користувачів та конфіденційність даних.

У роботі розглянуті основні виклики та загрози, що можуть виникнути в інтернет-магазині, і проведений аналіз існуючих методів захисту. Зокрема, акцент зроблено на використанні передових технологій безпеки, таких як Web Application Firewall (WAF), Content Security Policy (CSP) та протокол HTTPS.

Детально розглянуті питання захисту від SQL-ін'єкцій, кросс-сайтових сценаріїв та інших потенційних атак. Спеціальна увага приділяється захисту персональних даних користувачів та забезпеченню конфіденційності інформації.

Результатом дослідження є впровадження комплексу заходів, спрямованих на забезпечення безпеки та надійності функціонування інтернет-магазину на основі Laravel.

Ключові слова: LARAVEL, ІНТЕРНЕТ-МАГАЗИН, ВЕБ-БЕЗПЕКА

ЗМІСТ

ВСТУП

Взаємодія бізнесу зі споживачами та партнерами глибоко змінилася завдяки мережним технологіям, впливаючи на процеси купівлі-продажу та формування бізнес-моделей. Інтернет-технології, як складова інформаційних систем, стали невід'ємною частиною сучасного бізнесу. Однак для підтримання ефективності інформаційних технологій необхідне постійне оновлення, оскільки їх застосування без цього може спричинити моральний знос, що призводить до функціональної непридатності та фінансових збитків для підприємства. Забезпечення відповідного стану інформаційних технологій неможливе без ефективного використання інтернет-технологій.

В сучасному цифровому віку, коли електронна комерція стає невід’ємною частиною підприємництва, питання забезпечення безпеки інтернет-магазинів стають вкрай важливими. Зростання обсягів онлайн-торгівлі призводить до появи нових викликів у сфері інформаційної безпеки. Методи атак на веб-ресурси стають більш вдосконаленими, а потенційні загрози для конфіденційності, цілісності та доступності даних стають різноманітнішими. Ця дипломна робота присвячена дослідженню та застосуванню ефективних методів безпеки в інтернет-магазині, розробленому на платформі Laravel. Laravel, як високопродуктивний і елегантний фреймворк для розробки веб-застосунків, надає потужний інструментарій для створення високоякісних онлайн-торгівельних платформ. Однак важливо не лише створювати функціональні продукти, але і забезпечувати їхню повноту інформаційної безпеки.

Метою даної роботи є проведення комплексного аналізу потенційних загроз безпеці в інтернет-магазинах, розгляд можливих атак та виявлення слабких місць веб-застосунку, розробка та реалізація ефективних методів захисту для запобігання можливим інцидентам безпеки. Дослідження цієї теми є актуальним і важливим завданням в умовах швидкого розвитку технологій

та зростання кількості онлайн-злочинів. Результати роботи можуть стати цінним внеском у покращення безпеки електронної комерції та сприяти подальшому розвитку інтернет-торгівлі.