НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ФУНКЦІОНУВАННЯ ІНТЕРНЕТ МАГАЗИНІВ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Варганов Павло Олексійович

Керівник: д.е.н., професор
Горбаченко Станіслав Анатолійович

Рецензент: к.т.н., доцент
Кухаренко Сергій Вікторович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____» _____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Варганову Павлу Олексійовичу

1. Тема роботи: «Забезпечення кіберзахисту функціонування інтернет магазинів»
Керівник роботи: д.е.н., професор Станіслав Анатолійович Горбаченко
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 рік
3. Дата видачі завдання «15» вересня 2023 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Узгодження теми з науковим керівником	29.11.2023	виконано
2	Пошук та аналіз технічної інформації про інтернет-магазини	15.12.2023-28.12.2023	виконано
3	Поглиблений аналіз сучасних загроз	14.01.2024	виконано
4	Вибір практик та стандартів з кіберзахисту	25.01.2024-13.02.2024	виконано
5	Аналіз інтернет магазину	18.02.2024-02.03.2024	виконано
6	Виявлення вразливостей та недоліків	05.03.2024-27.03.2024	виконано
7	Розробка функціональної структури системи	06.04.2024-22.04.2024	виконано

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему “Забезпечення кіберзахисту функціонування інтернет магазинів” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 5 рисунків, 2 додатки, 21 літературних джерел за переліком посилань. Робота виконана на 49 сторінках загального тексту і 38 сторінках основного тексту.

Метою роботи є провести оцінку рівня кіберзахисту інтернет-магазину «SportShop» та розробити рекомендації щодо його підвищення

У роботі розглянуто теоретичні основи проведення захисту інтернет-магазинів, аналізує найбільш поширені види загроз та вразливостей, які використовуються зловмисниками. Також наведено приклади реальних інцидентів, що свідчить про актуальність теми.

Результати роботи можуть бути використані:

– При створенні комп’ютерних систем управління ризиками для інших онлайн-комерційних проєктів;

– При розробці комплексних програм оптимізації кібербезпеки електронної торгівлі, включаючи сучасні алгоритми захисту;

– Для розробки наукових досліджень з проблем кіберзахисту електронної комерції.

Можливими напрямками подальших досліджень є:

– Дослідження моделей захисту електронної комерції у різних країнах та розробка уніфікованих стандартів;

– Аналіз ефективності застосування хмарних послуг, ДВС та хакінгу-як-сервісу для захисту електронної комерції.

ЗАХИСТ, СИСТЕМА, КОМПОНЕНТ, АНАЛІЗ, ВРАЗЛИВІСТЬ, ЗАГРОЗА.

ABSTRACT

Qualification work on the topic "Ensuring cyber protection of the functioning of online stores" for obtaining the first (bachelor’s) level of higher education in the specialty 125 Cybersecurity, educational program: Cyber security, contains 5 drawings, 2 appendixes , 21 literary sources according to the list of references.The work is completed on 49 pages of the general text and 38 pages of the main text.

The purpose of the work is to assess the level of cyber protection of the online store "SportShop" and develop recommendations for its improvement

The paper examines the theoretical foundations of protection of online stores, analyzes the most common types of threats and vulnerabilities used by attackers. Examples of real incidents are also given, which indicates the relevance of the topic.

The results of the work can be used:

– When creating computer risk management systems for other online commercial projects;

– When developing complex programs for optimizing cyber security of electronic commerce, including modern protection algorithms;

– To develop scientific studies on the problems of cyber protection of electronic commerce.

Possible areas of further research are:

– Study of e-commerce protection models in different countries and development of unified standards;

– Analysis of the effectiveness of using cloud services, ICE and hacking-as-a-service for e-commerce protection.

PROTECTION, SYSTEM, COMPONENT, ANALYSIS, VULNERABILITY, THREAT

ЗМІСТ

ВСТУП

Інформаційна безпека та кіберзахист є надзвичайно важливими для будь-яких онлайн-ресурсів, зокрема електронної комерції. Численні інциденти злому сайтів, витоку даних та фінансових шахрайств суттєво знижують довіру користувачів до цих сервісів.

Згідно досліджень компанії Cybersecurity Ventures, збитки від кіберзлочинності до 2025 року перевищать 6 трлн. доларів на рік. При цьому лише в Україні щорічні втрати від хакерських атак оцінюються в 250 млн. доларів.

Експерти відзначають, що найбільш уразливими для атак є саме інтернет-магазини. У них зосереджено великі обсяги конфіденційної інформації користувачів та платіжних даних.

Разом з тим, більшість онлайн-магазинів не приділяють належної уваги захисту своїх IT-систем та даних. Вони не виконують базові заходи кібергігієни, такі як регулярні оновлення, тестування на уразливості, контроль конфігурацій тощо.

Актуальність даної роботи полягає у комплексному дослідженні рівня кібербезпеки реального інтернет-магазину та розробці моделі його захисту, що дозволить:

- Виявити суттєві прогалини у захисті онлайн-торгівлі;
- Запропонувати практичні рішення для усунення недоліків;
- Сформувати рекомендації щодо удосконалення захисту інших онлайн-магазинів;
- Підвищити обізнаність з питань кібербезпеки бізнесу.

Та, на нашу думку, результати дослідження дозволять покращити рівень інформаційної безпеки онлайн-комерції в цілому.

Мета дослідження - провести оцінку рівня кіберзахисту інтернет-магазину «SportShop» та розробити рекомендації щодо його підвищення.

Для досягнення поставленої мети необхідно виконати такі завдання:

1. Провести технічне тестування системи кіберзахисту «SportShop» з використанням спеціалізованих утиліт.

2. Виявити існуючі недоліки та прогалини у захисті інформаційних ресурсів.

3. Проаналізувати рівень відповідності стандартам та кращим практикам кібербезпеки.

4. Розробити функціональну модель комплексної системи кіберзахисту.

5. Описати основні компоненти запропонованої моделі.

6. Сформулювати практичні рекомендації щодо вдосконалення захисту.

Об’єктом дослідження є система кіберзахисту інтернет-магазину «SportShop».

Предметом дослідження є оцінка рівня захищеності та розробка моделі вдосконалення інформаційної безпеки онлайн-торгівлі на прикладі «SportShop».

Практичне значення отриманих результатів.

Результати проведеного дослідження мають вагоме практичне значення, тому-що:

1. На основі виявлених недоліків можна розробити конкретний план заходів щодо усунення прогалин та модернізації існуючих засобів захисту, що дозволить підвищити рівень довіри користувачів до онлайн-торгівлі.

2. Сформульовані рекомендації щодо підвищення рівня безпеки допоможуть іншим онлайн-магазинам оцінити стан своїх систем та своєчасно вжити заходів щодо можливих прогалин. Це зменшить ризики злому даних для електронної комерції в цілому.

3. Отримані результати можуть бути корисні для фахівців із кібербезпеки, які надають послуги аудиту та консалтингу. Дослідження показало поширені проблеми, на які необхідно звертати увагу під час тестування безпеки онлайн-магазинів.

1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРЗАХИСТУ ІНТЕРНЕТ-МАГАЗИНІВ

1.1 Огляд теоретичних підходів до кіберзахисту інтернет-магазинів.

Одним з перших і найбільш фундаментальних підходів є концепція захищеності (security). Вона полягає в створенні технічних, організаційних та правових заходів для забезпечення конфіденційності, цілісності та доступності інформаційних системи інтернет-магазину. До технічних заходів належить установка firewall, антивірусного та антиспамного ПЗ, шифрування даних, систем резервування даних тощо [9].

Організаційні заходи передбачають розробку політики інформаційної безпеки, протоколів доступу, політики паролів, призначення адміністратора безпеки та здійснення ним аудиту. До правових заходів належить розробка договорів із постачальниками послуг, договорів із клієнтами про конфіденційність персональних даних, а також законодавче регулювання питань кібербезпеки.

Другий підхід - концепція ризику, яка полягає у проведенні оцінки ризиків кібератак на інтернет-магазин та визначенні пріоритетів захисту відповідно до рівня ризику. Для цього проводиться аналіз загроз (виділяються можливі загрози), аналіз вразливостей (виявляються слабкі місця в системі), оцінюється міра впливу загроз (наслідки реалізації загроз) та ймовірність їх реалізації [5].

На основі цього присвоюються показники ризику (високий, середній, низький) тим чи іншим активам та процесам інтернет-магазину. Потім пріоритетним чином захищаються найбільш уразливі елементи з високим ризиком.

Третій підхід - це концепція невразливості, яка передбачає мінімізацію вразливостей системи до мінімуму [9]. Для цього використовують принципи «за замовчуванням», коли всі неавторизовані дії та доступи блокуються, принцип «менш прав», коли користувачам та програмам надається мінімальний рівень прав доступу.

Також розробляються системи аутентифікації, захищені комунікації, системи виявлення й реагування на інциденти, плани відновлення даних після атак. Використовуються методи криптографічного захисту даних, архітектури

«нульового довір’я», сегментації мереж та ізоляції.

Четвертий підхід - концепція постійного моніторингу та відстеження подій. Вона передбачає застосування систем виявлення вторгнень, аналізу логів, систем спостереження за мережею для оперативного реагування на інциденти. Для цього створюються SIEM-системи (Security Information and Event Management), в яких збирається логі перетину меж сегментів, доступів до ресурсів, подій в системах безпеки.

Це дозволяє виявляти підозрілу активність, аналізувати її та вживати заходів реагування [11]. Важливим є поєднання цього підходу з попередніми - ризик-орієнтованим підходом і концепцією невразливості. Це дозволяє максимально зменшити кількість уразливостей та ризиків, а також швидко виявляти та усувати інциденти.

Тому, для ефективного кіберзахисту інтернет-магазину необхідно комплексно застосовувати всі чотири описані теоретичні підходи: забезпечити захищеність на рівні технічних, організаційних та правових заходів; провести оцінку ризиків і пріоритизацію захисту; мінімізувати кількість уразливостей; здійснювати постійний моніторинг та відстеження подій в системі, що дозволить створити ефективну систему кіберзахисту інтернет-магазину.

1.2 Аналіз сучасних загроз та вразливостей інтернет-магазинів.

Сучасні інтернет-магазини стикаються з рядом значних загроз, які можуть серйозно підірвати їхню діяльність і навіть завдати значних збитків. Нижче розглянемо деякі з найбільш поширених загроз з детальним описом кожної з них:

1. Аутентифікація (Authentication):

Аутентифікація використовує принаймні один з трьох механізмів (факторів): «щось, що ми маємо», «щось, що ми знаємо» або «щось, що ми є». Розглянемо атаки, спрямовані на обхід або експлуатацію вразливостей у механізмах реалізації аутентифікації веб-серверів.

- Підбір (Brute Force):

Підбір – це автоматизований процес проб і помилок, який використовується для того, щоб вгадати ім’я користувача, пароль, номер кредитної картки, ключ шифрування і т.д. Зловмисники використовують словники та пробують мільйони комбінацій символів для вгадування даних доступу. Якщо використовуються слабкі паролі, є ймовірність успішного підбору. Існує прямий та зворотний підбір. При прямому перевіряються різні паролі для одного логіна, при зворотному - різні логіни для одного пароля. Незважаючи на тривалість, підбір є популярною атакою для обходу аутентифікації.

- Недостатня аутентифікація (Insufficient Authentication):

Недостатня аутентифікація може виникнути коли веб-сайт дозволяє отримувати доступ до важливої інформації чи адміністрування без належної перевірки. Деякі ресурси приховують за спеціальними адресами, але це не є надійним захистом. URL все одно можна знайти шляхом перебору типових директорій, аналізу помилок чи документації. Важливі сторінки повинні мати обов’язкову аутентифікацію користувача залежно від рівня доступу та інформації. Приховування ресурсу не є адекватним захистом від недостатньої аутентифікації.

- Небезпечне відновлення паролів (Weak Password Recovery Validation):

Небезпечна функція відновлення паролів дозволяє зловмисникам несанкціоновано отримувати доступ до чужих облікових записів. Користувачі часто не пам’ятають паролі від багатьох сайтів. Для відновлення використовують секретні питання, підказки чи персональні дані. Зловмисник може відгадати або відстежити ці дані. Після ідентифікації користувача отримує новий пароль. Цей механізм не забезпечує надійну перевірку особи і дозволяє зловмисникам обходити аутентифікацію для доступу до чужих акаунтів. Необхідно застосовувати більш жорсткі процедури відновлення.

2. Авторизація (Authorization):

Багато сайтів обмежують доступ до певного вмісту чи функцій тільки певним користувачам. Зловмисники можуть здійснювати атаки для обходу таких обмежень і отримання несанкціонованого доступу. Вони використовують різні техніки для підвищення своїх привілеїв і доступу до захищених ресурсів, до яких в них немає

прав. Такі атаки спрямовані на вразливості у методах, якими сайти визначають чи має користувач дозвіл на певні дії. Мета - обійти обмеження доступу та отримати привілеї, недоступні зловмиснику.

- Передбачуване значення ідентифікатора сесії (Credential/Session Prediction):

Передбачуване значення ідентифікатора сесії дозволяє зловмисникам перехоплювати сесії інших користувачів шляхом вгадування унікального ID сесії. Після первинної аутентифікації, сервер генерує ID сесії замість повторної передачі логіна та паролю. Якщо хакер здогадається цей унікальний ідентифікатор, він зможе посилати запити від імені іншого користувача, отримавши доступ до його акаунту. Ця атака дозволяє перехопити чужу сесію шляхом вгадування її ідентифікатора.

- Недостатня авторизація (Insufficient Authorization):

Недостатня авторизація виникає, коли веб-сервер дозволяє атакуючому отримувати доступ до важливої інформації або функцій, який повинен бути обмежений. Аутентифікація не гарантує повного доступу до всіх функцій сервера, тому необхідно реалізувати розмежування доступу. Правила доступу повинні обмежувати дії користувача відповідно до політики безпеки, а доступ до важливих ресурсів сайту має бути дозволений тільки адміністраторам.

- Відсутність таймауту сесії (Insufficient Session Expiration):

Якщо сесія не завершується через деякий час бездіяльності, існує ризик використання старих данних для авторизації. Це може дозволити зловмиснику отримувати доступ до особистої інформації користувача або здійснювати шахрайські транзакції від його імені. Крім того, довгий таймаут сесії збільшує ймовірність вгадування ідентифікатора сесії, що полегшує нелегітимний доступ. Для захисту від таких інцидентів необхідно встановити оптимальний час життя сесії, після якого вона автоматично закривається.

- Фіксація сесії (Session Fixation):

Зловмисник може присвоїти користувачеві певне значення ідентифікатора сесії до входу останнього в систему. Це досягається за допомогою різних методів,

таких як міжсайтове виконання сценаріїв.

Існують два основних типи систем управління сесіями: «дозволяючі», які допускають визначення ідентифікатора браузером, та «суворі», де використовуються лише сервер-генеровані значення. «Дозволяючі» системи є вразливішими, оскільки дозволяють зловмиснику обрати будь-який ідентифікатор.

Після фіксації ідентифікатора зловмисник отримує доступ до системи під виглядом користувача. Більшість атак цілиться на значення cookie. Для захисту важливо використовувати «суворі» системи та перешкоджати фіксації сесій.

3. Атаки на клієнтів (Client-side Attacks):

При перегляді сторінок встановлюються довірчі відносини між користувачем та сервером, оскільки очікується отримання лише перевіреного контенту. Водночас люди не сподіваються на атаки з боку відвідуваного ресурсу. Скориставшись цією довірою, зловмисники можуть застосовувати різні методи атак на вразливості пристроїв користувачів. Розгялнемо їх:

- Підміна вмісту (Content Spoofing):

Деякі хакери вміло використовують особливості динамічних веб-сторінок, щоб підступно нашкодити користувачам. Вони можуть підмінити посилання на джерело даних HTML-коду, таким чином сховавши справжнє його походження. Коли жертва відкриє той сайт, у пам’яті браузера залишатиметься адреса легального ресурсу, а сторінка відобразить інформацію зовсім з іншого, злих намірів.

В цей спосіб зловмисник змусить користувача повірити, ніби він переглядає надійний сайт, у той час як насправді частину інформації було додано ззовні. Таким чином вони можуть обдурити людину і примусити розкрити особисті дані на підробленій сторінці [15].

Хакери часто використовують такі хитрощі, щоб захопити чужі облікові записи або поширювати шкідливі дані. Тому користувачам варто бути уважними і завжди перевіряти щирість тих сторінок, на які вони переходять в Інтернеті [19].

- Міжсайтове виконання сценаріїв (Cross-site Scripting, XSS):

Хакери можуть використовувати уразливість міжсайтового виконання

скриптів (XSS), щоб ввести користувачів в оману. Зловмисник може передати на сайт шкідливий JavaScript-код, який потім буде виконаний браузером жертви.

Це дає змогу читати чи модифікувати дані, доступні через браузер, або перенаправити на інші ресурси. Хакер таким чином отримує можливість використовувати акаунт користувача.

Існує два варіанти атаки: «непостійна», коли код передається в одному запиті, та «збережена», де він зберігається на сервері і діє тривалий час. Обидва методи дозволяють зловмиснику підступно отримати доступ до інформації чи провести інші злісні дії.

- Розщеплення HTTP-запиту (HTTP Response Splitting):

Зловмисник може скористатися вразливістю сервера, надіславши спеціально сформований запит [12]. У відповідь сервер виділить дві частини, другу з яких повністю контролює хакер.

Так він здатен ввести в оману проксі-сервер чи кеш браузера, підмінивши їх дані. Це дасть змогу:

- виконати JavaScript на стороні жертви;
- отримати куки користувача;
- перехопити сторінки з особистою інформацією.

4. Виконання коду (Command Execution):

Опишемо атаки, спрямовані на виконання коду на веб-сервері. Всі сервери використовують дані, віддані користувачем при обробці запитів. Часто ці дані використовуються при складанні команд, що застосовуються для генерації динамічного вмісту. Якщо при розробці не враховуються вимоги безпеки, зловмисник отримує можливість модифікувати виконавчі команди.

- Переповнення буфера (Buffer Overflow):

Переповнення буфера відбувається, коли об’єм вхідних даних перевищує розмір виділеної пам’яті.

У цьому випадку додаткові дані перезапишуть інші ділянки пам’яті, що може:

- викликати помилки та збої програми;

- дозволити змінювати шлях виконання коду;
- виконувати довільні команди в контексті процесу.

Особливо небезпечна ця уразливість для програм, написаних на C/C++. Якщо веб-сервер містить такі компоненти, він може стати мішенню для атаки.

Зловмисник здатенй провести переповнення буфера й дистанційно отримати повний контроль над системою. Тому цей клас помилок є критичною загрозою для безпеки.

- Атака на функції форматування рядків (Format String Attack):

При використанні цих методів атак програма модифікує шлях виконання шляхом перезапису областей пам’яті за допомогою функцій форматування символьних змінних. Уразливість виникає, коли дані користувача використовуються як аргументи функцій форматування рядків, таких як fprintf, printf, sprintf, setproctitle, syslog і інші. Якщо атакуючий передає додаткам рядок, що містить специфікатори форматування («%f», «%p», «%n» і т.д.), то він може:

- виконати довільний код на сервері;
- зчитати значення зі стеку;
- спричинити виникнення помилок у програмі або відмову в обслуговуванні.

- Впровадження операторів LDAP (LDAP Injection):

Атаки LDAP Injection спрямовані на веб-сервери, які взаємодіють з службою Lightweight Directory Access Protocol (LDAP) на основі введених користувачем даних. Цей протокол використовується для доступу до служб каталогів, таких як Active Directory в Windows, SQL Server, PL SQL в Oracle тощо. Багато веб-додатків використовують введені користувачем дані для створення динамічних веб-сторінок [13]. Якщо ці дані не перевіряються на вірність, зловмисник може модифікувати SQL-запит, який відправляється додатком до сервера баз даних. Цей запит виконується з тими ж привілеями, що й компонент програми, який виконує запит (наприклад, сервер баз даних або веб-сервер). В результаті атаки зловмисник може отримати повний контроль над сервером баз даних і навіть операційною системою.

- Впровадження серверних розширень (SSI Injection):

Одним із класів цієї атаки є виконання коду на сервері, яке дозволяє зловмиснику дистанційно запускати певні дії. Часто це пов’язано з відсутністю перевірки даних від користувача до їх обробки.

При генерації HTML сервер може використовувати сценарії отримані від користувача, наприклад Server-side Includes. Якщо зловмисник передасть такий сценарій, то зможе отримати доступ до ресурсів сервера чи вбудувати шкідливий код.

При обробці даних від користувача необхідно перевіряти їх на наявність сценаріїв чи інших заборонених дій. Інакше це створює ризики для безпеки системи та конфіденційності користувачів. Важливо ретельно фільтрувати вхідні дані перед їх обробкою [13].

- Впровадження операторів XPath (XPath Injection):

XPath використовується для пошуку елементів в XML-документах. Якщо параметри XPath-запитів формуються на основі даних від користувача, то зловмисник може модифікувати запит, щоб обійти перевірки чи отримати доступ до несанкціонованої інформації.

Наприклад, є XML з даними користувачів. За звичайних умов XPath дозволяє отримати рахунок конкретного користувача за його ім’ям та паролем. Однак якщо запит формується на підставі даних від користувача, зловмисник може додати оператори для отримання всіх рахунків або іншої інформації.

Тому необхідно перевіряти та фільтрувати параметри XPath перед його виконанням.

Усі ці загрози між собою пов’язані, оскільки мають спільну мету - отримати контроль над інтернет-магазином або доступ до конфіденційної інформації, яка в ньому зберігається. Хакери та зловмисники використовують різноманітні техніки та тактики для реалізації цієї мети - від нападів кіберзлочинців через вразливості в ПЗ або недосконале керування ризиками до шахрайства та соціальної інженерії. Більшість з уразливостей, проаналізованих вище, можуть бути використані зловмисниками для отримання доступу до конфіденційних даних клієнтів або

вантаження роботи інтернет-магазину. Тому дієве управління ризиками та захист інформації є основою для мінімізації наслідків цих загроз.

Реальні приклади:

У лютому 2018 року інтернет-магазин F.ua зіткнувся з незвичайним випадком шахрайства, яке було спрямоване на одержання незаконної вигоди шляхом використання репутації та бренду онлайн-торговельної платформи. Невідомий діяч, який мав доступ до бази електронних адрес реальних осіб, зареєстрував ці контакти на сайті інтернет-магазину F.ua. Проте замість пароля він вводив повідомлення рекламного характеру, яке містило посилання на спам-ресурс та пропозицію про нібито невикористаний грошовий бонус.

Така дія була спрямована на отримання незаконної вигоди, адже після реєстрації користувачі отримували листа з електронної пошти онлайн-магазину, який містив вказаний рекламний текст і посилання. Відповідно, шахрай міг отримати прибуток від кліків на це посилання або продажу персональних даних користувачів третім особам.

Для попередження подібних випадків керівництво F.ua прийняло систему заходів, зокрема обмеження кількості символів для пароля та заборону використання певних типів посилань.

Подібна ситуація трапилася і в інтернет-магазині MebelOk, про що розповіла його співзасновниця Оксана Донська. Водночас бувають випадки, коли проблеми створюють самі розробники онлайн-торговельних платформ через помилки або неуважність. Так, Дмитро Покотило звернув увагу на неправильну індексацію Google окремих сторінок сайтів, що не мають суттєвого SEO-змісту. А Оксана Донська пригадала випадок випадкового видалення всієї бази даних через дії адміністратора сервера, який вдалося усунути завдяки наявності резервної копії.

1.3 Огляд найкращих практик та стандартів з кіберзахисту для інтернет-магазинів.

В умовах зростання кількості кіберзлочинів і посилення загроз у сфері інформаційної безпеки обов’язковим є застосування ефективних заходів захисту в

онлайн-торгівлі [11]. Адже інтернет-магазини є привабливою мішенню для хакерів і шахраїв, оскільки у них зберігаються дані великої кількості користувачів.

Розглянемо найкращі практики:

1) Дотримання стандартів PCI DSS, розроблених Радою з платіжних карт для мінімізації ризиків крадіжки даних платіжних карток. Серед ключових принципів PCI DSS - інсталяція брандмауерів та системи DDoS-захисту, шифрування транзакцій і зберігання даних, періодичне проведення тестувань і перевірок, оновлення програмного забезпечення.

2) Дотримання стандартів OWASP, який містить рекомендації щодо захисту веб-додатків, аналізу вразливостей та аудиту безпеки. Зокрема, OWASP рекомендує вживати такі заходи:

- Шифрування даних користувачів і транзакцій на всіх етапах;

- Коректна настройка системи керування контентом та фільтрів ввідних даних;

- Перевірка наявності останніх оновлень в ПЗ та виправлення вразливостей;

- Регулярне проведення проникнення тестів і фонового моніторингу.

3) Дотримуватися загальних принципів кібергігієни: застосовувати багатофакторну автентифікацію; контролювати доступ користувачів та приставити облікові записи; періодично оновлювати ПЗ; захищати бази даних за допомогою SSL/TSL; здійснювати резервне копіювання; встановити систему моніторингу й логування.

4) Робота з персоналом - проводити тренінги щодо кібергігієни та гарантувати дотримання політики інформаційної безпеки всіма працівниками. Варто дотримуватися принципу мінімального доступу - надавати облікові записи з мінімальними правами лише необхідним особам.

Серед технічних заходів слід використовувати WAF-фільтри для захисту веб-додатків, DDoS-мітігатори, системи SIEM для моніторингу та виявлення потенційних інцидентів. Зручними є хмарні сервіси моніторингу та звітності на основі AI, що полегшують виявлення патернів та правильне реагування на загрози.

Окремим напрямком є регулярне тестування на проникнення, що дає змогу перевірити наявні слабкі місця та вразливості до кібератак [18]. При цьому потрібно запросити незалежних експертів, аби отримати об’єктивну оцінку ситуації та рекомендації щодо захисту.

Враховуючи постійну зміну загроз і методів атак, а також нові вимоги законодавства про захист персональних даних, вагомим є безперервне удосконалення системи інфобезпеки на основі проведених оцінок і перевірок, що допоможе нівелювати ризики для бізнесу, зберегти довіру клієнтів та уникнути значних фінансових втрат [20].

2 ДІАГНОСТИКА КІБЕРЗАХИСТУ ІНТЕРНЕТ-МАГАЗИНУ «SPORTSHOP»

2.1 Аналіз інтернет-магазину «Sportshop» на предмет кіберзахисту.

Для оцінки рівня кіберзахисту інтернет-магазину «Sportshop» було проведено технічне тестування його інфраструктури та веб-додатків.

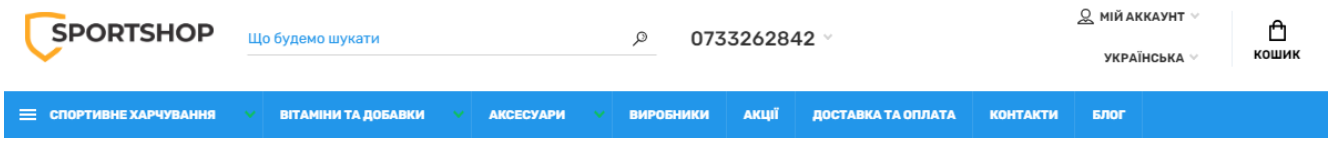

Рисунок 2.1 – Інтернет-магазин «Sportshop»

Тестування включало:

– Аналіз версій протоколів HTTPS та TLS, що використовуються. Перевірено відповідність сучасним стандартам безпеки;

– Сканування сайту за допомогою утиліт для отримання інформації про потенційні веб-вразливості;

– Інспекція відповідей HTTP-заголовків на предмет наявності необхідних захисних механізмів (CSP, HSTS, та ін.);

– Аналіз процесів аутентифікації та управління сесіями з метою виявлення евентуальних уразливостей;

– Перевірка захисту куків та налаштувань їх безпечного зберігання;

– Оцінка відповідності сучасним стандартам мобільної оптимізації.

Результати цих тестів дозволили найбільш об’єктивно оцінити поточний рівень захищеності сайту та виявити його слабкі місця.

Утилітами для сканування були:

– Nikto;

– ZAP (Zed Attack Proxy);

– Burp Suite.

Вибір саме цих трьох утиліт для проведення тестування інформаційної безпеки інтернет-магазину «Sportshop» був обґрунтований наступними факторами:

1. Nikto:

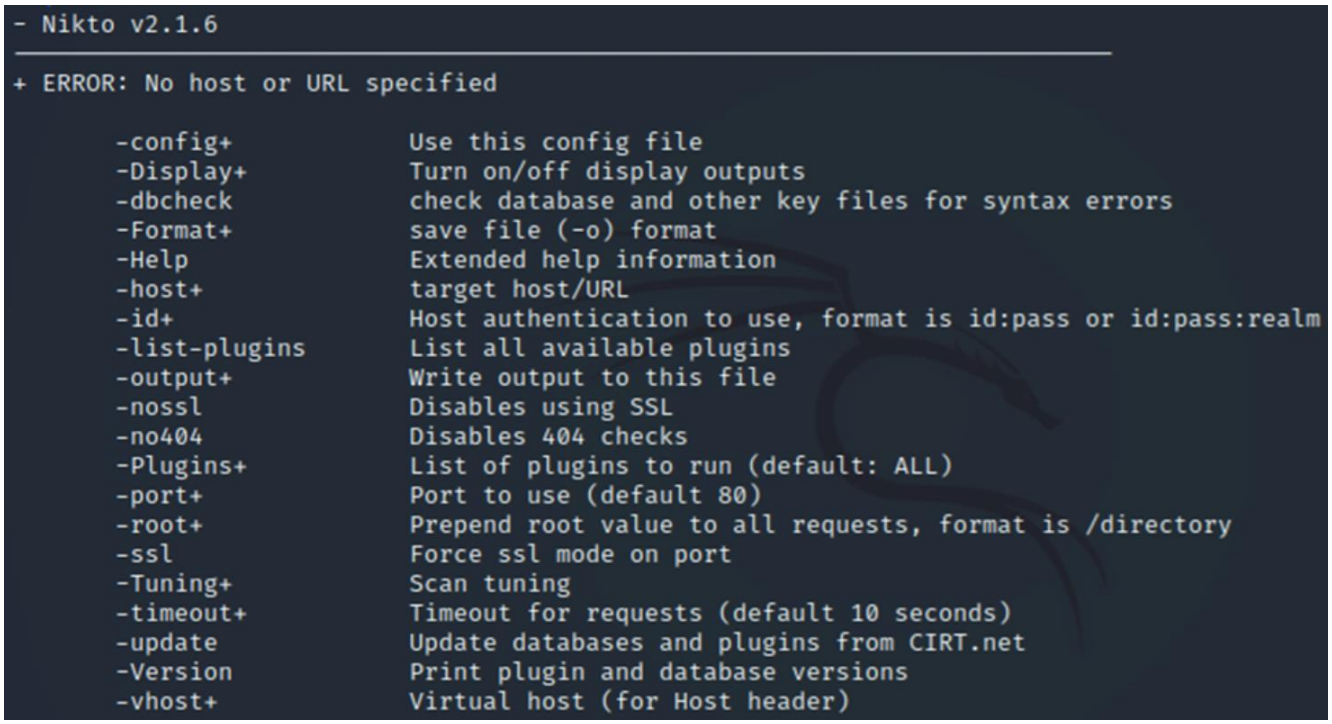

Рисунок 2.2 – Утиліта Nikto

Nikto являє собою утиліту з відкритим початковим кодом, призначену для сканування веб-серверів та виявлення потенційних проблем безпеки. Серед основних методів, що використовуються Nikto:

– Перевірка конфігурації веб-сервера та версій програмного забезпечення. Зокрема, здійснюється ідентифікація типу сервера (Apache, Nginx тощо), його версії та наявності оновлень, які усувають вразливості. Це дозволяє виявити застарілі компоненти, що можуть містити уразливості.

– Аналіз структури каталогів та доступних для перегляду файлів. Наприклад, Nikto перевіряє наявність службових файлів (php.ini, backup-файлів тощо), які часто містять цінну інформацію для зловмисників.

– Сканування URL-адрес та перевірка на доступність сторінок, прихованих від звичайних користувачів (наприклад, /administrator/). Саме це допомагає виявити наявність помилок конфігурації.

– Перевірка заголовків HTTP-відповідей на предмет встановлення захисних політик (HSTS, X-Content-Type-Options тощо), що свідчить про рівень захищеності.

– Моделювання атак шляхом спроб доступу до вбудованих функцій програмних мов (PHP, ASP, CGI), що допомагає виявити можливості SQL-ін’єкцій, XSS та інших уразливостей.

2. ZAP (Zed Attack Proxy):

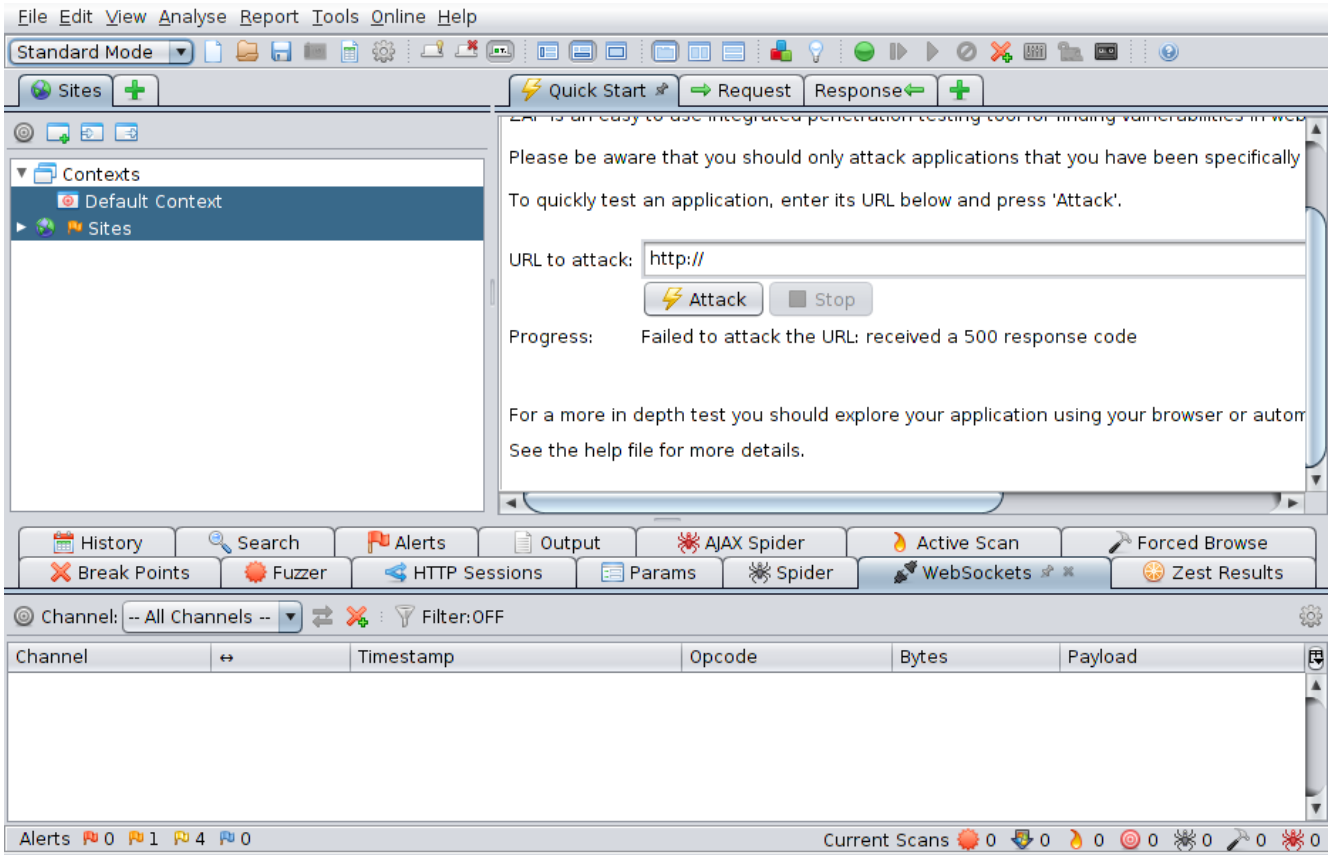

Рисунок 2.3 – Утиліта ZAP (Zed Attack Proxy)

Потужний open-source інструмент, призначений для виявлення уразливостей веб-додатків.

ZAP працює за принципом проксі-сервера, перехоплюючи весь HTTP(S)-трафік між клієнтом та сервером. Це дає змогу йому як пасивно аналізувати відповіді на запити, так і безпосередньо тестувати застосунок через імітацію різноманітних веб-атак та ін’єкцій.

Одним із основних методів ZAP є пасивне сканування, коли аналізуються відповіді сервера на нормальні запити клієнта. При цьому шукаються ознаки:

- Використання застарілих версій протоколів та компонентів, що містять відомі уразливості;
- Відсутність захисних HTTP-заголовків (CSP, HSTS тощо);
- Наявність потенційно небезпечних параметрів у URL/формах.

Крім того, ZAP здійснює активне тестування шляхом імітації різних класичних атак:

- XSS - введення JavaScript-коду для перевірки його виконання;
- SQL-ін’єкції - модифікація SQL-запитів для отримання доступу до БД;
- Перехоплення сесій - фальсифікація авторизаційних заявок.

3. Burp Suite.

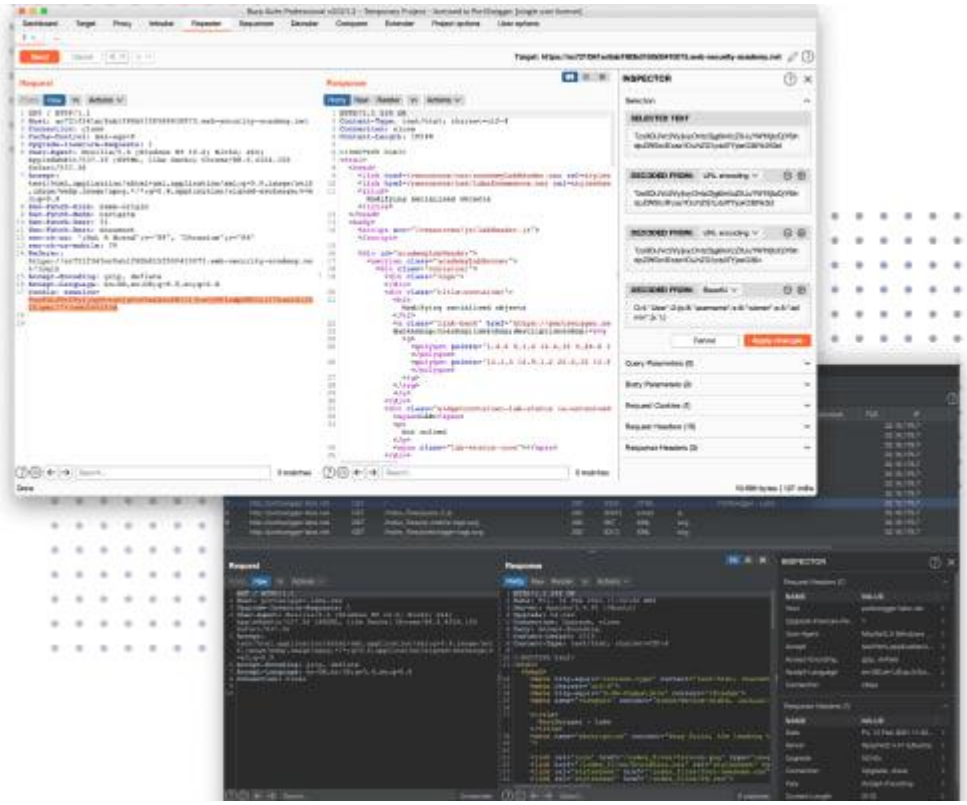

Рисунок 2.3 – Утиліта Burp Suite

Burp Suite - це інтегрована платформа для тестування безпеки веб-додатків. Вона включає в себе набір інструментів, які дозволяють проводити різноманітні види тестування безпеки, включаючи сканування вразливостей, перехоплення та

модифікацію трафіку, аналіз протоколу та багато іншого. Основні методи роботи Burp Suite включають:

1. Сканування вразливостей: Burp Suite здатний автоматично виявляти різні типи вразливостей у веб-додатках, такі як кросс-сайт скриптинг (XSS), SQL-ін’єкції, вразливості на основі вводу користувача, некоректне управління авторизацією тощо.

2. Перехоплення трафіку: Burp Suite дозволяє перехоплювати та аналізувати HTTP трафік між веб-додатком і клієнтом. Це дозволяє виявляти потенційні вразливості, а також тестувати та модифікувати запити та відповіді.

3. Аналіз протоколу: Burp Suite надає інструменти для детального аналізу протоколів, таких як HTTP, HTTPS, WebSocket, і багато інших. Це допомагає розуміти взаємодію між клієнтом і сервером і виявляти потенційні вразливості.

Переваги Burp Suite включають:

- Широкий функціонал: Burp Suite має великий набір інструментів для проведення різноманітних видів тестування безпеки.
- Дружній інтерфейс: Інтерфейс Burp Suite є досить інтуїтивно зрозумілим, що дозволяє навіть новачкам швидко освоїти утиліту.
- Розширюваність: Burp Suite підтримує розширення, що дозволяє розробникам створювати власні додаткові функції та інструменти для рішення конкретних задач.

В цілому, Burp Suite є потужним інструментом для тестування безпеки веб-додатків, який використовується як професійними тестувальниками, так і експертами з інформаційної безпеки.

Використання саме цих трьох утиліт давало змогу провести комплексне тестування на різних рівнях - від перевірки конфігурації серверів до аналізу самого веб-застосунку та його структури, що дозволило нам максимально всебічно оцінити рівень кіберзахисту магазину «Sportshop».

2.2 Виявлення недоліків та слабких місць у кіберзахисті «Sportshop».

Під час проведеного тестування було виявлено низку технічних недоліків у реалізації захисних механізмів на сайті «Sportshop»(Додаток А).

Під час тестування було виявлено такі основні проблеми:

1. Відсутні основні HTTP-заголовки безпеки створюють значні ризики для сайту «Sportshop».

Це стосується заголовка Strict-Transport-Security. Його відсутність означає, що сайт може бути досягнутий через незашифрований HTTPS. Це дозволяє здійснювати атаки «людина посередині» та перенаправляти користувачів на фальшиві сторінки з метою викрадення особистих даних [3].

Також відсутній X-Frame-Options робить сайт уразливим для clickjacking-атак, коли сторінки вбудовуються в iframe сторонніх сайтів без відома користувача. Це дозволяє виконувати дії від його імені на цій сторінці [13].

Відсутність XSS-Protection та Content-Security-Policy створює ризики проведення XSS-атак для виконання коду в контексті сайту. CSP є більш потужним інструментом для запобігання цій проблемі [3].

2. Куки не містять захисних атрибутів HttpOnly та Secure.

Відсутність захисних атрибутів HttpOnly та Secure у куки сайту «Sportshop» створює додаткові ризики для конфіденційності користувачів [13].

Наявність лише атрибута HttpOnly означає, що куки будуть доступні для JavaScript на сайті, що робить їх вразливими до викрадення через уразливості типу XSS. Впливовий зловмисник зможе отримати та використовувати ідентифікаційні дані користувачів.

Відсутність атрибута Secure створює ризики перехоплення куків при роботі через незашифрований HTTP, а також можливості їх модифікації, щодозволяє проводити різні атаки на основі данних з кукіс, наприклад фальсифікації сесії.

3. Використовуються універсальні сертифікати з дикими кардами.

Використання універсальних сертифікатів з дикими кардами (wildcard certificates) на сайті «Sportshop» не є найкращим підходом і створює додаткові ризики.

Такі сертифікати дозволяють зашифрувати безліч піддоменів за допомогою одного сертифіката. Проте це суттєво знижує рівень ідентифікації домену, оскільки дозволяє замінити будь-який піддомен на фальшивий [4].

Це ускладнює перевірку цілісності сертифіката клієнтом та довіру до нього. Крім того, негативно позначається на прозорості власників subdomain та їх відповідальності.

Випадкова особа може отримати сертифікат для піддомену шляхом генерації випадкових букв перед точкою. Це дозволяє проводити фішингові атаки без труднощів [13].

4. Прямий доступ до файлів конфігурації (config.php та ін.), в яких можуть міститись облікові дані.

Прямий доступ до файлів конфігурації, таких як config.php, може становити ризик для безпеки, оскільки в таких файлах часто містяться чутливі дані:

- Імена баз даних, користувачі та паролі для підключення до СУБД, що дає змогу зловмиснику отримати доступ до БД та дані сайту/системи.
- Імена таблиць, назви полів і т.п., що полегшує проведення SQL-ін’єкцій або дізнання про структуру БД.
- Налаштування модулів, компонентів, API-ключі та ін, що може призвести до несанкціонованого використання функціоналу або обходу захистів.
- Внутрішні параметри та логіка роботи системи, що полегшує подальшу експлуатацію вразливостей.

Тому, до таких файлів мають мати доступ лише сервер, а не будь-який користувач з мережі, що запобігає потраплянню чутливої інформації у несанкціоновані руки.

5. Потенційні вразливості застарілих компонентів (Vignette CMS, Siteseed тощо).

Вони можуть призвести до таких ризиків:

– Відомі уразливості - старі версії програмного забезпечення часто містять вже виявлені та задокументовані уразливості, експлуатація яких не потребує значних зусиль.

– Відсутність підтримки - старі компоненти не отримують оновлень та виправлень багів, тому вразливості можуть лишатися неусуненими роками.

– Застарілі протоколи - деякі системи працюють із застарілими технологіями, що суттєво підвищує ризики (наприклад, HTTP взамін HTTPS).

– Невідповідність стандартам - нові вимоги безпеки та методи атак можуть не враховуватись через брак оновлень.

– Витік інформації - старі скрипти, конфігурації чи логічні помилки можуть призводити до витоку даних.

Тому, застосування застарілих компонентів підвищує ризики їхньої вразливості та вимагає якнайшвидшої заміни на більш сучасні та безпечні аналоги [11].

6. Вразливості конфігурації веб-сервера.

Вони зазвичай призводять до таких наслідків:

– Доступ до тестових скриптів та каталогів дає змогу зловмиснику отримати інформацію про систему та налаштування сервера, що полегшує подальшу експлуатацію інших вразливостей.

– Відсутність фільтрів для файлів конфігурації дозволяє отримати доступ до внутрішніх налаштувань сервера, користувацьких даних БД та інформації про сайт.

– Можливе виконання довільних команд на сервері шляхом маніпуляції змінними середовища чи конфігураційними даними.

– Простіший доступ до ресурсів файлової системи, що дозволяє завантажувати/видаляти файли, читати/записувати дані та ін.

– Обхід механізмів аутентифікації та захисту за допомогою використання внутрішніх інтерфейсів та URL.

7. Відсутні заголовки XSS-захисту.

Інтернет-магазин може бути уразливим до атак міжсайтового скриптингу (XSS), що може призвести до впровадження шкідливого JavaScript на сторінці, яке може використовуватись для викрадення інформації користувачів або виконання небажаних дій.

8. Відсутній Content-Security-Policy.

Відсутня політика безпеки контенту, яка може обмежити виконання небезпечних скриптів на сторінках сайту, що може призвести до збільшення ризику вразливостей XSS.

9. Відсутні моніторинг та попередження про спроби атак.

Адміністратори сайту не отримують повідомлень про спроби атак або ненормальну активність, що може призвести до того, що атаки залишаються непоміченими та мають продовжуватись [15].

10. Можливі проблеми з компонентами управління сайтом (Vignette CMS).

Інтернет-магазин використовує застарілу або уразливу версію CMS, що може бути використана злоумисниками для вторгнення або компрометації сайту.

11. Відсутність стандартних HTTP-заголовків (Cache-Control, Last-Modified тощо).

Інтернет-магазин може позначати неналежне управління кешуванням та версіонуванням контенту, що може призвести до проблем з безпекою та збоїв у роботі сайту.

12. Неналежна обробка POST-запитів (відсутність CSRF-захисту).

Сайт може бути уразливим до атак міжсайтового підроблення запитів (CSRF), що може призвести до виконання небажаних дій від імені авторизованого користувача [17].

13. Можливі помилки конфігурації веб-серверу, що дозволяють обхід авторизації.

14. Вразливості схеми аутентифікації та управління сесіями – дуже часто можуть бути використані для підробки ідентифікаційних даних користувачів або для викрадення сесійних ключів.

15. Сканування виявило кілька потенційно небезпечних файлів і скриптів, що може дозволити зловмисникам виконати атаки, такі як внедрення коду, витік інформації або заборона обслуговування.

16. Сторонні DNS-запити, які можуть використовуватись для відстеження.

Більшість сайтів використовують зовнішні сервіси (CDN, статистика відвідувань та ін.), які можуть здійснювати DNS-запити до сторонніх доменів для отримання різних ресурсів та послуг. Ці запити містять IP-адресу сесії користувача та можуть бути використані для його відстеження та побудови профілю через серію переходів [13].

Для уникнення цього необхідно:

– Перевірити конфігурацію всіх зовнішніх інтеграцій на предмет мінімізації сторонніх запитів;

– Використовувати локальні копії статичних ресурсів (картинки, CSS, JS тощо);

– Встановити політику безпеки контенту (CSP) для блокування завантаження ресурсів із сторонніх доменів;

– Уникати динамічних DNS-запитів та звертатися безпосередньо до статичних IP-адрес.

17. Відсутній захист від DDoS та формування перевантажень.

DDoS-атаки можуть призводити до відмови в обслуговуванні сервісів та збоїв роботи сайту. Для їх захисту рекомендується:

– Використовувати хмарні сервіси моніторингу трафіку та захисту від DDoS (Akamai, Cloudflare, Imperva та ін.);

– Встановити хмарні WAF-фільтри біля межі провайдера для блокування підозрілих запитів;

– Забезпечити можливість масштабування пропускної здатності серверів;

– Обмежити пакетну та запитну частоту на рівні прильоту на шлюз;

– Зменшити атакувальну поверхню за рахунок усунення старих скриптів та непотрібних функцій;

– Використовувати сервіси сповіщень про DDoS та налаштувати автоматичне перенаправлення трафіку через них;

– Запобігати збоям за допомогою CDN та контентної доставки з кращих точок.

18. Можливості аналізу трафіку для пошуку вразливостей.

19. Неналежна структура сайту та наявність застарілих компонентів.

20. Відсутність механізмів автентифікації та ідентифікації користувачів (наприклад, мультифакторна аутентифікація), що створює ризики несанкціонованого доступу в разі викрадення логінів/паролів.

21. Відсутність шифрування даних у сховищах (БД). Дозволяє в разі проникнення отримати незашифровану інформацію.

22. Брак протоколів керування версіями та міграціями додатків. Може призвести до використання застарілих модулів з відомими вразливостями [11].

23. Відсутні обмеження по IP при отриманні доступу до адмінки, що дозволяє спроби brute-force атак [9].

24. Можливі уразливості в компонентах типу завантаження файлів через форми і скрипти обробки.

25. Брак контролю цілісності контенту, що дозволяє змінювати сторінки третім особам.

26. Відсутні базові перевірки вхідних даних на наявність небезпечного синтаксису (перевірка на ін’єкції).

27. Можливі проблеми в безпеці мобільних додатків або інтерфейсів, якщо такі є.

28. Відсутня профілактика DDoS та потужних перевантажень сервісів.

2.3 Порівняння з кращими практиками та стандартами з кіберзахисту.

Найкращі практики та стандарти кіберзахисту, до яких варто порівняти рівень захищеності інтернет-магазину «Sportshop», включають:

1. OWASP Top 10 - перелік 10 найпоширеніших веб-уразливостей, рекомендованих для тестування та усунення.

2. STANDARD HTTPS - використання TLS 1.2 або вище, HSTS, CSP, кінцевий сертифікат та атрибути HttpOnly, Secure для кукіс.

3. W3C Web Content Accessibility Guidelines (WCAG) - правила доступності веб-контенту для забезпечення безперешкодного доступу.

4. OWASP ASVS - стандартизований набір вимог до рівня безпеки веб-додатків. Може слугувати путівником для аудиту.

5. NIST Cybersecurity Framework (CSF) - комплексний підхід до управління ризиками та продемонстрування рівня захищеності.

6. PCI DSS - вимоги до захисту платіжних даних. Доречні для е-комерс сайтів.

7. ISO/IEC 27001/27002 - міжнародні стандарти управління інформаційною безпекою.

NIST SP800-53 - детальні технічні вимоги щодо захисту федеральних систем США.

OWASP ASV - вимоги до процесу тестування безпеки додатків.

IETF публікації (RFC) - нормативні документи щодо протоколів та практик мережевої безпеки.

Порівняння з цими стандартами дозволить найоб’єктивніше оцінити рівень захищеності «Sportshop» та виявити конкретні заходи оптимізації.

3 ЗАПРОПОНОВАНА МОДЕЛЬ СИСТЕМИ КІБЕРЗАХИСТУ ДЛЯ ІНТЕРНЕТ-МАГАЗИНУ «SPORTSHOP»

3.1 Функціональна структура системи

Для покращення рівня кібербезпеки інтернет-магазину «SportShop» доцільно розробити та впровадити комплексну систему захисту з наступною функціональною структурою:

1. Захист периметру:
   - Мережеві фільтри (NGFW):
   - Брандмауер (з модулем DDoS-захисту);
   - IDS/IPS (виявлення та запобігання вторгненню);
   - WAF (фільтрація HTTP(S)-запитів);
   - Проксі (захист HTTP(S)-трафіку).
2. Аутентифікація та SSO:
   - Багатофакторна аутентифікація;
   - Централізоване управління обліковими записами;
   - Служба одноразового входу для різних функціональних одиниць.
3. Захист баз даних:
   - Шифрування таблиць і полів;
   - Контроль доступу за ролями;
   - Аудит транзакцій;
   - Резервне копіювання;
   - Автоматичне оновлення.
4. Моніторинг безпеки:
   - Система збору логів;
   - Аналіз поведінки користувачів;
   - Виявлення аномальної активності;
   - Оповіщення адміністраторів.
5. Управління конфігурацією:
   - Встановлення та оновлення ПЗ;

- Контроль версій компонентів;
- Захист конфігураційних файлів;
- Управління доступом.

6. Захист застосунків:
   - Захист від ін’єкцій;
   - Захист від XSS/CSRF;
   - Контроль доступу;
   - Фільтрація входів;
   - Автоматичне тестування.
7. Інформаційна безпека:
   - Навчання персоналу;
   - Політика безпеки;
   - Менеджмент інцидентів;
   - Технічна підтримка;
   - Сертифікація системи.

На схемі нижче зображено основні компоненти запропонованої архітектури системи кіберзахисту «SportShop» і взаємозв’язки між ними для забезпечення комплексного захисту інтернет-магазину. Ця система дозволить підвищити рівень інформаційної безпеки та запобігти більшості загроз, виявлених на етапі тестування.

Далі, в підрозділі 3.2 ця схема буде детально розглянута.

А для успішної реалізації запропонованої моделі кіберзахисту «SportShop» необхідно дотриматися таких рекомендацій:

- Провести аудит існуючої IT-інфраструктури для визначення необхідних оновлень.
- Розробити детальний проект впровадження системи з розподілом ролей та відповідальності.
- Підібрати необхідне програмне забезпечення та укласти договори з постачальниками.

– Підготувати персонал пройти навчання з кібербезпеки, управління системою, політикою безпеки.

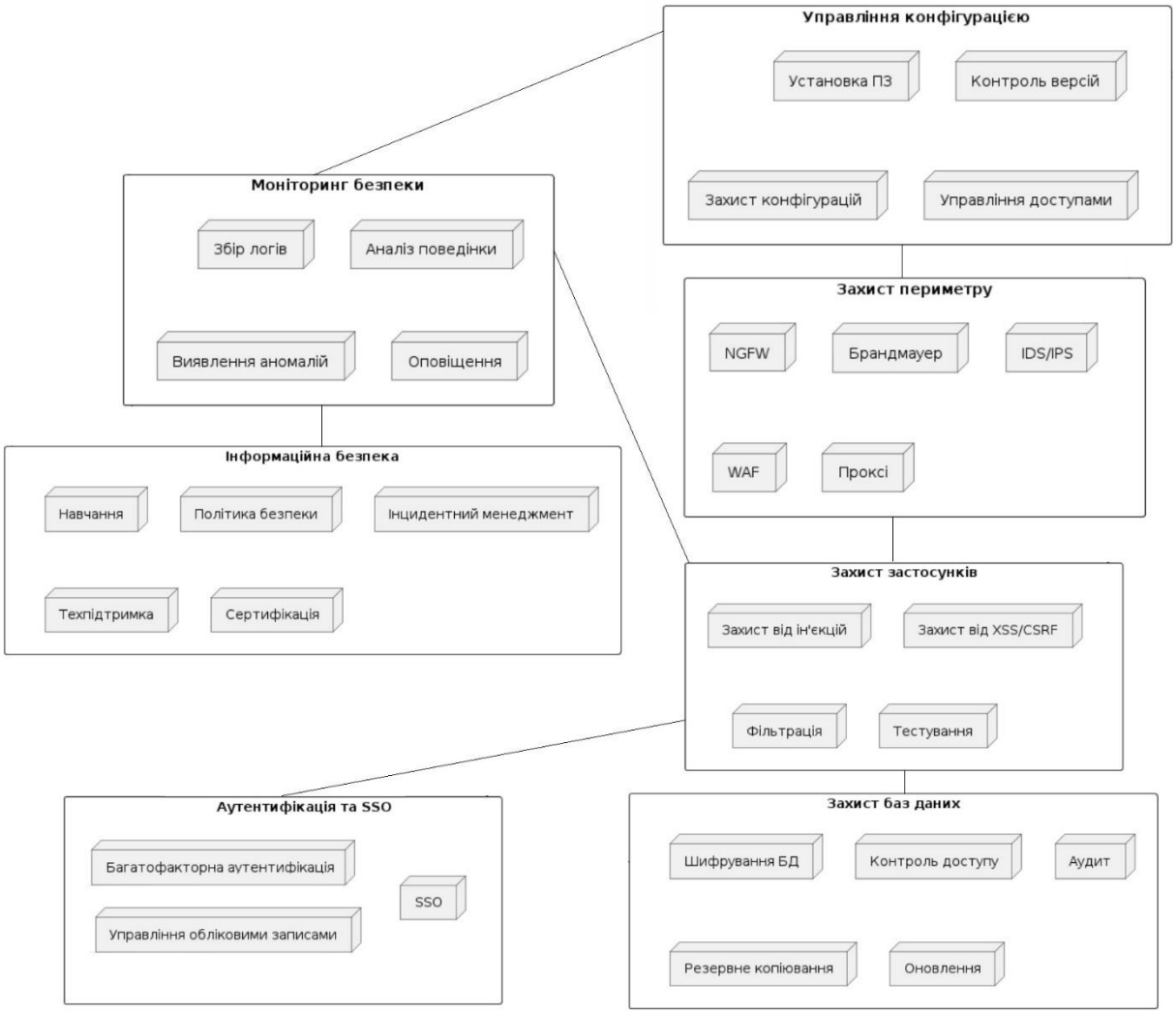

Рисунок 3.1 - Основні функціональні блоки та їх взаємозв’язки для кіберзахисту «SportShop»: периметр, аутентифікація, захист БД, моніторинг, конфігурація, застосунки та інформаційна безпека

– Реалізувати впровадження системи крок за кроком з тестуванням на кожному етапі.

– Провести регулярні аудити системи, оновлення ПЗ і політик, навчання персоналу.

– Забезпечити безперервний моніторинг та оперативну реакцію підрозділу безпеки.

– Уточнювати структуру системи, враховуючи зміни бізнес-процесів і тенденції в кіберзагрозах.

Дотримання цих рекомендацій дозволить ефективно реалізувати запропоновану модель кіберзахисту «SportShop» і досягти бажаного рівня захищеності систем.

3.2 Опис основних компонентів системи кіберзахисту для інтернет-магазину «SportShop», та рекомендації для уникнення кіберзагроз в майбутньому

Для більш детального розуміння функціонування запропонованої моделі системи кіберзахисту, розглянемо окремі її основні компоненти:

1. Захист периметру.

До складу захисту периметру входять спеціалізовані засоби, що забезпечують захист на межі з зовнішніми мережами:

- NGFW (Next Generation Firewall) - мережеві фільтри нового покоління, які поєднують функції файрволу, IDS/IPS, антивірусу, фільтрації web-трафіку та малварі.
- Брандмауер - основний елемент захисту периметру, який фільтрує вхідний/вихідний трафік за правилами.
- IDS/IPS - системи виявлення/запобігання вторгненням, які аналізують трафік та виявляють зловмисні дії.
- WAF - веб-аплікативний фільтр, який захищає HTTP(S)-сервіси від уразливостей.
- Проксі - у разі використання хмарних сервісів дозволяє захистити внутрішні мережі.

2. Аутентифікація та SSO.

- Багатофакторна авторизація (MFA) додає додаткові фактори (SMS, ключ, біометрія) для несанкціонованого доступу.
- Централізоване управління обліковими записами (UMC) забезпечує єдиний підхід до налаштувань.

- SSO (Single Sign-On) дозволяє користувачам авторизуватися один раз для доступу до різних систем.

3. Захист баз даних.

- Шифрування БД забезпечує захист конфіденційної інформації у випадку витоку/викрадення даних.
- Контроль доступу за ролями дозволяє надати привілеї користувачам лише до необхідних даних.
- Резервне копіювання та відновлення БД забезпечує відновлення її стану у разі аварійних ситуацій.

4. Моніторинг безпеки.

- Система збору логів важливих компонентів (NGFW, фільтри, сервери тощо) дає інформацію про події.
- Аналіз поведінки користувачів за допомогою SIEM ліквідовує ризики внутрішніх загроз.
- Виявлення аномальної активності шляхом кореляції показників та встановлення бенчмарків норми.
- Оповіщення адміністраторів про підозрілі події у режимі реального часу дає швидку реакцію.

5. Управління конфігурацією.

- Автоматизована установка та оновлення ПЗ всіх компонентів запобігає ручним помилкам.
- Контроль версій дозволяє відстежувати конфігурацію та відновлювати при необхідності.
- Захист конфігураційних файлів від несанкціонованого доступу/змін забезпечує їх цілісність.
- Управління доступами на основі ролей надає права лише санкціонованим особам.

6. Захист застосунків.

- Фільтрація вхідних даних на предмет небезпечного синтаксису усуває ризики ін’єкцій.

- Захист від XSS/CSRF встановлює перевірку токенів та екранування виходів.
- Контроль доступу забезпечується через систему авторизації та ACL.
- Автотестування на основі OWASP/SANs Top 10 перевіряє нові уразливості.

7. Інформаційна безпека.

- Навчання персоналу підвищує обізнаність щодо кіберзагроз та безпечної поведінки.
- Політика безпеки встановлює єдині правила для всіх працівників та сторонніх.
- Інцидентний менеджмент чітко врегульовує процес реагування на порушення.
- Сертифікація системи підвищує довіру клієнтів та партнерів.

Саме таким чином, на нашу думку, всі компоненти в межах єдиної системи кіберзахисту забезпечать комплексний захист інтернет-магазину «SportShop».

3.3 Рекомендації щодо подальшого кіберзахисту «SportShop»

Для подальшого підвищення рівня захищеності інтернет-магазину «SportShop» пропонується впровадити наступні заходи:

1. Аудит безпеки веб-додатків
2. Аудит інфраструктури
3. Оновлення програмних компетенцій
4. Зміна паролів адміністраторів
5. Навчання персоналу
6. Моніторинг веб-серверів
7. Сканування застосунків
8. Аналіз логів додатків
9. Шифрування трафіку
10. Аудит БД

11. Бекап БД

12. Аналіз конфігурацій

13. Моніторинг сайту

14. Звіти керівництву

15. Файрвол

16. Управління правами

17. VPN

18. Антивірус

Це дозволить систематизувати процес підвищення рівня кіберзахисту «SportShop», контролювати його виконання та вчасно реагувати на загрози. Дотримання цих рекомендацій забезпечить належний захист онлайн-магазину.

Детальний опис цих заходів зазначений у Додатку Б.

3.4 Рекомендації для інших інтернет-магазинів на основі отриманих результатів

Оцінка рівня кібербезпеки інтернет-магазину «SportShop» та аналіз виявлених недоліків дозволили сформувати рекомендації для підвищення захищеності інших онлайн-магазинів, що мають такі ж вразливості.

Головне те, що, необхідно запровадити комплексний підхід до кібербезпеки, який передбачає захист всіх ланок бізнесу (периметру, застосунків, БД тощо), що дає змогу мінімізувати ризики і забезпечити компенсацію можливих недоліків окремих елементів.

Необхідно провести злагоджену роботу із:

– Виявлення та усунення існуючих уразливостей шляхом зовнішнього та внутрішнього аудитів;

– Впровадження найкращих практик на основі міжнародних стандартів типу OWASP, PCI DSS, ISO27001;

– Забезпечення захисту периметру, включаючи NGFW, WAF, DDoS-захист на рівні провайдера;

– Шифрування даних у БД, сертифікація системи зберігання;

– Контроль конфігурації та оновлень за допомогою інструментів управління версіями;

– Застосування багатофакторної автентифікації та сингл-сайн-она (SSO);

– Дотримання принципів мінімальних привілеїв для доступу до ресурсів;

– Регулярна перевірка функцій на наявність вразливостей та фіксація їх уразливих місць;

– Ведення журналів подій для моніторингу та виявлення аномалій;

– Навчання персоналу питань інформаційної безпеки для підвищення обізнаності.

Ще одним суттєвим фактором є застосування спеціалізованих програмних та апаратних засобів кіберзахисту. До них варто віднести:

– NGFW (мережеві фільтри нового покоління);

– SIEM (системи моніторингу та кореляції подій);

– WAF (захист веб-додатків та API);

– Інструменти автоматизованого тестування на вразливості;

– Програми управління конфігураціями та версіями;

– Криптографічні пристрої шифрування даних;

– DDoS-захист на рівні провайдера або хмарних сервісів;

– MFA (багатофакторна аутентифікація).

Використання комплексного підходу із залученням як процесних, так і технічних рішень дозволить іншим онлайн-магазинам досягти бажаного рівня кібербезпеки, уникнувши ризиків, виявлених при аналізі «SportShop». Це, у свою чергу, забезпечить захищеність бізнесу, його репутацію та лояльність клієнтів.

ВИСНОВКИ

В першому розділі нашої роботи було:

1. Проведено аналіз основних теоретичних підходів до кіберзахисту інтернет-магазинів, які передбачають застосування комплексу технічних, організаційних та правових заходів, оцінку ризиків, мінімізацію вразливостей системи та постійний моніторинг подій. Для ефективного захисту необхідно застосовувати всі чотири підходи комплексно.

2. Проаналізовано основні загрози та вразливості, на які націлені сучасні кібератаки на інтернет-магазини, зокрема: аутентифікація, авторизація, атаки на клієнтів та сервер, виконання шкідливого коду. Більшість з них пов’язані з метою отримання доступу до конфіденційної інформації або накладання збоїв на роботу сервісу.

3. Розглянуто найкращі практики та стандарти кіберзахисту для інтернет-магазинів, серед яких: PCI DSS, OWASP, загальні принципи кібергігієни, робота з персоналом та технічні заходи. Дотримання їх є обов’язковим для забезпечення безпеки бізнесу та клієнтів.

4. Наведено приклади реальних інцидентів, пов’язаних з кіберзагрозами для інтернет-магазинів, що свідчить про актуальність теми дослідження та необхідність застосування ефективних заходів захисту.

В другому розділі нашої роботи було:

1. Проведено комплексне тестування інтернет-магазину «Sportshop» за допомогою утиліт Nikto, ZAP та Burp Suite, що дало змогу оцінити його рівень захищеності з різних аспектів.

2. Виявлено низку недоліків у кіберзахисті, зокрема відсутність основних HTTP-заголовків безпеки, незахищені куки, використання універсальних сертифікатів, прямий доступ до конфігураційних файлів, застарілі компоненти та вразливості конфігурації.

3. Описано також відсутність XSS-захисту, Content-Security-Policy, моніторингу інцидентів, недосконалість аутентифікації та управління сесіями, наявність потенційно небезпечних файлів.

4. Виявлені проблеми не відповідають кращим практикам та стандартам кіберзахисту, описаним у розділі.

В третьому розділі нашої роботи було:

1. Запропоновано функціональну структуру системи кіберзахисту для інтернет-магазину «SportShop», що включає 7 основних компонентів: захист периметру, аутентифікацію, захист БД, моніторинг, конфігурацію, застосунки та інформаційну безпеку.

2. Зображено блок-схему функціональних блоків та їх взаємозв’язків для запропонованої системи кіберзахисту.

3. Описано основні компоненти системи кіберзахисту: захист периметру, аутентифікацію, захист баз даних, моніторинг, управління конфігурацією, захист застосунків та інформаційну безпеку.

4. Наведено рекомендації щодо успішної реалізації запропонованої моделі, зокрема проведення аудиту, розробки проекту, підготовки персоналу, впровадження в кілька етапів.

5. Сформульовано рекомендації для покращення кіберзахисту «SportShop» у майбутньому, зокрема щодо регулярних аудитів, оновлень, навчань, моніторингу тощо.

ПЕРЕЛІК ПОСИЛАНЬ

1. Спортивний магазин «SportShop» URL: https://sportshop.com.ua/
2. Black, E. IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation. Crown Pub, 2001.
3. Publishing C. G. Don't Panic! I'm a Professional Senior Cybersecurity Analyst : Customized 100 Page Lined Notebook Journal Gift for a Busy Senior Cybersecurity Analyst: Far Better Than a Throw Away Greeting Card. Independently Published, 2020. 102 p.
4. Quotes C. Cybersecurity Engineer I'm Not Arguing I'm Just Explaining Why I'm Right. Independently Published, 2020.
5. Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and general model. ISO/IEC SC27 N2161, 1998.
6. Information Processing Systems – Open Systems Interconnection
7. (ISO), Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) – Application Level Syntax Rule
8. Баранов О. А. Про тлумачення та визначення поняття "кібербезпека". Правова інформатика. 2014. № 2 (42). С. 54–62.
9. КОНДРАТЮК М. В. КІБЕРБЕЗПЕКА УКРАЇНИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ. Law and Society. 2019. Т. 6, № 2. С. 42–48. URL: https://doi.org/10.32842/2078-3736-2019-6-2-7
10. Красильников С. Р. Розробка освітньо-професійної програми підготовки фахівців спеціальності "кібербезпека" на компетентнісній основі. Вісник Хмельницького національного університету. Технічні науки. 2016. № 3 (237). С. 82–86.
11. Кузьменко О., Маклюк О., Чернишова О. КІБЕРБЕЗПЕКА БІЗНЕСУ ПІД ЧАС ВІЙНИ. Економіка та суспільство. 2022. № 44. URL: https://doi.org/10.32782/2524-0072/2022-44-21
12. Лебідь А. Є., Лебедь А. Е., Lebid A. Y. Інформаційна та кібербезпека в умовах гібридних воєн: український контекст : thesis. 2019. URL: https://essuir.sumdu.edu.ua/handle/123456789/77115

13. Нечипоренко І. Д. Кібербезпека: захист від фішингу : thesis. 2018. URL: http://essuir.sumdu.edu.ua/handle/123456789/66886
14. Плєхова Г., Суханова Н., Левтеров А. КІБЕРБЕЗПЕКА: ЗАГРОЗИ, РІШЕННЯ. Theoretical Foundations in Economics and Management. 2022. P. 681–692. URL: https://doi.org/10.46299/isg.2022.mono.econ.2.9.6 (date of access: 17.04.2024).
15. ПОЛІЩУК В. КІБЕРЗЛОЧИНИ ТА КІБЕРБЕЗПЕКА: БОРОТЬБА З КОМП'ЮТЕРНИМИ ЗЛОЧИНАМИ І КІБЕРАТАКАМИ. Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки. 2023. № 3(66). С. 44–47. URL: https://doi.org/10.32689/2522-4603.2023.3.7
16. Про проведення парламентських слухань на тему: "Кібербезпека, критична інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення" : Постанова Верховної Ради України від 04.02.2020 р. № 500-IX. URL: https://zakon.rada.gov.ua/laws/show/500-20#Text
17. Сопілко І. ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА: ПОРІВНЯЛЬНО-ПРАВОВИЙ АСПЕКТ. Scientific works of National Aviation University. Series: Law Journal "Air and Space Law". 2021. Т. 2, № 59. С. 110–115. URL: https://doi.org/10.18372/2307-9061.59.15603.
18. Тенденції розвитку інтернет-бізнесу : thesis / Е. А. Короткова та ін. 2015. URL: http://essuir.sumdu.edu.ua/handle/123456789/43532
19. Bykov V. Y., Burov O. Y., Dementievska N. P. КІБЕРБЕЗПЕКА В ЦИФРОВОМУ НАВЧАЛЬНОМУ СЕРЕДОВИЩІ. Information Technologies and Learning Tools. 2019. Т. 70, № 2. С. 313. URL: https://doi.org/10.33407/itlt.v70i2.2876
20. Kosenko A. V., Vanina Y. A. Особливості організації бізнесу в мережі Інтернет. Theory and Practice of Public Administration. 2019. Т. 2, № 65. С. 143–150. URL: https://doi.org/10.34213/tp.19.02.18
21. Mariyam R. C. КІБЕРБЕЗПЕКА ЯК СПЕЦІАЛЬНИЙ ПРИНЦИП ДІЯЛЬНОСТІ ЕЛЕКТРОННИХ ЗМІ. EurasianUnionScientists. 2019. Т. 5, № 65. URL: https://doi.org/10.31618/esu.2413-9335.2019.5.65.282

ДОДАТКИ

Додаток А. Результати перевірок. Основні проблеми сайту.

```
+ /: Retrieved x-powered-by header: PHP/7.3.33.
+ /: The anti-clickjacking X-Frame-Options header is not present.
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-
Frame-Options
+ /: Uncommon header 'x-nginx-upstream-cache-status' found, with
contents: EXPIRED.
+ /: Uncommon header 'x-server-powered-by' found, with contents:
Engintron.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header
is not defined. See: https://developer.mozilla.org/en-
US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: Cookie OCSESSID created without the secure flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie OCSESSID created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie language created without the secure flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie language created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie currency created without the secure flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie currency created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie jetcache_webp created without the secure flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie jetcache_webp created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /Q4zLoFyQ.save: Cookie ckeeper created without the secure flag.
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /Q4zLoFyQ.save: Cookie ckeeper created without the httponly flag.
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /Q4zLoFyQ.save: Cookie remarketing_cid created without the secure
flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /Q4zLoFyQ.save: Cookie remarketing_cid created without the
httponly flag. See: https://developer.mozilla.org/en-
US/docs/Web/HTTP/Cookies
+ /Q4zLoFyQ.php#: Cookie PHPSESSID created without the secure flag.
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /Q4zLoFyQ.php#: Cookie PHPSESSID created without the httponly
flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible
dirs)
+ /*?tracking=/: Cookie tracking created without the secure flag.
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /*?tracking=/: Cookie tracking created without the httponly flag.
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
```

```
+ /robots.txt: contains 28 entries which should be manually viewed.
See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The Content-Encoding header is set to «deflate» which may mean
that the server is vulnerable to the BREACH attack. See:
http://breachattack.com/
+ : Server banner changed from 'nginx' to 'Apache'.
+ /archive.pem: The X-Content-Type-Options header is not set. This
could allow the user agent to render the content of the site in a
different fashion to the MIME type. See:
https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/
+ Server is using a wildcard certificate: *.biotech.com.ua. See:
https://en.wikipedia.org/wiki/Wildcard_certificate
+ Server is using a wildcard certificate: *.euroamino.com. See:
https://en.wikipedia.org/wiki/Wildcard_certificate
+ Server is using a wildcard certificate: *.sportshop.com.ua. See:
https://en.wikipedia.org/wiki/Wildcard_certificate
+ /: Web Server returns a valid response with junk HTTP methods
which may cause false positives.
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in
forum_edit_post.php, forum_post.php and forum_reply.php.
+ /lists/admin/: PHPList pre 2.6.4 contains a number of
vulnerabilities including remote administrative access, harvesting
user info and more. Default login to admin interface is
admin/phplist.
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have
multiple security problems which could not be tested remotely. See:
https://seclists.org/bugtraq/2002/Jul/262
+ /ssdefs/: Siteseed pre 1.4.2 has 'major' security problems.
+ /sshome/: Siteseed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to
be viewed via a 'URL trick'. Default login/pass could be
admin/admin.
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted
Wiki pages to be viewed via a 'URL trick'. Default login/pass could
be admin/admin.
+ /scripts/samples/details.idc: NT ODBC Remote Compromise. See:
http://attrition.org/security/advisory/individual/rfp/rfp.9901.nt_od
bc
+ /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by
requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not
attempted. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2000-0709
+ /~root/: Allowed to browse root's home directory. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1013
+ /cgi-bin/wrap: Allows viewing of directories.
+ /forums//admin/config.php: PHP Config file may contain database
IDs and passwords.
+ /forums//adm/config.php: PHP Config file may contain database IDs
and passwords.
```

```
+ /forums//administrator/config.php: PHP Config file may contain
database IDs and passwords.
+ /forums/config.php: PHP Config file may contain database IDs and
passwords.
+ /guestbook/guestbookdat: PHP-Gastebuch 1.60 Beta reveals sensitive
information about its configuration.
+ /guestbook/pwd: PHP-Gastebuch 1.60 Beta reveals the md5 hash of
the admin password.
+ /help/: Help directory should not be accessible.
+ /hola/admin/cms/htmltags.php?datei=./sec/data.php: hola-cms-1.2.9-
10 may reveal the administrator ID and password. See:
https://vulners.com/exploitdb/EDB-ID:23027
+ /global.inc: PHP-Survey's include file should not be available via
the web. Configure the web server to ignore .inc files or change
this to global.inc.php. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2002-0614
+ /inc/common.load.php: Bookmark4U v1.8.3 include files are not
protected and may contain remote source injection by using the
'prefix' variable. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2003-1253
+ /inc/config.php: Bookmark4U v1.8.3 include files are not protected
and may contain remote source injection by using the 'prefix'
variable. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2003-1253
+ /inc/dbase.php: Bookmark4U v1.8.3 include files are not protected
and may contain remote source injection by using the 'prefix'
variable. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2003-1253
+ /geeklog/users.php: Geeklog prior to 1.3.8-1sr2 contains a SQL
injection vulnerability that lets a remote attacker reset admin
password. See: https://vulners.com/osvdb/OSVDB:2703
+ /gb/index.php?login=true: gBook may allow admin login by setting
the value 'login' equal to 'true'. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2002-1560
+ /guestbook/admin.php: Guestbook admin page available without
authentication.
+ /getaccess: This may be an indication that the server is running
getAccess for SSO.
+ /cfdocs/expeval/openfile.cfm: Can use to expose the system/server
path.
+ /tsweb/: Microsoft TSAC found. See:
https://web.archive.org/web/20040910030506/http://www.dslwebserver.c
om/main/fr_index.html?/main/sbs-Terminal-Services-Advanced-Client-
Configuration.html
+ /vgn/performance/TMT: Vignette CMS admin/maintenance script
available.
+ /vgn/performance/TMT/Report: Vignette CMS admin/maintenance script
available.
+ /vgn/performance/TMT/Report/XML: Vignette CMS admin/maintenance
script available.
```

```
+ /vgn/performance/TMT/reset: Vignette CMS admin/maintenance script
available.
+ /vgn/ppstats: Vignette CMS admin/maintenance script available.
+ /vgn/previewer: Vignette CMS admin/maintenance script available.
+ /vgn/record/previewer: Vignette CMS admin/maintenance script
available.
+ /vgn/stylepreviewer: Vignette CMS admin/maintenance script
available.
+ /vgn/vr/Deleting: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Editing: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Saving: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Select: Vignette CMS admin/maintenance script available.
+ /scripts/iisadmin/bdir.htr: This default script shows host info,
may allow file browsing and buffer a overrun in the Chunked Encoding
data transfer mechanism, request /scripts/iisadmin/bdir.htr??c:\
. See: https://docs.microsoft.com/en-us/security-
updates/securitybulletins/2002/MS02-028
+ /scripts/iisadmin/ism.dll: Allows you to mount a brute force
attack on passwords.
+ /scripts/tools/ctss.idc: This CGI allows remote users to view and
modify SQL DB contents, server paths, docroot and more.
+ /bigconf.cgi: BigIP Configuration CGI.
+ /blah_badfile.shtml: Allaire ColdFusion allows JSP source viewed
through a vulnerable SSI call.
+ /vgn/style: Vignette server may reveal system information through
this file. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2003-0401
+ /SiteServer/Admin/commerce/foundation/domain.asp: Displays known
domains of which that server is involved. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/Admin/commerce/foundation/driver.asp: Displays a list
of installed ODBC drivers. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/Admin/commerce/foundation/DSN.asp: Displays all DSNs
configured for selected ODBC drivers. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/admin/findvserver.asp: Gives a list of installed Site
Server components. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/Admin/knowledge/dsmgr/default.asp: Used to view
current search catalog configurations.
+ /basilix/mbox-list.php3: BasiliX webmail application prior to
1.1.1 contains a XSS issue in 'message list' function/page.
+ /basilix/message-read.php3: BasiliX webmail application prior to
1.1.1 contains a XSS issue in 'read message' function/page.
+ /clusterframe.jsp: Macromedia JRun 4 build 61650 remote
administration interface is vulnerable to several XSS attacks.
+ /IlohaMail/blank.html: IlohaMail 0.8.10 contains a XSS
vulnerability. Previous versions contain other non-descript
vulnerabilities.
+ /bb-dnbd/faxsurvey: This may allow arbitrary command execution.
```

```
+ /cartcart.cgi: If this is Dansie Shopping Cart 3.0.8 or earlier,
it contains a backdoor to allow attackers to execute arbitrary
commands.
+ /scripts/Carello/Carello.dll: Carello 1.3 may allow commands to be
executed on the server by replacing hidden form elements. This could
not be tested by Nikto. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2001-0614
+ /scripts/tools/dsnform.exe: Allows creation of ODBC Data Source.
+ /scripts/tools/dsnform: Allows creation of ODBC Data Source.
+ /SiteServer/Admin/knowledge/dsmgr/users/GroupManager.asp:
Microsoft Site Server script used to create, modify, and potentially
delete LDAP users and groups. See:
https://securitytracker.com/id/1003420
+ /SiteServer/Admin/knowledge/dsmgr/users/UserManager.asp: Microsoft
Site Server used to create, modify, and potentially delete LDAP
users and groups. See: https://securitytracker.com/id/1003420
+ /prd.i/pgen/: Has MS Merchant Server 1.0.
+ /readme.eml: Remote server may be infected with the Nimda virus.
+ /scripts/httpodbc.dll: Possible IIS backdoor found.
+ /scripts/proxy/w3proxy.dll: MSProxy v1.0 installed.
+ /siteseed/: Siteseed pre 1.4.2 have 'major' security problems.
+ /pccsmysqladm/incs/dbconnect.inc: This file should not be
accessible, as it contains database connectivity information.
Upgrade to version 1.2.5 or higher.
+ /iisadmin/: Access to /iisadmin should be restricted to localhost
or allowed hosts only.
+ /PDG_Cart/order.log: PDG Commerce log found. See:
http://zodi.com/cgi-
bin/shopper.cgi?display=intro&template=Intro/commerce.html
+ /ows/restricted%2eshow: OWS may allow restricted files to be
viewed by replacing a character with its encoded equivalent.
+ /view_source.jsp: Resin 2.1.2 view_source.jsp allows any file on
the system to be viewed by using \..\ directory traversal. This
script may be vulnerable.
+ /w-agora/: w-agora pre 4.1.4 may allow a remote user to execute
arbitrary PHP scripts via URL includes in include/*.php and
user/*.php files. Default account is 'admin' but password set during
install.
+ /vider.php3: MySimpleNews may allow deleting of news items without
authentication. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2002-2320
+ /officescan/cgi/cgiChkMasterPwd.exe: Trend Micro Officescan allows
you to skip the login page and access some CGI programs directly.
See:
https://web.archive.org/web/20030607054822/http://support.microsoft.
com/support/exchange/content/whitepapers/owaguide.doc
+ /admin/config.php: PHP Config file may contain database IDs and
passwords.
```

Додаток Б. План заходів з кібербезпеки «SportShop».

№	Назва заходу	Відповідальна особа	Періодичність	Термін виконання	Результат очікуваний	Коментарі
1	Аудит безпеки веб-додатків	Керівник відділу безпеки	Що півроку	31.01, 31.07	Виявлення та усунення уразливостей	Замовити послугу сторонній компанії
2	Аудит інфраструктури	Системний адміністратор	Щокварталу	15.04, 15.07, 15.10, 15.01	Усунення проблем конфігурації	Виконати внутрішньо з використанням утиліт
3	Оновлення програмних компонентів	Системний адміністратор	Щомісяця	01 число кожного місяця	Усунення вразливостей відомими оновленнями	Проводити автоматично за можливості
4	Зміна паролів адміністраторів	Системний адміністратор	Щокварталу	15.04, 15.07, 15.10, 15.01	Підвищення рівня захисту	Створювати випадкові паролі з великої кількості символів
5	Навчання персоналу	HR-менеджер	Щопівроку	30.06, 31.12	Формування культури безпеки	Тренінги «Фішинг», «уразливості», «дії при інцидентах»
6	Моніторинг веб-серверів	Системний адміністратор	Безперервно	-	Виявлення аномальної активності	Використання SIEM та системи алертів
7	Сканування застосунків	Системний адміністратор	Щомісяця	01 число кожного місяця	Виявлення уразливостей	Автоматизоване сканування Acunetix та Нікто
8	Аналіз логів додатків	Системний адміністратор	Щоденно	-	Виявлення підозрілої активності користувачів	Фільтрація за IP, діями, геолокацією
9	Шифрування трафіку	Системний адміністратор	Безперервно	-	Захист від атак «людина по-середині»	Встановлення SSL сертифікатів на www та адмінку
10	Аудит БД	Системний адміністратор	Щокварталу	15.04, 15.07, 15.10, 15.01	Виявлення слабких місць	Перевірка конфігурації, захисту, резервного копіювання
11	Бекап БД	Системний адміністратор	Щоденно	-	Захист від втрати даних	Автоматичне стиснуте ретельне копіювання на зовнішні носії

12	Аналіз конфігурацій	Системний адміністратор	Щотижня	Понеділок	-	Порівняння поточних файлів з шаблонними, виявлення змін
13	Моніторинг сайту	Системний адміністратор	Безперервно	-	Виявлення збоїв, збільшення навантаження	Слідкування за пропускною здатністю, часом відповіді, помилками
14	Звіти керівництву	Керівник відділу безпеки	Щомісяця	01 число кожного місяця	Інформування про стан безпеки	Події, результати тестувань, рекомендації, плани
15	Файрвол	Системний адміністратор	Безперервно	-	Захист периметру	Конфігурація правил доступу, IPs, протоколів
16	Управління правами	Системний адміністратор	Безперервно	-	Обмеження доступу	Налаштування ролей та ACL для систем, ресурсів
17	VPN	Системний адміністратор	Безперервно	-	Захист віддаленого доступу	Шифрування трафіку, аутентифікація, моніторинг підключень
18	Антивірус	Системний адміністратор	Безперервно	-	Захист від загрозПО	