Міністерство освіти і науки України

Тернопільський НАЦІОНАЛЬНИЙ технічний Університет

імені Івана Пулюя

ФАКУЛЬТЕТ КОМП’ЮТЕРНО ІНФОРМАЦІЙНИХ СИСТЕМ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

КАФЕДРА КІБЕРБЕЗПЕКИ

**Вишковський Сергій Робертович**

УДК 004.9:61

**ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОГО ВЕБ-САЙТУ "TRAVEL ANYWHERE" ТА МЕТОДІВ ЇХ УСУНЕННЯ**

спеціальність 125 «Кібезбезпека»

**Автореферат**

наукової роботи на здобуття освітнього ступеня «магістр»

Тернопіль-2018

|  |
| --- |
| Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя |
| Керівник роботи: | кандидат технічних наук, доцентЗагородна Наталія ВолодимирівнаТернопільський національний технічний університет імені Івана Пулюя,  |
| Рецензент: | кандидат технічних наук, доцентЗолотий,Тернопільський національний технічний університет імені Івана Пулюя |

Захист відбудеться 26 грудня 2018 р. о 11.00 годині на засіданні Державної екзаменаційної комісії кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя за адресою: м. Тернопіль, вул. Руська 56.

Науковий керівник к.т.н., доц. Загородна Н.В.

**ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ**

***Актуальність теми***. Число компаній, які застосовують веб-технології для підвищення продуктивності роботи і залучення нових клієнтів, зростає з кожним роком. Безсумнівно, інтернет-сервіси несуть з собою безліч переваг, але є й зворотна сторона медалі – з ростом числа додатків збільшується і кількість кіберзагроз. Так, компанія Symantec в своєму звіті Global Internet Security Threat Report (ISTR) вказує, що кіберзлочинці при зломі веб-сайтів зазвичай використовують вразливості веб-додатків, що працюють на сервері, або експлуатують деякі вразливості операційної системи, на якій працюють ці додатки. Наприклад, за допомогою атак типу XSS хакер може перенаправити запити користувачів на шкідливі веб-сторінки, а за допомогою SQL-ін’єкцій – витягувати з баз даних сайту різну конфіденційну інформацію. У відповідь на масові зломи систем безпеки був створений консорціум OWASP – Open Web Application Security Project, це відкритий проект забезпечення безпеки веб-додатків. Однак і зловмисники, і фахівці в області кібербезпеки продовжують знаходити вразливості в веб-додатках, які можуть привести до серйозних втрат з боку бізнесу. Основною причиною більшості взломів в веб-додатках є написаний розробниками програмний код. Розробники можуть допускати помилки при написанні коду або не усвідомлювати всю важливість використання прийомів безпечного програмування – все це призводить до появи вразливостей в додатках.

За даними щорічного дослідження корпоративних ризиків «Барометр рисков Allianz 2016», яке було складено на основі опитування більш  ніж 820  ризик-менеджерів і страхових експертів з 44 країн, вперше в ТОП-3 корпоративних ризиків увійшли кіберзлочини. Вони ж вказуються як найбільш значний ризик для підприємств в довгостроковій перспективі наступних 10 років. Згідно з прогнозами дослідницької компанії Cybersecurity Ventures, до 2021 року збиток від кібершахрайства збільшиться вдвічі у порівнянні з 2015 роком і досягне $ 6 трлн. Основною метою кіберзлочинців традиційно є різні фінансові організації, в першу чергу – банки, а також майданчики електронної комерції. При цьому, згідно з даними звіту Trend Micro Incorporated за перше півріччя 2016 року, однією з найбільш значущих загроз у фінансовій галузі як і раніше залишаються банківські трояни. Вкрадена троянами інформація використовується правопорушниками для проведення шахрайських транзакцій або продається на підпільних сайтах. Більш того, в результаті подібних шкідливих дій фінансові організації змушені нести витрати на компенсацію збитків, які понесли їх клієнти в результаті кібератак. Дуже часто основною точкою злому організації стає саме веб-додаток. Загроза злому веб-додатків залишається однією з найсерйозніших проблем для веб-ресурсів будь-якої спрямованості. Відчути себе хакером сьогодні може навіть людина, слабо підготовлений технічно – методи злому і необхідні інструменти доступні у відкритому вигляді і легко можуть бути знайдені за допомогою звичайних пошуковиків.

Тому існує необхідність у створення веб-застосунку, який би був відносно захищеним і користувач відвідуючи такий сайт не відчував загрози що його особисті данні, або що ще гірше це гроші, можуть бути викрадені навіть без його відому.

***Мета та завдання дослідження***. Метою дослідження є аналіз можливих атак і загроз на веб-додатки. Необхідно проаналізувати існуючі вразливості веб-сайту "Travel anywhere" та методи вирішення проблеми зі знайденими вразливостями. Для цього необхідно розв’язати такі задачі: проаналізувати методи створення безпечних веб-додатків, які будуть стійкими до різних атак; проаналізувати можливі атаки на сайти можливості їх усунення; проаналізувавши вразливості сайту "Travel anywhere" надати варіанти усунення цих вразливостей.

**Об'єкт дослідження –** веб-додатки, інформаційний веб-сайт "Travel anywhere".

**Предмет дослідження –** вразливості веб-додатків, інформаційні загрози та атаки на веб-ресурси.

**Методи дослідження –** сукупність теоретичних та практичних методів для реалізації захищеного інформаційного веб-додатку.

***Наукова новизна роботи:*** Визначення критеріїв безпечного сайту, вибір методів усунення вразливостей до різного роду атак на веб-додаток "Travel anywhere".

***Практичне значення*** Отримано нову інформаційну веб-систему для подорожей, яка представляє собою зручну та інтуїтивно зрозумілу веб-систему, та захищену до різних видів атак.

***Апробація результатів дипломної роботи.*** Основні положення дослідження доповідалися й обговорювалися на науково-практичній конференції: VІ Науково-технічна конференція "Інформаційні моделі, системи та технології" (12-13 грудня 2018 року).

***Публікації.*** За результатами дослідження опубліковано 1 публікація загальним обсягом 1 др. арк.

***Структура роботи.*** Дипломна робота складається з вступу, 6-ти розділів, висновків, основного тексту, а також таблиць і рисунків, списку використаних джерел і додатків.

**ОСНОВНИЙ ЗМІСТ РОБОТИ**

У **вступі** розкривається сутність та стан наукової проблеми, її значимість; обґрунтовано необхідність проведення дослідження, його актуальність;сформульовано мету і задачі дослідження , наукову новизну та практичне значення отриманих результатів.

В **першому розділі** «Створення веб-додатків» було розглянуто предметну область, проаналізовано стан використання інформаційних технологій у сфері веб розробки. Досліджено різні методи впровадження інформаційних технологій в сферу веб-програмування. Було проаналізовано існуючі методи написання сайтів. Також проведено опис мов програмування які використовуються для створення веб-додатків.

В **другому розділі** «Вразливості веб-додатків на основі методології OWASP» було визначено критерії інформаційної вразливості веб-додатків, їх опис та деякі загальні рекомендації для безпечного програмування.

В **третьому розділі** «Вразливості веб-сайту "Travel anywhere" та методи їх усунення» було обрано мову програмування, фреймворк для розробки, СУБД та програмну основу та показано доцільність їх використання для створення захищеного інформаційного сайту. Було проаналізовано вразливості веб-сайту "Travel anywhere" та надано варіанти і способи їх усунення.

У **четвертому розділі** «Спеціальна частина» обґрунтовуюється вибір Zend Framework для безпечної розробки веб-сайту та описано його переваги.

У **п'ятому розділі** «Обґрунтування економічної ефективності» проведено розрахунки техніко-економічної ефективності проведення розробки безпечного веб-додатку.

У **шостому розділі** «Охорона праці та безпека в надзвичайних ситуаціях» наведено результати аналізу умов праці відповідно до нормативно-правових актів, а також забезпечення дотримання вимог законодавства щодо прав працівників у галузі охорони праці та безпеки в надзвичайних ситуаціях.

Розділ безпека в надзвичайних ситуаціях пояснює планування заходів цивільного захисту на об’єкті у випадку надзвичайних ситуацій. Також описано вплив виробничого середовища на працездатність та здоров’я користувачів комп’ютерів яке враховано при проектуванні та розробці інформаційного веб-сайту.

У **сьомому розділі** «Екологія» розглянуто соціологічні проблеми урбанізації та охорони здоров’я, їх наслідки та методи усунення. Також описано системи екологічної інформації та їх використання.

**ВИСНОВКИ**

У результаті виконання дипломної роботи було проаналізовано та досліджено перспективи та раціональність використання інформаційних та веб-технологій у веб-програмування, а також розроблено інформаційний сайт для подорожей, стійкий до різного виду атак. Веб-систему виконано згідно всіх поставлених вимог.

Зроблено аналітичний огляд стану використання інформаційних та веб-технологій у веб-програмування та проблеми їх впровадження. Проаналізовано існуючі способи написання сайтів. Обґрунтовано вибір технології для реалізації веб-системи, проаналізовано засоби реалізації баз даних у веб-технологіях, а також обрано середовище та засоби розробки.

Спроектовано базу даних для інформаційного сайту, а також структуру головної та користувацької частин веб-сайту, спроектовано поведінку та інформаційні сутності.

Реалізовано метод завантаження даних авторизованого користувача в системі. Спроектовано та розроблено інтерфейс веб-системи з усіма необхідними формами.

Для перевірки правильності функціонування інформаційної веб-системи, здійснено верифікацію коду та тестування веб-сайту на кросбраузерність та кросплатформеність.

**СПИСОК ОПУБЛІКОВАНИХ РОБІТ ЗА ТЕМОЮ ДИПЛОМНОЇ РОБОТИ**

1. С.Р. Вишковський. Дослідження вразливостей інформаційних веб-сайтів та методів їх усунення / Тези доповіді VІ Науково-технічна конференція "Інформаційні моделі, системи та технології", 12-13 грудня 2018 року. – Том ІІ. – Тернопіль, 2018. – С. 62-63.

**АНОТАЦІЯ**

***Вишковський С. Дослідження вразливостей інформаційного веб-сайту "Travel anywhere" та методів їх усунення – Рукопис.***

У дипломній роботі проведено аналіз стану використання інформаційних та веб-технологій у сфері кібербезпеки та безпечного програмування, було розроблено інформаційний веб-сайт "Travel anywhere*"*.

Розглянуто предметну область, проаналізовано стан використання інформаційних технологій у веб-програмуванні. Досліджено можливі загрози та атаки на інфомарцію в сфері інтернет застосунків. Було проаналізовано існуючі аналоги вирішення проблем та доведено доцільність використання фреймворків при розробці безпечних сайтів.

Визначено критерії інформаційної веб-системи, її основну мету та функції. Обрано мову програмування, СУБД та програмну основу та показано доцільність їх використання для створення інформаційного сайту. Наведено життєвий цикл інформаційної веб-системи та обґрунтовано вибір середовища розробки. Було проаналізовано засоби реалізації баз даних у веб-технологіях та спроектовано базу даних для веб-сайту, а також наведено кроки для забезпечення безпеки передачі даних.

Реалізовано захист від різного роду атак на інформацію. Розроблено модуль блогу для інформаційного сайту. Також було наведено реалізацію інтерфейсу з обґрунтуванням вибору кольорової гами, шрифтів та структури шаблону і систему розподіленого доступу для захищеності веб-сайту.

Ключові поняття: СУБД, ІНФОРМАЦІЙНИЙ РЕСУРС, ІНФОРМАЦІЙНА СИСТЕМА, ВЕБ-ТЕХНОЛОГІЇ, JAVASCRIPT, HTML, MYSQL, JSON, PHP, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЯ

**ANNOTATION**

***Vyshkovskyi S. Investigation of vulnerabilities of information website "Travel anywhere" and methods of their elimination - Manuscript.***

In the thesis the analysis of the state of use of information and web technologies in the field of cybersecurity and safe programming was conducted, and an information website "Travel anywhere" was developed.

The subject area is considered, the state of use of information technologies in web programming is analyzed. The possible threats and attacks on information technologies in the field of Internet applications have been investigated. The existing analogs of the problem solving were analyzed and the expediency of using the frameworks in the development of secure sites was proved.

The criteria of the information web system, its main purpose and functions are determined. The language of programming, the DBMS and the software basis is chosen and the expediency of their use for the creation of the information site is shown. The life cycle of an informational web system is presented and the choice of development environment is justified. It analyzed the means of implementing databases in web technologies, and designed a database for the website, as well as steps to ensure the security of data transmission.

Implemented protection against all kinds of attacks on information. Developed blog module for information site. An implementation of the interface with the justification of the choice of color gamut, fonts and template structure and the distributed access system for the protection of the website was also presented.

Keywords: DBMS, INFORMATION RESOURCE, INFORMATION SYSTEM, WEB TECHNOLOGIES, JAVASCRIPT, HTML, MYSQL, JSON, PHP, CYBER SECURITY, INFORMATION