ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

ТРИГУБЕЦЬ Богдан Іванович

Розробка CMS та методів захисту web-сайтів на її основі

Спеціальність 125 «Кібербезпека»

Автореферат

дипломної роботи на здобуття освітньо-кваліфікаційного рівня «магістр»

Тернопіль — 2019

Дипломною роботою є рукопис.

Роботу виконано у Тернопільському національному технічному університеті імені Івана Пулюя.

Науковий керівник: доктор технічних наук
Марценюк Василь Петрович,
Тернопільський національний технічний університет імені Івана Пулюя, кафедра кібербезпеки, доцент.

Рецензент: д.к.н., професор
Кунанець Наталія Едуардівна,
Тернопільський національний технічний університет імені Івана Пулюя, кафедра комп'ютерних наук, доцент.

Захист відбудеться 24 грудня 2019 р. о 9 год. на засіданні Державної екзаменаційної комісії у Тернопільському національному технічному університеті імені Івана Пулюя за адресою:
46001, м. Тернопіль, вул. Руська, 56.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. У сучасному технологічному світі web-сервіси стали невід'ємною частоною життя багатьох людей та інструментом для вирішення багатьох повсякденних проблем, а поняття безпеки відіграє одну з передових ролей у сучасному інформаційному просторі вцілому. Саме тому аналіз існуючих інструментів для спрощення взаємодії користувача з інтернет-магазинами, розробка на їх основі власної CMS, а також аналіз основних загроз роботи web-сайтів, та їх врахування при розробці захищеної CMS, є актуальним.

Мета і завдання дослідження. Метою магістерської роботи є дослідження існуючих інструментів для спрощення взаємодії користувача з інтернет-магазинами та для спрощення взаємодії інтернет-магазинів з службами доставки, розробка на їх основі власної CMS для українського ринку, а також аналіз основних загроз роботи web-сайтів, та їх врахування при розробці захищеної CMS та web-сайтів на її основі. Мета дослідження обумовила поставлення та розв'язання наступних завдань:

- проаналізувати популярні CMS для інтернет-магазинів;
- дослідити функції, інтеграція яких спростить взаємодію користувача з інтернет-магазином, та спростить взаємодію менеджерів з службами доставки при відправці замовлень;
- проаналізувати популярні вразливості та атаки на web-сайти;
- дослідити методи захисту CMS від можливих атак;
- обґрунтувати використання вибраних технологій;
- розробити сучасну та захищену CMS для інтернет-магазину.

Об'єктом дослідження є функціонал та система захисту CMS.

Предметом дослідження є моделі, структури та методи створення CMS.

Методи дослідження. В процесі цього дослідження було використано такі загальнонаукові методи пізнання як порівняння, системний аналіз, моделювання та метод пошуку для визначення функціоналу нової CMS та забезпечення інформаційної безпеки web-ресурсу.

Наукова новизна роботи: було розроблено нову захищену CMS для інтернет-магазинів з сучасними інтеграціями для роботи на українському ринку.

Практичне значення дослідження полягає у застосуванні розробленої CMS для захищеної роботи з інтернет-магазинами на українському ринку.

Апробація результатів дослідження. Основні положення та результати дослідження обговорювалися та були схвалені на VII науково-технічній конференції Тернопільського Національного Технічного Університету імені Івана Пулюя "Інформаційні моделі, системи та технології" (Тернопіль, 2019).

Структура роботи. Магістерська робота складається із вступу, 7-ми розділів, висновків, списку використаних джерел із 33 найменувань. Робота містить X рисунків. Обсяг основного тексту становить 88 сторінок, перелік використаних джерел 3 сторінки. Загальний обсяг дипломної роботи складає 91 сторінка.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність створення нової CMS для інтернет-магазинів, описано мету та завдання розробки.

У першому розділі — *С“творення web-сайтів та проблеми їх захисту” —* розповідається про роль сучасних web-сервісів у повсякденному житті, досліджуються підходи до створення web-сайтів, варіанти власної розробки та розробки з використанням готової CMS, визначення чітких завдань, які має вирішувати розроблений сервіс.

При мінімальному функціоналі зазвичай немає неохідності вдаватися до послуг web-розробників, так як на ринку існує багато спеціальних сервісів, які пропонують готові CMS, що дають змогу звичайному користувачу, без навиків програмування та розробки, створити власний інтернет-блог чи сайт-візитку для онлайн-представлення власного бізнесу. Для таких цілей це найкращий варіант, адже він не вимагає багато фінансових та часових затрат, та дозволяє швидко розробити необхідний функціонал, використовуючи вже готові сторонні розробки.

Проте якщо задачі, які були поставленні перед розробником, вимагають креативних та унікальних рішень, які на даний момент не представлені на ринку, або вимагають внесення суттєвих коректівів у існуючі рішення, найкращим варіантом буде розробка власної CMS-платформи. Це дозволить максимально гнучко налаштувати web-сайт, врахувавши найдетальніші побажання як у дизайні, так і в нюансах функціоналу. Тому для створення якісного сервісу та для вирішення поставлених завдань на найкращому рівні web-сайт має використовувати лише найтехнологічніші інструменти, розробку яких найоптимальніше здійснювати на платформі власної розробки.

Розглянувши популярні CMS та роблячи акцент на функціях для максимальної зручності перегляду та замовлення товару для користувача, максимальної зручності обробки замовлення менеджерами інтернет-магазину та його передачі для відправки у поштову службу, було виявлено, що ніодна з представлених на українському ринку CMS не містить інтеграції усіх доступних на ринку функцій для оптимізації роботи інтернет-магазину, тому для їх повноцінної інтеграції необхідно використовувати власну розробку.

Далі було розглянуто найпопулярніші атаки на сервер та на програмну частину web-сайту, та було описано наступні атаки:

- DDoS-атака, повна назва якої distributed denial-of-service (розподілена атака на відмову в обслуговуванні), суть якої полягає у направленні величезної кількості запитів на певний сервер, кількість яких перевищує його пропускну здатність, в результаті чого від перенавантаження сервер перестає відповідати на запити реальних користувачів.
- атаки через FTP (File Transfer Protocol) — протокол передачі файлів, який використовують для обміну файлами з сервером. Найчастіше причиною успішного несанкціонованого доступу до web-сайту через атаку на FTP є наявність на комп’ютері користувача, який завантажує чи оновлює файли через цей протокол, вірусів, та через відсутність протоколу прикладного рівня SSH для шифрування данних;
- вразливість через відсутність SSL-сертифікату для HTTP (Hypertext Transfer Protocol), без якого дані також не шифруються, і тому вони не є захищеними. Використання незахищеного протоколу HTTP несе велику кількість небезпек і вразливостей, проте він все ще займає вагоме місце в мережі інтернет.

- SQL-ін’єкції — це атаки через запити до бази даних, які дозволяють зловмиснику виконати певні дії у структурі запиту, які не планувалася розробником.
- атака Cross Site Scripting (XSS), в основі якої лежить вразливість програмного коду, яка дозволяє зловмиснику додавати власні скрипти на сторінки сайту, які генеруються сервером.
- атака через недостатню аутентифікацію, спрямована на отримання доступу до функцій адмін-панелі сайту від імені адміністратора (або іншого користувача, який наділений великою кількістю прав). Суть цієї атаки полягає у використанні методів, які підміняють ідентифікатори користувача.
- атака через недостатню авторизацію, суть якої полягає в тому, що деякі CMS не мають розмежування прав доступу до певних розділів та функцій адмін-панелі між різними користувачами. Тобто, сервіс надає однакові права на внесення змін в фукціонал та контент сайту як для головного адміністратора, так і для звичайного редактора.
- проблема наявності готових стандартизованих методів атаки для популярних CMS, наявність автоматизованих рішень для brute-force-атак, вразливість через використання стандартних логінів та паролів, загальновідомі адреси адмін-панелі — все це робить ймовірність легкого підбору методів атаки дуже високою.

У другому розділі — *“Розробка CMS та методів захисту web-сайту”* — було визначено вимоги до функціоналу нової CMS та методів її захисту. Основна задача — розробити зручну платформу для інтернет-магазину, яка б максимально використовувала існуючі технології та можливості інтеграції для виконання поставлених задач в реаліях місцевого українського ринку, а також давала можливість подальшого розширення функціоналу web-сайту без суттєвих труднощів.

З огляду на поставлені задачі, нова CMS для інтернет-магазину має містити наступні базові функції для максимально зручної ергономіки:

- можливість групування товарів по розміру та перелінкування схожих товарів;
- можливість фільтрації товарів у розділі по багатьом параметрам;
- скрізний пошук по товарам на сайті (з використанням суміжних назв товарів, які не в казані в назві товару, як ключових слів);
- можливість встановлення знижок на товари;
- можливість групування товарів з різних категорії у одну колекцію;
- інтеграція з українськими поштовими операторами;
- можливість як кур’єрської доставки, так і отримання на відділенні;
- інтеграція з зручною українською платіжною системою;
- можливість вибору накладеного платежу для оплати при отриманні;
- аналіз доданих у корзину товарів та пропонування суміжних до них товарів у корзині;
- СМС та email-сповіщення про статус замовлення;
- автоматизація генерування накладних товару для поштового оператора;
- можливість відслідковування поточного статусу відправлення користувачем під час перегляду свого замовлення;

Наявність усіх вищеописаних функцій у початковій версії інтернет-магазину, та можливість швидкого додавання нового функціоналу, дозволить продуктам, розробленим на основі H83 CMS, бути конкурентоспроможними на українському ринку у порівнянні з іншими CMS для інтернет-магазинів.

Під час розробки було проведено інтеграцію з API Укрпошти, за допомогою якого було розроблено модуль доповнення адреси та відділення доставки для спрощення взаємлдії користувача з сайтом та запобігання введення неправильних адрес, структуризовано вхідні дані про адресу отримання для автоматичної генерації накладних поштового відправлення та розроблено модуль відслідковування поточного статусу замовлення та модуль замовлень для менеджерів магазину у адмін-панелі.

Для створення особистого профілю на сайті було проведено інтеграцію з соціальною мережею Facebook, для зручного проведення оплати було інтегровано через API найпопулярнішу в Україні платіжну систему LiqPay. Для інформування клієнтів про створення/оплату/відправку замовлення було обрано класичний метод надсилання email-листів на електронну скриньку через SendGrid API, та відправку СМС-повідомлень через API SMSC.ua та push-сповіщень через API OneSignal.

Аналізуючи популярні загрози для web-сайту, проаналізовані у першому розділі, було використано наступні рішення:

- налаштовано CDN та фільтрування вхідного трафіку через сервіс Cloudflare;
- проаналізовано усі переваги використання SSH-ключа замість паролю;
- проаналізовано переваги використання нових стандартів транспортного мережевого протоколу HTTP/3 та QUIC;
- обґрунтовано переваги використання HTTPS, який є безпечною версією протоколу HTTP, так як використовує TLS (або SSL) для шифрування HTTP-запитів та HTTP-відповідей;
- обґрунтовано використання Kernel-based Virtual Machine (KVM);
- досліджено правильне налаштування .htaccess та .htpasswd, які допомагають ліквідувати вразливості доступу до файлів на web-сервері;
- досліджено правила безпечного програмування та перевірки вхідних данних, використовуючи як стандартні функції, так і сторонні бібліотеки для захисту;
- проаналізовано тенденції розвитку безпеки використання файлів Cookie, та нововведення 76-ої версії браузеру Google Chrome з підтримкою атрибуту SameSite. Атрибут SameSite дає змогу визначити можливість передачі Cookie під час отримання запиту зі стороннього ресурсу;
- інтегровано використання двохфакторної аутентифікації з використанням мобільного додатку Google Authenticator;
- проаналізовано необхідність розмежування прав доступу користувачів до функцій адмін-панелі;
- проаналізовано переваги використання власної розробки над популярними рішеннями, оскільки власна розробка дозволяє інтегровувати будь-який складний функціонал, та сторонні сервіси, які не представлені у вигляді додаткових модулів для існуючих CMS, що надає суттєві переваги при розробці нестандартних рішень, та з точки зору безпеки не пропонує готових рішень для реалізації популярних атак, які з легкістю можна знайти у мережі

під більшість популярних CMS. Необхідність персоналізованої розробки для атаки на CMS власної розробки суттєво збільшує вартість цих атак.

У третьом розділі — *Р“обота CMS”* — було показано механізм роботи деяких розділів та функції нової CMS. Було проілюстровано роботу модуля авторизації, показано механізм роботи другого фактору аутентифікації, генерації юзер-токенів та сервер-токенів, показано розділи для створення нових публікацій, каталог товарів, розділ замовлень та журнал подій, а також показано інтеграцію логування з використанням сервісу LogDNA та модуль аналізу наявності прав користувача при доступу до кожного з розділів.

У четвертому розділі — *“ Тестування атак на web-сайт”* — було вибрано середовище для тестування — Kali Linux. Web-сайт на основі CMS було протестовано на вразливість через SQL-ін’єкції за допомогою утиліти sqlmap, перевірено на вразливості типу XSS за допомогою утиліти XSSer, та за допомогою утиліти hydra було проведено brute-force атаку на SSH для суперкористувача root. Усі ці атаки були невдалими, що ще раз підтвердило правильність вибору методів захисту.

У п’ятому розділі — *“ Обґрунтування економічної ефективності”* — було проведено розрахунок норм часу на виконання науково-досліної роботи, визначено витрати на оплату праці на відрахування на соціальні заходи, проведено розрахунок матеріальних витрат, визначено термін окупності та обґрунтовано економічну ефективність.

У шостому розділі — *“ Охорона праці та безпека в надзвичайних ситуаціях”* — було описано, що проведені дослідження та розробка програмного забезпечення відбувалась з дотриманням основних правил користування комп’ютерною технікою, а працівники підприємств, де буде проводитися використання розробленої CMS для інтернет-магазину володіють знаннями з техніки безпеки, електробезпеки та пожежної безпеки, та проаналізовано загальні фактори ризику та можливі порушення здоров'я користувачів комп'ютерної мережі.

У сьомому розділі — *“ Екологія”* — було описано організаційні форми, види і способи статистичного спостереження в екології, джерела електромагнітних полів, іонізуючих випромінювань та методи їх знешкодження.

ВИСНОВКИ

У сучасному технологічному світі вдосконалення web-сервісів та створення нових програмних рішень забезпечує розвиток галузі вцілому, а дослідження актуальних вразливостей web-сайтів допомагає забезпечити їх стабільну та безпечну роботу.

У ході магістерської роботи було досліджено популярні CMS для роботи інтернет-магазинів на українському ринку, досліджено їх недоліки та напрямки, розглянуто найбільш актуальні для вдосконалення функції. Було досліджено та обрано ті функції, інтеграція яких спростить як взаємодію користувача з інтернет-магазином, так і взаємодію інтернет-магазину з службами доставки. Для модулю замовлень було розроблено інтеграцію з поштовим оператором Укрпошта за допомогою API. Було розроблено автодоповнення адреси отримувача у корзині,

автоматизовано генерацію накладних та розроблено сторінку відслідковування поточного статусу відправлення. Для спрощення реєстрації було використано API Facebook, для модулю оплати було обрано платіжну систему LiqPay, для E-mail та СМС сповіщень сервіси SendGrid та SMSC.ua відповідно, API OneSignal для сповіщень користувачів у браузері та API Telegram для сповіщення про нові замовлення для менеджерів проекту.

Було проаналізовано популярні вразливості web-сайтів та атаки на них, такі як DDoS-атаки, атаки через FTP/SSH, перехоплення даних при відсутності шифрування за допомогою SSL-сертифікату, від SQL-ін'єкції, XSS-атаки, а також атаки через недостатню авторизацію та аутентифікацію, та запропоновано методи захисту від них. Після їх інтеграції було проведено тестування, яке показало, що web-сайт захищений від даних типів атак.

В результаті даної роботи було розроблено сучасну та захищену CMS для інтернет-магазину, яка є зручною та конкурентноспроможною на українському ринку.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Розробка CMS та методів захисту web-сайтів на її основі [Текст] / Збірник тез VII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» – Тернопіль (11-12 грудня 2019 року), ТНТУ, 2019. – с. 104.

АНОТАЦІЇ

Тригубець Б.І. Метою роботи є дослідження існуючих інструментів для спрощення взаємодії користувача з інтернет-магазинами та для спрощення взаємодії інтернет-магазинів з службами доставки, розробка на їх основі власної CMS для українського ринку, а також аналіз основних загроз роботи web-сайтів, та їх врахування при розробці захищеної CMS та web-сайтів на її основі.

В даній роботі було здійснено розробку нової захищеної CMS для інтернет-магазину, яка є зручною та конкурентноспроможною на українському ринку.

Ключові слова: CMS, web-сайт, інтернет-магазин, захист web-сайтів, методи захисту, Укрпошта API, LiqPay API, SendGrid API, OneSignal API.

Tryhubets B.I. The aim of the work is to research existing tools to facilitate user interaction with online stores and to facilitate interaction of online stores with delivery services, to develop new CMS for the Ukrainian market, as well as to analyze the main threats to the operation of websites, and their consideration in the development secure CMS and websites based on it.

As result of this work, we developed a new secure CMS for online-shopping, which is convenient and competitive in the Ukrainian market.

Keywords: CMS, website, online-store, online-shopping, website security, security methods, Ukrposhta API, LiqPay API, SendGrid API, OneSignal API.