Міністерство освіти і науки України

Національний технічний університет

«Дніпровська політехніка»

Інститут електроенергетики

Факультет інформаційних технологій

Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеня бакалавра

студента *Грибанова Євгенія Вячеславовича*

академічної групи *125-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка засобів та заходів кіберзахисту веб-сайту підприємства «ТОВ НОВА ПЕЙ»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.е.н., доц. Ткач М.О.			
розділів:				
спеціальний	к.е.н., доц. Ткач М.О.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро

2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Грибанову Євгенію Вячеславовичу*** **академічної групи** ***125-20-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка засобів та заходів кіберзахисту веб-сайту підприємства «ТОВ НОВА ПЕЙ»***

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати комплексні системи захисту інформації веб-сайту підприємства «ТОВ НОВА ПЕЙ»	15.03.24-26.04.24
Розділ 2	Розробит систему захисту інформації в системі веб-сайту підприємства «ТОВ НОВА ПЕЙ»	27.04.24 – 31.05.24
Розділ 3	Розрахунки капітальних витрат, витрат на експлуатацію системи безпеки та термін окупності інвестицій застосування запропонованої системи	01.06.24 – 15.06.24

Завдання видано _____ Ткач М.О.
(підпис керівника)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Грибанов Є.В.
(підпис студента)

РЕФЕРАТ

Пояснювальна записка: 57 с , рис 3, табл 12 , додатків 6 , джерел 6 .

Об'єкт дослідження даної кваліфікаційної роботи – веб-сайт ТОВ НОВА ПЕЙ. Мета полягає у розробці комплексної системи кіберзахисту веб-сайту, спрямованої на запобігання загрозам інформаційної безпеки.

В першому розділі роботи обґрунтовано необхідність створення комплексної системи кіберзахисту (КСКЗ), надано загальну інформацію про об'єкт дослідження та проведено акт обстеження. Також визначено перелік джерел загроз, властивостей та актуальних загроз, які стосуються інформаційно-комунікаційної системи веб-сайту ТОВ НОВА ПЕЙ.

Другий розділ присвячений опису існуючого профілю захищеності та обраного нового профілю захищеності для веб-сайту ТОВ НОВА ПЕЙ. Крім того, розроблено рішення щодо захисту від актуальних загроз, таких як фішинг, SQL-ін'єкції, XSS-атаки, DDoS-атаки та шкідливе програмне забезпечення.

Третій розділ містить розрахунок витрат на впровадження та підтримку заходів забезпечення кібербезпеки. Практична значимість роботи полягає у створенні та впровадженні комплексної системи кіберзахисту, а також у використанні моделей загроз, моделі порушника, вразливостей та інших аспектів, пов'язаних з інформаційною безпекою.

КОМПЛЕКСНА СИСТЕМА КІБЕРЗАХИСТУ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ВРАЗЛИВОСТІ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

Explanatory note: p. 57, figure 3, table 12, appendices 6, sources 6.

The object of research of this qualification work is the website of NOVA PAY LLC. The goal is to develop a comprehensive website cyber protection system aimed at preventing information security threats.

In the first section of the work, the need to create a comprehensive cyber protection system (CSP) is substantiated, general information about the research object is provided, and an inspection report is conducted. A list of sources of threats, properties and current threats related to the information and communication system of the NOVA PAY LLC website is also defined.

The second section is devoted to the description of the existing security profile and the chosen new security profile for the NOVA PAY LLC website. In addition, solutions have been developed to protect against current threats such as phishing, SQL injections, XSS attacks, DDoS attacks and malware.

The third section contains the calculation of costs for the implementation and maintenance of cyber security measures. The practical significance of the work lies in the creation and implementation of a comprehensive cyber protection system, as well as in the use of threat models, the offender model, vulnerabilities and other aspects related to information security.

COMPLEX CYBER PROTECTION SYSTEM, THREAT MODEL, VIOLATOR MODEL, VULNERABILITIES, INFORMATION SECURITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

CSS - Cascading Style Sheets;

DNS - Domain Name System;

HTML - Hyper Text Mark up Language;

HTTP - Hyper Text Transer Protocol;

HTTPS - Hypertext Transfer Protocol Secure;

SMTP - Simple Mail Transfer Protocol;

SSH - Secure Shell;

SQL - Structured query language;

ІТС - Інформаційно-телекомунікаційна система;

КЗЗ - Комплекс засобів захисту;

КСЗІ - Комлпексні системи захисту інформації;

ПЗ - Програмне забезпечення;

СЗІ - Служба захисту інформації.

Зміст

ВСТУП

У сучасному цифровому світі веб-сайти підприємств стали ключовим інструментом для комунікації, представлення продуктів та послуг, а також для забезпечення роботи бізнесу в Інтернеті. Вони відіграють надзвичайно важливу роль у взаємодії з клієнтами, партнерами та іншими зацікавленими сторонами. Однак разом зі зростанням їхньої популярності збільшується й ризик кібератак.

Однією з найважливіших задач власників і адміністраторів веб-сайтів є забезпечення їхньої кібербезпеки. Це стає надзвичайно актуальним у зв'язку з ростом кількості та складності кіберзагроз, спрямованих на веб-ресурси. Навіть найменша вразливість може призвести до серйозних наслідків, таких як втрата даних, порушення конфіденційності або відмова у обслуговуванні.

Кваліфікаційна робота присвячена розгляду засобів та заходів кіберзахисту веб-сайту підприємства ТОВ "НОВА ПЕЙ". Основною метою дослідження є аналіз існуючих вразливостей та загроз, що існують для даного веб-сайту, а також розробка рекомендацій щодо їхнього виправлення та запобігання майбутнім інцидентам. Дана робота базується на практичному досвіді і теоретичних підходах до забезпечення безпеки в інформаційних системах, зокрема в контексті веб-додатків та інтернет-ресурсів.

Розгортання захисту веб-сайту вимагає комплексного підходу, який враховує не лише технічні аспекти, але й правила та процедури управління безпекою. Важливим елементом такого підходу є адаптація заходів до конкретних вимог та особливостей підприємства.

Отже, ця робота має на меті допомогти підприємству ТОВ "НОВА ПЕЙ" підвищити рівень своєї кібербезпеки та зменшити ризики, пов'язані з експлуатацією їхнього веб-сайту.

РОЗДІЛ 1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості

У рамках дипломної роботи проводиться аналіз засобів та заходів кіберзахисту веб-сайту підприємства ТОВ "НОВА ПЕЙ". Цей дослідження становить основу для виявлення потенційних загроз безпеці та виконання вимог стандартів кіберзахисту для веб-сторінок.

На прикладі веб-сайту компанії "НОВА ПЕЙ" аналізуються такі аспекти:

- Карта сайту (сторона користувача): Веб-сайт включає головну сторінку, розділи з корпоративною інформацією, каталог продукції чи послуг, сторінки для авторизації та реєстрації користувачів, а також особисті кабінети з можливістю управління персональними даними та замовленнями.
- Застосовані технології: Аналізуються технології, використовані для розробки веб-сайту, зокрема мови програмування, системи управління базами даних, серверні технології та застосунки, необхідні для функціонування веб-сайту.
- Заходи кіберзахисту: Оцінюються існуючі заходи безпеки, такі як захист від SQL-ін'єкцій, кросс-сайтових скриптів (XSS), зламу паролів, контроль доступу до ресурсів і відповідність стандартам захисту інформації.
- Адміністративна частина: Досліджується організація доступу до адміністративних панелей сайту, права доступу адміністраторів та модераторів, а також засоби моніторингу та аудиту безпеки.

Ця дипломна робота спрямована на підвищення рівня кіберзахисту веб-сайту підприємства ТОВ "НОВА ПЕЙ" шляхом ідентифікації потенційних вразливостей та розробки рекомендацій з їхнього усунення.

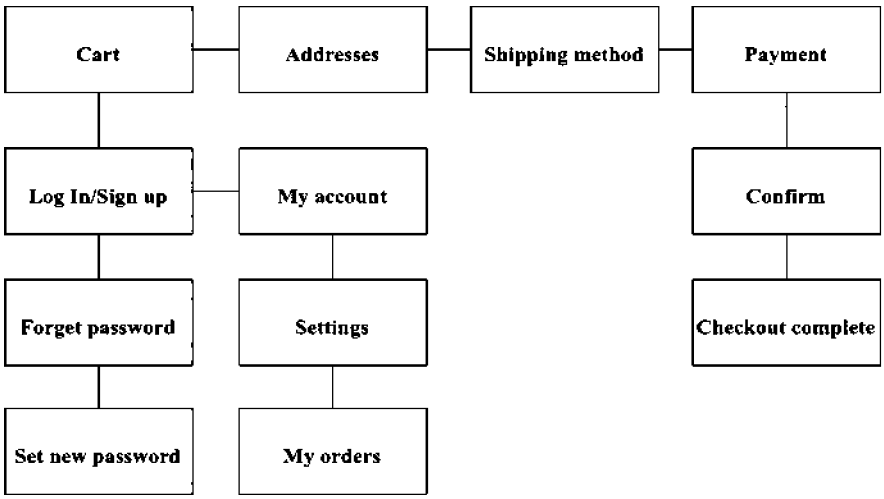


Рисунок 1.1- Карта сайту

1.2 Інформація, що зберігається на сайті

На веб-сайті підприємства ТОВ "НОВА ПЕЙ" зберігається різноманітна інформація, яка має важливе значення для функціонування та обслуговування користувачів. Основні категорії інформації включають:

- Каталог продукції або послуг: Детальна інформація про товари чи послуги, що пропонуються компанією, включаючи опис, технічні характеристики, ціни та наявність.
- Особисті дані користувачів: Інформація, яка введена користувачами під час реєстрації або під час здійснення покупок, така як ім'я, адреса, електронна пошта, інформація про платіжні дані тощо.
- Історія замовлень і статуси: Інформація про історію замовлень користувачів, включаючи активні, завершені або скасовані замовлення, статуси доставки чи виконання.

- Дані авторизації і сесій: Інформація про авторизаційні дані користувачів та деталі сесій, що забезпечують доступ до особистого облікового запису.

Ця інформація має велике значення для бізнес-процесів компанії, однак її збереження та обробка потребують належного захисту для запобігання несанкціонованому доступу та витоку даних. У рамках дипломної роботи буде проведений аналіз рівня захисту цих даних та рекомендації щодо його покращення.

1.3 Актуальні атаки, які можуть використовуватись, та протидія цим атакам

На веб-сайті ТОВ "НОВА ПЕЙ" можуть бути потенційно використані різноманітні типи кібератак, які загрожують конфіденційності та інтегритету інформації користувачів і підприємства. Ось деякі з них:

- Недостатній захист транспортного рівня (Insufficient transport layer protection): Ця атака може бути успішно виконана через використання протоколу HTTP, що не забезпечує шифрування даних під час їх передачі. Для захисту від цієї загрози обов'язково використовувати HTTPS, який забезпечує безпечну передачу усіх даних через шифрування.
- Витік інформації (Information leakage): Ця атака може стати результатом неправильної роботи програмного забезпечення або витоку конфіденційних даних через помилки у логіці програми. Для захисту потрібно ретельно тестувати програмну частину, використовувати системи моніторингу, наприклад, Sentry, для виявлення й усунення таких помилок.
- Кросс-сайтові скрипти (Cross-site scripting, XSS): Це міжсайтове використання скриптів, яке дозволяє зловмисникам внедрювати та виконувати JavaScript-код на браузері користувача. Для захисту від цієї атаки

важливо проводити валідацію та очищення вхідних даних, що надходять на сервер.

- Brute force атаки: Ці атаки полягають в генерації великої кількості спроб вгадування паролів або ідентифікаторів, що дає можливість зловмисникам отримати доступ до системи. Для захисту необхідно використовувати паролі високої складності та механізми обмеження спроб входу.
- Content spoofing: Ця атака передбачає підміну контенту сторінки з метою змусити користувача прийняти фальшивий контент за легітимний. Для захисту від цього типу атак рекомендується уникати використання фреймів і уважно перевіряти всі зовнішні дані перед їх відображенням.
- Cross-site request forgery (CSRF): Атака, що використовується для виконання недозволених дій від імені автентифікованого користувача. Для захисту потрібно використовувати унікальні токени та інші методи перевірки автентичності запитів.

Для зменшення ризиків кібератак рекомендується належно налаштувати систему кіберзахисту, регулярно аудитувати код, використовувати найсучасніші технології шифрування та забезпечувати навчання персоналу з питань кібербезпеки.

1.4 Характеристика веб-сайту

Для досягнення повної карти веб-сайту ТОВ НОВА ПЕЙ з точки зору кібербезпеки, необхідно визначити ключові аспекти, які впливають на безпеку та захист інформації в мережі Інтернет. Ось декілька важливих аспектів, які слід розглянути:

1. Тип і функціональність веб-сайту**:** Веб-сайт ТОВ НОВА ПЕЙ є представницькою платформою для надання інформації про послуги компанії, обміну контактами з клієнтами і можливими партнерами, а також для обробки замовлень і запитів. Враховуючи це, веб-сайт має підтримувати

безпеку персональних даних користувачів, обмежувати доступ до конфіденційної інформації, яка може знаходитися в базі даних компанії.

2. Архітектура і технічні рішення: Веб-сайт може використовувати певну CMS (Content Management System) або бути розробленим на основі власних технічних рішень. Важливо оцінити потенційні слабкі місця в архітектурі, такі як можливість SQL-ін'єкцій, Cross-Site Scripting (XSS) атак, а також оцінити відповідність веб-сайту стандартам безпеки OWASP (Open Web Application Security Project).

3. Захист інфраструктури: Хостинг веб-сайту із забезпеченням необхідного рівня фізичної і мережевої безпеки є важливим аспектом. Веб-сайт ТОВ НОВА ПЕЙ може розміщуватися на віртуальних або фізичних серверах, які повинні бути належним чином захищені від несанкціонованого доступу і зовнішніх атак.

4. Моніторинг і виявлення інцидентів: Важливо мати систему моніторингу безпеки, яка забезпечує вчасне виявлення потенційних загроз і інцидентів безпеки на веб-сайті. Це може включати системи виявлення вторгнень (IDS) і вторгнення (IPS), а також журналювання подій для подальшого аналізу.

5. Аудит і вдосконалення: Регулярні аудити безпеки і оновлення забезпечують, що веб-сайт відповідає сучасним стандартам безпеки і враховує останні уразливості та загрози.

1.4.1 Мова програмування та бібліотеки, що були використані при написанні back-end частини веб-сайту

Back-end частина веб-сайту ТОВ НОВА ПЕЙ реалізована з використанням наступних технологій:

1. Мова програмування: для написання back-end логіки веб-сайту була використана мова програмування Python. Python обрана через її гнучкість, широку підтримку та зручність для розробників. Одним із

ключових виборів Python є його активна спільнота та широкий вибір бібліотек для розв'язання різноманітних завдань, включаючи кібербезпеку.

2. Фреймворк: для побудови back-end частини веб-сайту використовується Django, який забезпечує структурований підхід до розробки, забезпечуючи вбудовану підтримку безпеки та дозволяючи зручне управління базою даних і адміністративні можливості.

3. База даних: В якості основної системи управління базами даних (СУБД) використовується PostgreSQL. PostgreSQL відома своєю надійністю та можливостями захисту даних, такими як розширені можливості шифрування та контроль доступу.

4. Бібліотеки та інструменти для кібербезпеки: При розробці використовуються різноманітні бібліотеки для забезпечення безпеки додатку, такі як:

- Django Security Middleware: Вбудований захисний мідлвар для Django, який дозволяє налаштовувати HTTP заголовки для захисту від різних видів атак, таких як Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) та ін.
- SQLAlchemy: Для безпечної обробки SQL запитів і запобігання SQL ін'єкціям.
- bcrypt: Для забезпечення безпечного зберігання та хешування паролів користувачів.

Використання цих технологій і бібліотек дозволяє забезпечити високий рівень кібербезпеки веб-сайту ТОВ НОВА ПЕЙ, мінімізуючи ризики вразливостей та забезпечуючи безпеку обробки конфіденційної інформації користувачів.

1.4.4 Автентифікація

Автентифікація веб-сайту ТОВ НОВА ПЕЙ забезпечується через сучасні методи та технології, що включають:

- Методи аутентифікації: Веб-сайт використовує стандартні методи аутентифікації, такі як форма логіну і пароль, для перевірки ідентичності користувачів.
- Захист паролів: Паролі зберігаються в захешованому форматі за допомогою алгоритму bcrypt, що забезпечує високий рівень безпеки.
- Двофакторна аутентифікація (2FA): для підвищення безпеки використовується двофакторна аутентифікація, яка вимагає введення додаткового підтвердження після введення пароля.

Ці заходи дозволяють забезпечити високий рівень безпеки та захисту особистих даних користувачів під час автентифікації на веб-сайті.

1.4.5 Авторизація

Авторизація на веб-сайті ТОВ НОВА ПЕЙ реалізована через систему контролю доступу, яка забезпечує обмеження прав доступу користувачів до різних ресурсів на основі їхніх ролей і прав:

- Ролі користувачів: Визначені ролі (адміністратор, модератор, користувач) мають певні права доступу до функціоналу веб-сайту.
- Контроль доступу: Використовується система ACL (Access Control List), яка налаштовується для кожного ресурсу і обмежує доступ лише до необхідної інформації та функціоналу в залежності від ролі користувача.

Це забезпечує конфіденційність даних і запобігає несанкціонованому доступу до чутливої інформації через веб-сайт.

1.4.6 Додаткове програмне забезпечення, яке використовувалось при написанні сайту

Під час розробки веб-сайту ТОВ НОВА ПЕЙ використовувалися додаткові програмні засоби для забезпечення безпеки, ефективності і зручності:

- NGINX: Використовується як веб-сервер для обробки запитів і забезпечення безпеки на рівні мережі.
- Let's Encrypt: Використовується для автоматичного отримання і підтримки SSL-сертифікатів для шифрування трафіку між користувачем і сервером.
- Fail2ban: Інструмент для виявлення потенційних зловмисників і блокування їх IP-адрес за певними правилами.
- Security Headers: Використовуються HTTP заголовки для покращення безпеки веб-додатку, включаючи заголовки Content Security Policy (CSP) і X-Frame-Options.

Ці інструменти допомагають забезпечити високий рівень безпеки, стійкості та ефективності веб-сайту ТОВ НОВА ПЕЙ.

1.4.6.1 База даних

База даних, що використовується для зберігання інформації веб-сайту ТОВ НОВА ПЕЙ, є критичним елементом архітектури додатку. Розглянемо деталі, пов'язані з вибором та налаштуванням бази даних:

- Тип СУБД: В якості основної системи управління базами даних використовується PostgreSQL, яка відома своєю надійністю, масштабованістю та розширеними можливостями безпеки.
- Захист даних: PostgreSQL забезпечує захист даних за допомогою розширених механізмів аутентифікації і контролю доступу (GRANT, REVOKE), а також шифрування даних як на рівні зберігання, так і на рівні передачі даних.

- Резервне копіювання та відновлення: Регулярне резервне копіювання даних здійснюється за допомогою інструментів, таких як pg_dump та pg_basebackup, що дозволяє швидко відновити базу даних у разі виникнення збою або атаки.
- Моніторинг та оптимізація: Використовуються інструменти для моніторингу продуктивності та оптимізації запитів, такі як pg_stat_statements, що дозволяють виявляти та усувати вузькі місця в роботі бази даних.

1.4.6.2 Віртуалізація

Віртуалізація є важливим компонентом інфраструктури веб-сайту ТОВ НОВА ПЕЙ, що забезпечує гнучкість, масштабованість та безпеку:

- Технології віртуалізації: Використовуються популярні платформи віртуалізації, такі як VMware або Hyper-V, для створення ізольованих віртуальних середовищ, в яких працюють компоненти веб-сайту.
- Контейнеризація: Використання Docker для контейнеризації додатків дозволяє забезпечити їх ізоляцію, легке розгортання та масштабування. Контейнери забезпечують ізоляцію від основної операційної системи та інших контейнерів, що підвищує безпеку.
- Оркестрація контейнерів: Використання системи оркестрації контейнерів, такої як Kubernetes, для автоматизації розгортання, управління та масштабування контейнеризованих додатків.

1.4.6.3 Розгортання на віддаленому сервері

Розгортання веб-сайту ТОВ НОВА ПЕЙ на віддаленому сервері включає декілька важливих аспектів для забезпечення надійності та безпеки:

- Хмарні сервіси: Використання хмарних платформ, таких як Amazon Web Services (AWS), Google Cloud Platform (GCP) або Microsoft Azure, забезпечує високу доступність, масштабованість і безпеку інфраструктури.

- CI/CD (Continuous Integration and Continuous Deployment): Впровадження CI/CD процесів для автоматизації розгортання та оновлення додатків. Інструменти, такі як Jenkins або GitLab CI/CD, забезпечують автоматичне тестування, інтеграцію і деплоймент змін коду.
- Безпека передачі даних: Використання SSL/TLS для шифрування трафіку між користувачами та сервером, а також VPN для захищеного доступу до інфраструктури з боку адміністративного персоналу.
- Моніторинг та управління: Інструменти моніторингу, такі як Prometheus та Grafana, дозволяють відстежувати стан системи, продуктивність і виявляти потенційні проблеми на ранніх етапах.

1.5 Інформаційні потоки

Інформаційні потоки на веб-сайті ТОВ НОВА ПЕЙ складаються з різних типів даних, що передаються між клієнтами, сервером та базою даних. Ці потоки включають:

- Клієнт-серверні взаємодії:
  - HTTP/HTTPS запити: Всі взаємодії між клієнтами та сервером здійснюються через захищені протоколи HTTPS для забезпечення конфіденційності та цілісності даних.
  - Форми введення даних: Клієнти можуть вводити особисті дані, які передаються на сервер для обробки, зберігання та подальшої взаємодії.
- Взаємодії між сервером та базою даних:
  - Запити на зчитування: Сервер здійснює запити на зчитування даних з бази даних для відображення інформації на веб-сайті.
  - Запити на запис/оновлення: Сервер також здійснює запити на запис та оновлення даних у базі даних, наприклад, при реєстрації нового користувача або зміні інформації.
- Адміністративні взаємодії:

- Адміністративний інтерфейс: Адміністратори використовують захищений інтерфейс для управління веб-сайтом, редагування контенту, управління користувачами та налаштуваннями.
- Журналювання та моніторинг: Дані про дії адміністративного персоналу та системні події зберігаються у журналах для подальшого аналізу та аудиту.

Ці інформаційні потоки мають бути належним чином захищені для запобігання несанкціонованому доступу, втраті або компрометації даних.

1.6 Персонал, що взаємодіє з адміністративною частиною сайту та його права доступу до основних сутностей, що проводять процеси сайту в дію

Серед усього персоналу підприємства взаємодіє саме з адміністративною частиною сайту:

- адміністратор;
- суперадміністратор;
- контент-менеджер;
- сео-менеджер;
- сейлз-менеджер.

Перелік сутностей до яких адміністративний персонал может мати доступ:

- адреси користувачів (білінгова та шипінгова адреса);
- облікові записи користувачів;
- персональні дані користувачів;
- платіжна інформація користувачів;
- замовлення користувачів;
- адміністратори.

Таблиця 1.2 - Перелік прав доступу

Продовження таблиці 1.2

Умовне позначення права доступу	Пояснення
C	Право на створення
R	Право на читання
U	Право на змінення (запис)
D	Право на видалення

Середовище користувачів:

Таблиця 1.3 - Адміністратор та його права

Назва сутності	Права доступу
Адреса користувача	R
Обліковий запис користувача	DR
Персональні дані користувачів	UR
Платіжна інформація користувачів	R
Замовлення користувачів	R
Адміністратори	R

Таблиця 1.4 - Суперадміністратор та його права

Назва сутності	Права доступу
Адреса користувача	R
Обліковий запис користувача	RU
Відгуки користувачів	RDU
Персональні дані користувачів	UR
Платіжна інформація користувачів	R
Замовлення користувачів	R
Адміністратори	CRUD

Таблиця 1.5 - Контент-менеджер та його права

Назва сутності	Права доступу
Відгуки користувачів	R
Персональні дані користувачів	-
Платіжна інформація користувачів	-
Замовлення користувачів	R
Адміністратори	R

Таблиця 1.6 - Сео-менеджер та його права

Назва сутності	Права доступу
Адреса користувача	-
Обліковий запис користувача	-
Відгуки користувачів	R
Персональні дані користувачів	-
Платіжна інформація користувачів	-
Замовлення користувачів	R
Адміністратори	R

Таблиця 1.7 - Сейлз-менеджер та його права

Назва сутності	Права доступу
Адреса користувача	R
Обліковий запис користувача	R
Відгуки користувачів	R
Персональні дані користувачів	R
Платіжна інформація користувачів	R
Замовлення користувачів	RUD
Адміністратори	R

Окрему роль на сайті має звичайний користувач. Користувача можна розділити на два типи:

- авторизований користувач;
- гість.

Будь-який користувач має можливість переглядати основні сторінки сайту:

1) головна сторінка;
2) сторінка послуг;
3) відгуки;
4) інформація про компанію;

Додатково тільки авторизований користувач має право на такі дії:

1) Додавати опцію або обирати;
2) Переглядати тільки власні дії;
3) Залишати відгуки;
4) Переглядати налаштування персонального облікового запису на сайті;
5) Редагувати дані персонального облікового запису на сайті;
6) Створювати замовлення;
7) Переглядати особисті замовлення та їх статус.

1.7 Висновок

В ході дослідження було розглянуто ключові аспекти кібербезпеки веб-сайту ТОВ НОВА ПЕЙ, включаючи:

- Технічні засоби та методи: Використання сучасних мов програмування, фреймворків та бібліотек для забезпечення безпеки back-end частини веб-сайту.
- Автентифікація та авторизація: Впровадження надійних методів автентифікації та контролю доступу для захисту від несанкціонованого доступу.

- Інфраструктура: Використання віртуалізації, контейнеризації та хмарних сервісів для гнучкості, масштабованості та безпеки.
- Інформаційні потоки: Забезпечення безпеки передачі даних між клієнтами, сервером та базою даних.
- Персонал та права доступу: Регулювання доступу до адміністративної частини веб-сайту для запобігання несанкціонованим діям та захисту конфіденційної інформації.

Ці заходи дозволяють забезпечити високий рівень безпеки веб-сайту ТОВ НОВА ПЕЙ, захистити персональні дані користувачів та підтримувати надійність та доступність системи.

РОЗДІЛ 2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості

В даному розділі на прикладі WEB-сторінки, що розглядається буде:

- проведений аналіз загроз;
- складена модель загроз та порушника;
- проведене тестування на реалізацію знайдених загроз;
- складений профіль захищеності Т2 системи посилаючись на «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» НД ТЗІ 2.5010;
- проведена реалізація системи захисту;
- повторне тестування на реалізацію визначених загроз.

2.2 Модель порушника

Модель порушника - це формальний або неформальний опис дій порушника, який відображає його практичні та теоретичні можливості, його знання, час і місце дії можливого порушення. Як порушника ми розглядаємо особу, що може одержати несанкціонований доступ до інформації, що зберігається на сайті.

Модель порушника повинна визначати:

- можливі цілі порушника за ступенем небезпечності для WEB-сторінки та інформації, що потребує захисту;
- гіпотеза про кваліфікацію порушника;
- умовивід про характер дій можливого порушника;

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі в подальшому для використання в особистих цілях;
- здобути можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;
- нанесення збитків шляхом знищення інформаційних

цінностей сайту.

Базово можливі порушники поділяються на дві основі групи: зовнішні та внутрішні.

До зовнішніх можливих порушників WEB-сторінки, що розглядається відноситься будь-який користувач сайту (гість або авторизований користувач), який може намагатися підібрати паролі до облікових записів інших користувачів або намагатися провести SQL-ін'єкції та інші види відомих атак.

До внутрішніх можливих порушників WEB-сторінки, що розглядається відносяться будь-який персонал адміністративної частини сайту, так як майже усі ролі адміністративного персоналу мають доступ до читання майже усіх даних, що зберігаються на сайті. Також до внутрішніх порушників відносяться активні в даний час розробники сайту (сайт на даний час вже є працюючим, тому розробники приймають участь у програмній підтримці додатку), які мають права суперадміні- страторів та єдині особи, які мають доступ до повної програмної і серверної частини WEB-сторінки включаючи доступ до йоскег-контейнерів проекту, що знаходяться на інстансу (повний обсяг даних додатку і всіх його частин на віддаленому сервері) через мережевий протокол 88Н. Окремо потрібно виділити тестувальни- ків, які у цілях тестування повинні перевірити весь обсяг функціоналу усіх користувачів на всіх сторінках та оболонках додатку, маючи при цьому права одночасно всіх ролей, так як функціонал адміністративної частини сайту також потребує перевірки на наявність будь-яких помилок та розбіжностей у специфікації та актуального функціоналу сайту.

2.2.1Специфікація моделі порушника

2.2.1.1 Специфікація моделі порушника за мотивом здійснення можливого порушення

- MI - Безвідповідальність (не розуміння наслідків під час скоєння будь- якого порушення)

- М2 - Самоствердження (порушник намагається довести собі або оточуючим чого він/вона вартий)

- М3 - Корисливий мотив (метою порушення виступає особиста невідома вигода)

2.2.1.2 Специфікація моделі порушника за рівнем кваліфікації та обізнаності

- К0 - Не знає функціональної особливості системи, основні закономірності формування даних та запитів, які приходять до WEB-сторінки;

- К1 - Знає функціональні особливості системи, основні закономірності формування даних та запитів, які приходять до WEB-сторінки;

- К2 - Володіє високим рівнем обізнаності основних технічних і програмних засобів роботи WEB-сторінки, слабке розуміння параметрів, що працюють із запитами, що приходять до WEB-сайту;

- К3 - Володіє усією інформацією, що пов'язана з роботою WEB-сторінки, запитами, які приходять до WEB-сайту, параметрами і функціональною частиною додатку.

2.2.1.3 Специфікація моделі порушника за місцем дії

Дана специфікація моделі порушника не є актуальною для даного виду «об'єкту» ІТС, так як це WEB-сайт. Доступ до WEB-сайту доступний будь-якому користувачу з будь-якого девайсу і будь-якої частини світу через вихід до Інтернету. Доступ до адміністративної частини сайту надається лише авторизованим адміністраторам та їх суміжним ролям також через вихід до Інтернету з будь- якої частини світу, з будь-якого девайсу. Аналогічна ситуація є і з доступом docker-контейнерів в актуальних розробників сайту.

2.2.1.4 Специфікація моделі порушника за часом дії:

- 41 - у робочий час під час робочого тижня, коли реагування на будь-яку атаку найшвидше;

- 42 - на вихідних, коли реагування на будь-яку атаку буде менш швидким;

- 43 - у неробочий час (вночі) у робочі дні або на вихідних, коли реагування на будь-яку атаку буде найменш швидким.

Реагування на атаку на сайті проводиться через логування будь-яких дій на сервері, базі даних. Якщо під час обробки запиту на сервер або до бази даних виникає помилка або проводиться спроба будь-яких із відомих атак, сервер відправляє нотифікацію (повідомлення) до закритого каналу сповіщень корпоративного мессенджера Slack з текстом про помилку або іншу видиму проблему у додатку та посиланням на зовнішній ресурс Sentry. Цей ресурс спеціально налаштований для подібних проблем, в ньому розкриваються усі помилки або проблеми, які виникли при роботі сайту з повним розширенням і текстом (навіть з номер рядку у коді, де виникла помилка, якщо помилка виникла на сервері). Також при виникненні подібних ситуацій одночасно відправляється таке саме повідомлення усім адміністраторам, суперадміністраторам та розробникам сайту.

Так як користування сайтом може проходити у будь-який час та звідусіль, найбільш вразливим часом буде проміжок з 10 години вечора по 8 ранку, коли реагування на повідомлення з легуванням буде найменш успішним і результативним через людський фактор.

2.2.1.5 Специфікація моделі порушника за показником можливості подолання системи захисту інстансу

Для того, щоб отримати доступ до середовища додатку на віддаленому сервері і взаємодіяти з docker-контейнерами WEB-сайту використовується мережевий протокол SSH. Для встановлення зв'язку клієнт-сервер є два варіанти:

- клієнт має збережений на своїй локальній машині приватний ключ сервера, до якого клієнт намагається під'єднатись з допомогою протоколу SSH;

- публічний ключ клієнта записаний в список дозволених хостів на віддаленному сервері, до якого клієнт намагається під'єднатись з використанням SSH.

Посилаючись на такі дані можна визначити такі специфікації моделі порушника за даним типом:

- ЗО - не має збереженого на локальній машині приватного ключа сервера і на сервері в дозволених хостах публічний ключ даного клієнта - відсутній;

- 31 - має збережений на локальній машині приватний ключ сервера або на сервері в дозволених хостах записаний публічний ключ даного клієнта.

2.2.1.6 Модель порушника зовнішнього типу

Таблиця 2.1 - Модель порушника зовнішнього типу

Роль по відношенню до сайту	Мотив	Кваліфікація	Можливість обійти захист	Час дії	Сума загроз
Гість	МІ	КО	ЗО	43	4
Авторизований користувач	М2	КО	ЗО	43	5
Конкурент	М3	К2	ЗО	41	6
Хакер	М3	КЗ	ЗО	43	9

Таблиця 2.2 - Модель порушника внутрішнього типу

Роль по відношенню до сайту	Мотив	Кваліфікація	Можливість обійти захист	4ас дії	Сума загроз
Суперадміністратор	М3	КЗ	31	43	10
Адміністратор	М2	К2	ЗО	42	6
Сео-менеджер	М2	К1	ЗО	41	4
Сейлз-менеджер	М2	К1	ЗО	41	4
Контент-менеджер	М2	К1	ЗО	41	4

Окремими моделями порушника виступають актуальні розробники і

тесту- вальники сайту. По оцінкам модель порушника для цих ролей:

- розробник - має роль суперадміністратора, тому сума загроз для цієї моделі дорівнює 10;

- тестувальник - має одночасно всі ролі (переназначаються кожну ітерацію тестування), максимальну суму загроз має роль суперадміністратора, тому прирівнюємо дану оцінку і тестувальнику (10).

2.3 Модель загроз та вразливостей

2.3.1 Властивості інформації

- К - Конфіденційність - властивість інформації, що гарантує доступ до інформації лише авторизованим особам;

- Ц - Цілісність - властивість інформації, що гарантує можливість модифікації інформації лише авторизованим особам;

- Д - Доступність - властивість інформації, що гарантує доступ до інформації лише авторизованим користувачам не очікуючи довше заданого інтервалу часу.

Таблиця 2.3 - Коефіцієнти можливості реалізації загрози

Коефіцієнт реалізації загрози	Опис
1	Майже неможливо
2	Малоймовірно
3	Можливо, але недоцільно
4	Можливо та доцільно
5	Висока ймовірність

Таблиця 2.4 - Оцінка критичності наслідків реалізації загрози

Коефіцієнт реалізації загрози	Опис
1	Не критичні
2	Низька критичність
3	Середня критичність
4	Висока критичність
5	Неймовірна висока критичність

2.3.2 Перелік загроз

Таблиця 2.5 - Загрози з визначенням порушень властивостей інформації

Опис загрози	Джерело загрози	Наслідки	Порушення	Коефіцієнт можливості реалізації	Критичність наслідків	Оцінка загрози
Підбір приватного ключа від інстансу	Зовнішнє	Порушник має доступ до всіх сіоскег-контейнерів. Порушник може змінити налаштування доступів для інших ад мі ні стративних користувачів	К,Ц,Д	1	5	6

Продовження таблиці 2.5

Опис загрози	Джерело загрози	Наслідки	Порушення	Коефіцієнт можливості реалізації	Критичність наслідків	Оцінка загрози
Підбір логіну та паролю одного із авторизованих користувачів	Зовнішнє	Порушник має доступ до одного із облікових записів сайту (персональні дані, платіжна інформація). Сайт втрачає клієнта і репутація, як сайту, що є безпечним.	К	1	3	4
Навмисна передача конфіденційних даних адміністративної частини сайту або особистих даних користувачів	Внутрішнє	Фінансові втрати як у підприємства так і користувачів сайту	К,Ц	4	5	9
Випадкове видалення деяких даних з адміністративної частини сайту	Внутрішнє	Тимчасова втрата існуючого товару або замовлень клієнтів з даних сайту	ДД	3	2	5
Перехоплення даних під час передавання	Зовнішнє	Дані, що передаються під час запитів до сайту можуть бути перехоплені	К,Ц	1	4	5

Продовження таблиці 2.5

Опис загрози	Джерело загрози	Наслідки	Порушення	Коефіцієнт можливості реалізації	Критичність наслідків	Оцінка загрози
Витік інформації	Внутрішнє	Через відсутність ретельного тестування дорелізного продукту, до production середовища потрапляє функціонал з витоком даних, що може призвести до колосальних збитків	К,Ц,Д	2	5	7
Міжсайтове скриптування	Зовнішнє	Через несвоєчасу очистку даних з прийманих запитів, можно проводити підбір даних для заповнення форми або використовувати дану атаку для спаму	К,Ц	2	4	6

Посилаючись на зібрані дані, щодо загроз, які можуть бути реалізовані на сайті, найбільш критичною загрозою є навмисна передача адміністративних даних додатку третім особам з боку персоналу з адміністративними правами. Для запобігання і зменшення ризику реалізації цієї загрози потрібно більш чітко розмежувати права доступу між ролями адміністративного персоналу, так як більша частина всього персоналу має право на читання усіх даних, що зберігаються на сайті.

Для запобігання передачі приватного ключа інстансу третім особам від розробників, найкращим варіантом буде - не використання приватного ключа для доступа до інстансу через мережевий протокол 88H. Замість цього на ісінтансі додати в список хостів додати публічні ключі всіх авторизованих членів персоналу, яким дозволений вхід до інстансу через 88H.

2.4 Тестування веб-сайту на програмні вразливості за допомогою спеціальних інструментів, таких як OWASP ZAP та Burp Suite

Вступ до тестування на вразливості

Тестування на програмні вразливості є критичним етапом у забезпеченні кібербезпеки веб-сайту. Воно дозволяє виявити потенційні загрози та уразливості, що можуть бути використані зловмисниками для несанкціонованого доступу або компрометації системи.

Інструменти для тестування

OWASP ZAP (Zed Attack Proxy)

OWASP ZAP є одним із найбільш популярних інструментів для тестування безпеки веб-додатків, розробленим проєктом Open Web Application Security Project (OWASP). ZAP використовується для виявлення уразливостей шляхом перехоплення та аналізу HTTP/HTTPS трафіку.

Основні функції OWASP ZAP:

- Перехоплення трафіку**:** Аналіз трафіку між клієнтом і сервером для виявлення можливих уразливостей.
- Автоматичне сканування: Виявлення загальних уразливостей, таких як SQL-ін'єкції, XSS (Cross-Site Scripting) та інші.
- Фаззинг: Генерація випадкових даних для виявлення нестандартних поведінок додатку.
- Інтеграція з CI/CD: Можливість інтеграції з інструментами безперервної інтеграції та доставки.

Burp Suite

Burp Suite є комплексним інструментом для тестування безпеки веб-додатків, розробленим компанією PortSwigger. Він пропонує широкий спектр інструментів для мануального та автоматичного тестування на вразливості.

Основні функції Burp Suite:

- Proxy: Перехоплення і модифікація HTTP/HTTPS трафіку між браузером та веб-додатком.
- Scanner: Автоматичне сканування веб-додатків для виявлення уразливостей.
- Intruder: Інструмент для автоматизованого тестування параметрів і виявлення вразливих місць.
- Repeater: Інструмент для ручного повторення та модифікації окремих запитів.
- Extender: Можливість розширення функціоналу за допомогою додаткових модулів.

Процес тестування

1. Підготовка до тестування:

a. Встановлення та налаштування OWASP ZAP та Burp Suite.

b. Конфігурація проксі-сервера для перехоплення трафіку.

2. Автоматичне сканування:

a. Виконання автоматичного сканування за допомогою OWASP ZAP та Burp Suite для виявлення загальних уразливостей.

3. Ручне тестування:

a. Використання модулів Proxy, Repeater та Intruder в Burp Suite для ручного аналізу та тестування специфічних частин веб-додатку.

4. Аналіз результатів:

a. Оцінка знайдених вразливостей, класифікація за критичністю та підготовка звіту.

Звітування та виправлення

Створення звіту: Документування знайдених вразливостей, включаючи деталі про методи експлуатації та можливі наслідки.

Рекомендації щодо виправлення: Надання рекомендацій для розробників щодо виправлення знайдених уразливостей.

2.5 Повторне тестування веб-сайту на програмні вразливості після внесення змін

Важливість повторного тестування

Повторне тестування, або ретестинг, є важливим етапом процесу забезпечення безпеки веб-сайту. Він дозволяє перевірити ефективність виправлень та забезпечити, що всі знайдені вразливості були належним чином усунені.

Процес повторного тестування

1. Внесення змін:
   - Розробники вносять виправлення, базуючись на звітах та рекомендаціях, наданих після первинного тестування.
2. Оновлення середовища тестування:
   - Розгортання оновленого веб-сайту в тестовому середовищі для проведення повторного тестування.
3. Повторне автоматичне сканування:
   - Виконання автоматичного сканування за допомогою OWASP ZAP та Burp Suite для перевірки виправлених вразливостей.
4. Ручне тестування:
   - Проведення ручного тестування для перевірки специфічних частин веб-додатку та підтвердження усунення вразливостей.
5. Аналіз результатів повторного тестування:
   - Оцінка результатів повторного тестування, підтвердження усунення вразливостей або виявлення нових проблем.
6. Звітування:
   - Створення звіту про результати повторного тестування, включаючи підтвердження усунення знайдених раніше вразливостей та рекомендації щодо подальших дій.

- Постійний процес забезпечення безпеки

- Регулярне тестування: Впровадження регулярного тестування безпеки в процесі розробки та експлуатації веб-додатку.
- Інтеграція в CI/CD: Інтеграція інструментів тестування безпеки з CI/CD процесами для автоматичного виявлення та виправлення вразливостей на ранніх етапах розробки.

2.6 Профіль захищеності

Для обраного веб-сайту, використовуючи технології, такі як OWASP ZAP та Burp Suite, профіль захищеності визначено за допомогою наступних параметрів:

КА-2 (Базова адміністративна конфіденційність)

Реалізовано за допомогою OWASP ZAP та Burp Suite. Ця функція дозволяє адміністратору безпеки регулювати доступ користувачів до інформації із захищених об'єктів. Загальнодоступна інформація є відкритою для всіх категорій користувачів, тоді як доступ до захищених об'єктів регулюється атрибутами доступу, встановленими адміністратором безпеки.

КВ-1 (Конфіденційність при обміні)

Забезпечується за допомогою SSL/TLS, що захищає дані під час їх передачі через незахищене середовище. OWASP ZAP і Burp Suite дозволяють виявляти уразливості в реалізації конфіденційності при обміні даними.

ЦА-1 (Мінімальна адміністративна цілісність)

Забезпечено контроль цілісності даних, що передаються між користувачами та захищеними об'єктами веб-сайту. Політика цілісності стосується всіх категорій користувачів і забезпечується програмними засобами для виявлення та запобігання несанкціонованих змін даних.

ЦО-1 (Відкат)

Реалізовано за допомогою функцій резервного копіювання бази даних та можливостей відкату змін через систему контролю версій, як-от Git. Це

дозволяє відновити дані до попереднього стану у випадку виникнення помилок або інших інцидентів.

ЦВ-1 (Мінімальна цілісність при обміні)

Забезпечується механізмами верифікації цілісності даних, що передаються між веб-сервером і клієнтськими пристроями. OWASP ZAP та Burp Suite допомагають виявляти і запобігати атакам на цілісність даних під час їх передачі.

ДВ-1 (Відновлення після збоїв)

Забезпечено резервним копіюванням даних і механізмами відновлення через Git, що дозволяє повернути систему до відомого захищеного стану після збоїв або помилок.

ДР-1 (Використання ресурсів)

Контролюється використання ресурсів веб-сайту за допомогою контейнеризації з використанням Docker, що дозволяє обмежувати доступ до обчислювальних ресурсів і запобігати їх перевантаженню.

НР-2 (Реєстрація)

Реалізовано веденням журналу всіх подій, що мають відношення до безпеки, зокрема спроби входу/виходу, зміну атрибутів доступу, модифікацію даних та інші критичні події.

НИ-2 (Ідентифікація і автентифікація)

Реалізовано за допомогою механізмів, що дозволяють визначити і перевірити особу користувача, який намагається одержати доступ до захищених об'єктів веб-сайту.

НК-1 (Достовірний канал)

Забезпечує встановлення достовірного каналу зв’язку між користувачем і системою безпеки, гарантуючи, що жодна взаємодія не може бути змінена іншим користувачем або процесом.

НО-1 (Розподіл обов’язків)

Реалізовано шляхом визначення ролей і категорій користувачів з

конкретними повноваженнями, що дозволяє зменшити ризик від помилкових або зловмисних дій.

НЦ-1 (Цілісність комплексу засобів захисту)

Визначає механізми контролю цілісності компонентів системи захисту, забезпечуючи взаємодію між різними засобами захисту та дотриманням політики цілісності.

НТ-1 (Самотестування)

Реалізовано за допомогою автоматизованих тестів і інструментів безперервної інтеграції, як-от CircleCI, що забезпечують перевірку правильності функціонування системи та її компонентів.

НВ-1 (Ідентифікація і автентифікація при обміні)

Забезпечує взаємну ідентифікацію компонентів системи перед початком взаємодії, гарантує, що обмін даними відбувається між достовірними суб'єктами.

Профіль захищеності веб-сайту включає комплекс заходів і інструментів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, а також на виявлення та усунення можливих уразливостей.

2.7 Висновок

У другому розділі кваліфікаційної роботи були складені модель можливого порушника та модель загроз, ґрунтуючись на ролях персоналу адміністративної частини, які були розглянуті у першому розділі.

Проведено тестування для виявлення програмних вразливостей у коді веб-сайту ТОВ "Нова Пей". Посилаючись на знайдені вразливості, було описано алгоритм чіткого виправлення всіх попереджень. Після виправлення цих попереджень було досягнуто покращення в коді та оновлено основні бібліотеки, на яких базується робота додатку.

Крім того, був складений профіль захищеності веб-сайту з використанням відповідних технологій, а також розроблено план реалізації політики захисту для нереалізованих функцій профілю захищеності. Ці заходи сприятимуть підвищенню рівня безпеки веб-сайту та забезпеченню захисту даних користувачів.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Розробка засобів захисту інформації для веб-сайту потребує економічного обґрунтування, базуючись на аналізі витрат на розробку та впровадження. Тому метою економічного розділу є проведення розрахунків, які дозволять визначити економічний ефект від впровадження та налаштування комплексних засобів захисту інформації для веб-сайту.

3.1 Розрахунок капітальних витрат

Капітальні витрати – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

– вартість розробки проекту інформаційної;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Розрахунок вартості розробки КСЗІ здійснюється з використанням двох показників – трудомісткості розробки КСЗІ і витрат на її розробку.

Трудомісткість буде розраховуватися за формулою:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д} \text{ годин}, \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку КСЗІ складає 30 год.;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації складає 30 год.;

$t_{а}$ – тривалість процесу аналізу ризиків 22 год.;

tвз – тривалість визначення вимог до заходів, методів та засобів захисту 21 год.;

tозб – тривалість вибору основних рішень з забезпечення безпеки інформації 12 год.;

товр – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації 9 год.;

tд – тривалість документального оформлення політики безпеки 8 год.

$$t = 30+30+22+21+12+9+8 = 132 \text{ годин.}$$

3.2 Розрахунок витрат на створення елементів КСЗІ

Витрати на розробку елементів КСЗІ

Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки КСЗІ З мч:

$$Крп = Ззп + Змч \quad (3.2)$$

$$Крп = 33000 + 788,04 = 33788,04 \text{ грн.}$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) і визначається за формулою:

$$Ззп = t * Зіб \text{ грн.} \quad (3.3)$$

$$Ззп = 132 * 250 = 33000 \text{ грн,}$$

де t - загальна тривалість розробки політики безпеки, годин;

Зіб - средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

132 - годин на розробку елементів КСЗІ;

250 - заробітна плата грн/годину;

Вартість машинного часу для розробки КСЗІ на ПК визначається за формулою:

$$Змч = t * Смч, \text{ грн.} \quad (3.4)$$

$$Змч = 132 * 5,97 = 788,04 \text{ грн,}$$

де t - трудомісткість розробки КСЗІ на ПК, годин;

Смч - вартість 1 години машинного часу ПК, грн./година.

Смч = Р * tнал * Се + (Фзал * На)/Fр + (Клпз * Напз)/Fр, грн. (3.5)

Смч =0,9 * 3 * 2,64 +(3800*0,4)/ 2160+ (20000*0,2)/ 2160= 9,68 грн/год,

де Р - встановлена потужність ПК, кВт; Р – 0,9 кВт

tнал – кількість задіяних роб.станцій при створенні КСЗІ; tнал – 1;

Се – тариф на електричну енергію, грн/кВт година; Се – 2,64 грн/кВт год;

Фзал – залишкова вартість ПК на поточний рік, грн.; Фзал – 3800 грн;

На – річна норма амортизації на ПК, частки одиниці; На – 0,4;

Напз – річна норма амортизації на ліцензійне програмне забезпечення,частки одиниці; Напз – 0,2;

Клпз – вартість ліцензійного програмного забезпечення, грн.; Клпз – 20000 грн

Fр – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 2160).

3.3 Капітальні (фіксовані) витрати.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

К = Кпр + Кзпз + Кпз + Каз + Кнавч + Кн (3.6)

К = 33788,04+80000+50000= 163 788,04 тис. грн,

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн; сторонні організації не залучалися, коефіцієнт не враховано.

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ) для тестування веб-сайту, тис.грн; необхідно придбати OWASP ZAP, Burp Suite. Ціна ліцензії буде коштувати 80 000 грн.

Крп – вартість розробки політики безпеки інформації- 0грн;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів- 0 грн;

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;– 50 000 грн.

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. Не враховано.

3.4 Розрахунок експлуатаційних витрат

Експлуатаційні витрати - це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі. Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = Св + Ск + Сак, \text{ тис. грн.} \quad (3.7)$$

$$С = 949\ 126 + 500\ 000 = 1\ 449\ 126 \text{ грн},$$

де Св –відновлення системи інформаційної безпеки 500 000 грн

Сак - витрати, викликані активністю користувачів системи інформаційної безпеки;Сак – 0 грн.

Ск - витрати на керування системою в цілому, складають:

$$Ск = Сн + Са + Сз + Сєв + Сел + Со + Стос \text{ грн}, \quad (3.8)$$

$$Ск = 8000+494+303600+66792+570240 = 949\ 126 \text{ грн},$$

де Сн – витрати на навчання адміністративного персоналу й кінцевих користувачів; Сн –8000грн;

Со – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування; Со – 0 грн;

Стос – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки, визначається у відсотках від вартості капітальних витрат (1-3%); Стос – 494 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, складає:

$$Сз = Зосн + Здод, \text{ грн.} \quad (3.9)$$

$$Сз = 22000*12 +2300*12 = 303600 \text{ грн},$$

де Зосн, Здод – основна і додаткова заробітна плата відповідно, грн. на рік.

$$Сєв = 303600*0,22 = 66792.$$

Зосн – 23000 грн на місяць, Здод – 10 відсотків від Зосн, тому Здод – 2300 грн.

Сел – вартість електроенергії, визначається

$$Сел = P * Fp * Це, грн. \quad (3.10)$$

$$Сел = 100 * 2160 * 2,64 = 570\ 240 грн.$$

де P – встановлена потужність апаратури інформаційної безпеки, кВт;(P = 100 кВт)

Fp – річний фонд робочого часу системи інформаційної безпеки; (Fp = 2160 год.)

Це – тариф на електроенергію, грн/кВт*годин; (Це = 2,64 грн/кВт за год.)

3.5 Оцінка величини збитку

$$U = Пп + Пв + V \quad (3.11)$$

$$U = 40000+148300+437500 = 625800 грн,$$

де Пп - оплачувані втрати робочого часу та простої співробітників атакованого веб сайту, грн; Пп – 40000 грн.;

Пв - вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн; Пв – 148300 грн.;

V - втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн. V – 145833 грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$Пп = (\Sigma Зс/F)*tп, грн. \quad (3.12)$$

$$Пп = (800000/180)*9 = 40000 грн,$$

де Зс – загальна кількість витрат на заробітну плату співробітників за місяць, Зс – 800000 грн;

F – місячний фонд робочого часу, F – 180 год.;

tп – час простою внаслідок атак, tп – 9 год.

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$Пв = Пви + Ппв + Пзч, \quad (3.13)$$

де Пви – витрати на повторне уведення інформації, грн.;

Ппв – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Пзч – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви:

$$Пви = (ΣЗс/F)*tви \quad (3.14)$$

$$Пви = (80000/180)*18 = 8000 грн.$$

Витрати на відновлення вузла або сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки tв і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$Ппв=(ΣЗо/F)*tв, \quad (3.15)$$

де Зо = заробітна плата системного адміністратора, 23000 грн на місяць;

F – місячний фонд робочого часу (при 45 годинному робочому тижні становить 180 ч.);

tв = 18 годин повторного введення загубленої інформації унаслідок атаки;

$$Ппв =(23000/180)*18 = 2300 грн.$$

Пзч – вартість заміни устаткування або запасних частин складає 138000 грн.

$$Пв = 8000 + 2300 + 38000 = 48300 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = (O/Fr)*(tп + tв + tви), \quad (3.16)$$

$$V= (21000000/2160)*(9+18+18) = 437500 \text{ грн,}$$

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, О –21 000000 грн у рік;

Fг – річний фонд часу роботи організації; Fr – 2160 год.

tп – час простою вузла унаслідок атаки; tп – 9 год.;

tви = час відновлення після атаки персонало, що обслуговує корпоративну мережу; tви – 18 год.;

tв = час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі; tв – 18 год.

Таким чином, загальний збиток від атаки складе:

$$В= \Sigma i \, \Sigma n*U \quad (3.17)$$

$$В=4*3*437500= 5\ 250\ 000 \text{грн,}$$

де і – кількість атакованих вузлів; і – 4;

n – кількість прогнозованих атак на рік; n – 3 ;

3.6 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$Е = В * R- С, \quad (3.18)$$

де В – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E= 5\ 250\ 000*0,5 – 1\ 449\ 126 = 1\ 175\ 874 \text{ грн.}$$

3.7 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = E/K, \text{ частки одиниці.} \quad (3.19)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн. Коефіцієнт повернення інвестицій ROSI:

$$ROSI = = 1\ 175\ 874 /163\ 788,04 =7,18$$

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$To = K/E = 1/ROSI = 1/7,18= 0,14 = 51,1 \text{ день.}$$

3.8 Висновок

За результатами проведеного розрахунку економічної частини виявлено, що капітальні витрати становлять 163 788,04 грн, а експлуатаційні витрати - 1 449 126 грн. Було встановлено, що загальний збиток, спричинений атакою на вузол або сегмент веб сайту, складає 5 250 000 грн. Загальний ефект від впровадження системи інформаційної безпеки оцінюється в 1 175 874 грн.

Згідно з коефіцієнтом ROSI, який дорівнює 0,14 можна стверджувати, що створені елементи політики безпеки є повністю обґрунтованими. Термін окупності елементів політики безпеки складає 51 робочий день.

ВИСНОВКИ

Проаналізовані потенційні загрози, які можуть виникнути через виявлені уразливості. Розроблено заходи захисту від несанкціонованого доступу до інформації, що зберігається на сайті, з використанням програмних засобів, що використовувалися під час розробки проекту і залишаються актуальними.

Проведений детальний аналіз потенційних загроз та створена модель потенційного порушника. Проведене тестування, програмної частини сайту на виявлення вразливостей за допомогою спеціальних програмних інструментів і бібліотек. Розроблені рекомендації для запобігання можливим загрозам.

Виявлені вразливості в програмному коді проекту виправлені, після чого проведене повторне тестування для перевірки їх відсутності. За результатами тестування підтверджено ефективність виправлень.

Також був проведений розрахунок щодо доцільності впровадження запропонованих організаційних та програмних рішень, що підкріплює необхідність і ефективність запропонованих заходів забезпечення безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Hacking Exposed Web Applications, Third Edition by Joel Scambray, 2003. 384 с;

2. Онлайн платформа систему контролю версій та зберігання репозиторіїв бібліотек і проектів [Електронний ресурс] - https://github.com (до наданого посилання додається назва програмної бібліотеки, яка використовувалась);

3. Національний стандарт НД ТЗІ 1.6-005-2013 "Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці".

4. Національний стандарт НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу".

5. Сайт ТОВ НОВА ПЕЙ [Електронний ресурс] Режим доступу до ресурсу: https://novapay.ua/

6. Національний стандарт НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".

7. Андерсон Р., Безпека Інформаційних Систем. Київ: Діалектика, 2007. 456с.

8. Смирнов В. А., "Аналіз сучасних загроз інформаційній безпеці веб-додатків," Інформаційні технології та засоби захисту, том 3, № 1, с. 45-59, 2020.

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	1	
5	А4	1 Розділ	16	
6	А4	2 Розділ	16	
7	А4	3 Розділ	9	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	1	

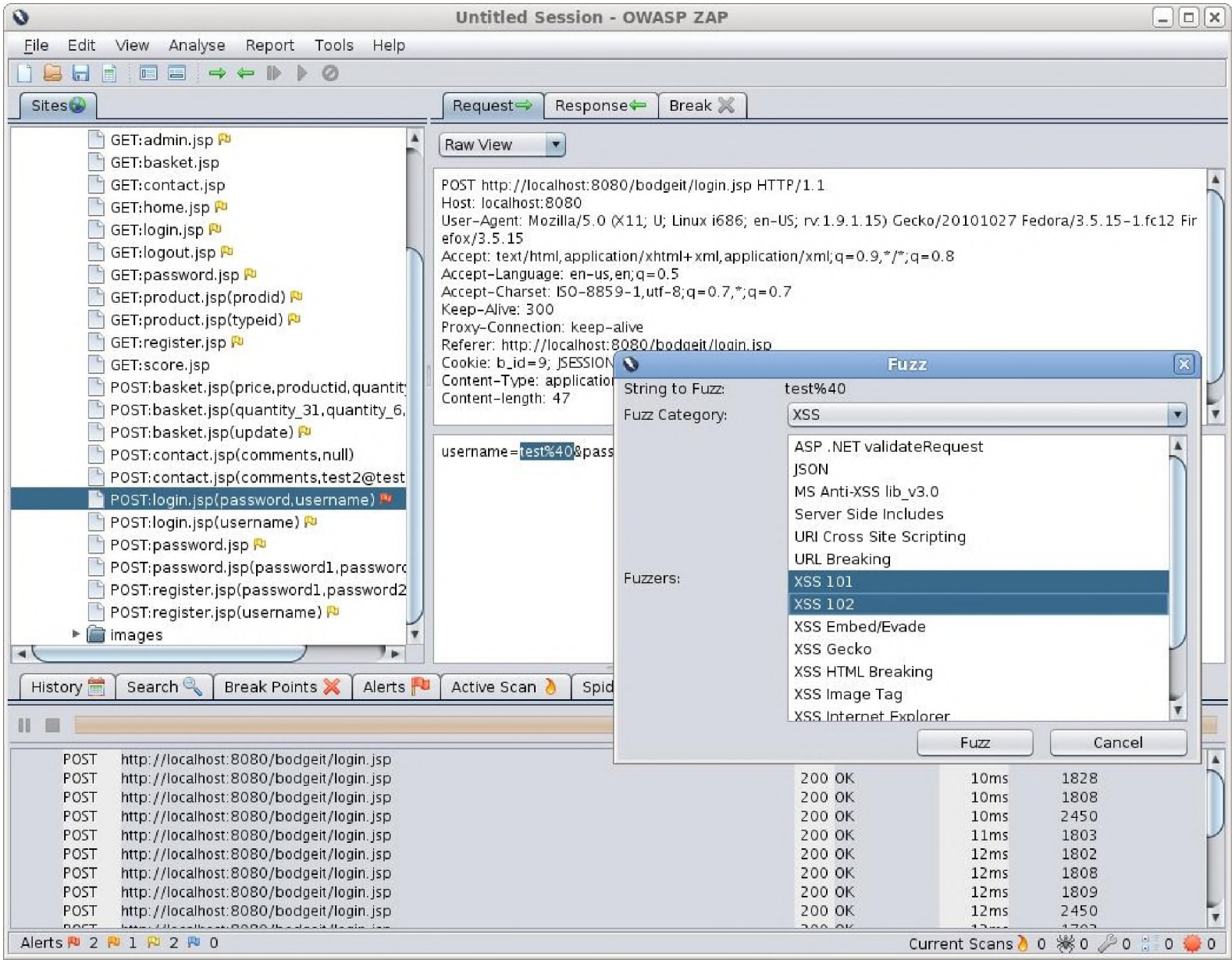
ДОДАТОК Б. ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ

Грибанов Є.В. 125-20-2.docx

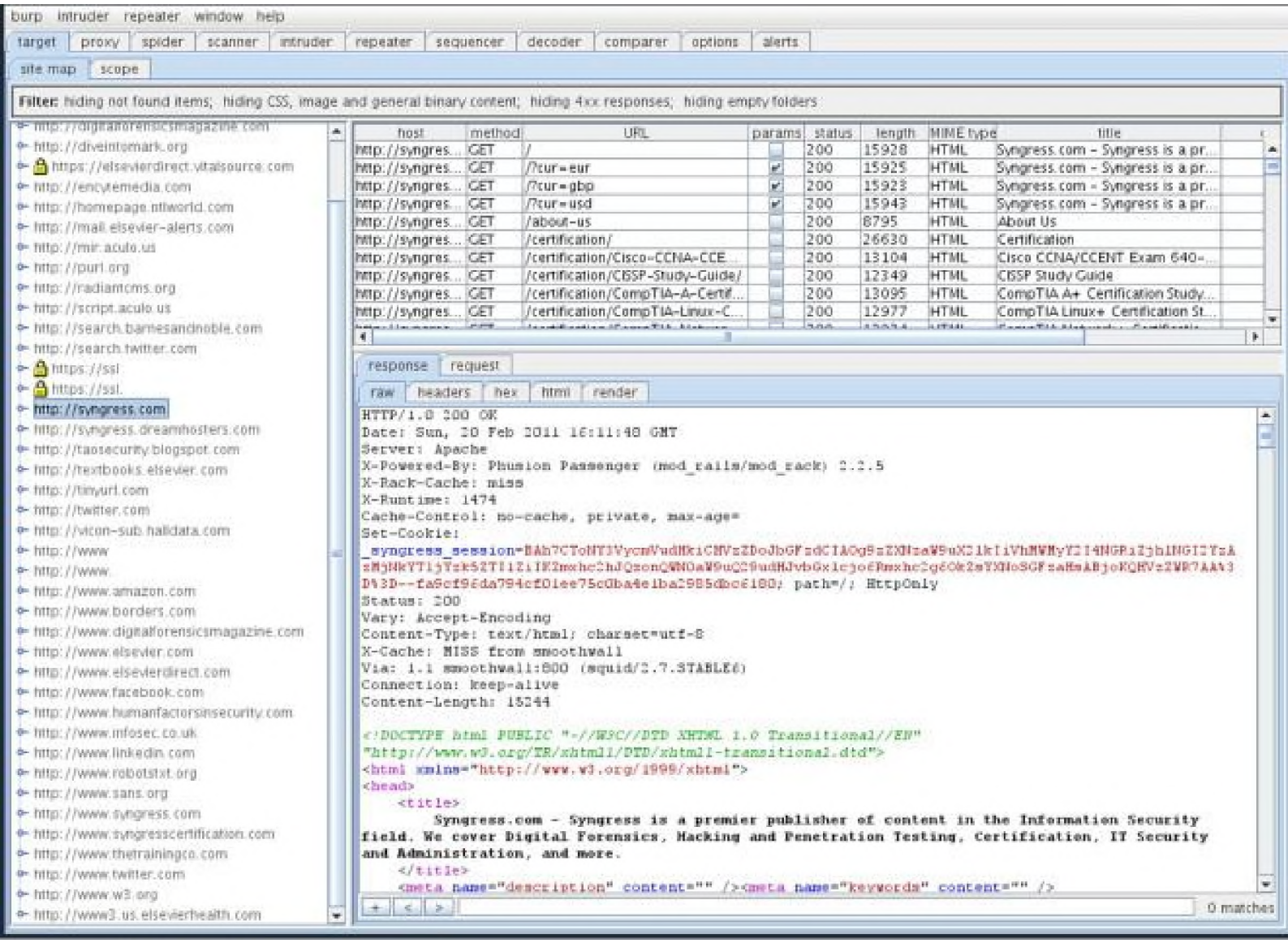
Грибанов Є.В. 125-20-2.ppt

Грибанов Є.В. 125-20-2.pdf

ДОДАТОК В. ТЕСТУВАННЯ ПРОГРАМОЮ OWASP ZAP



ДОДАТОК Г. ТЕСТУВАННЯ ПРОГРАМОЮ BURP SUITE



ДОДАТОК Д. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку б. («_____»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Е. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

На кваліфікаційну роботу студента групи 125-20-2 Грибанова Є.В.

на тему: «Розробка засобів та заходів кіберзахисту веб-сайту підприємства «ТОВ НОВА ПЕЙ»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на __ сторінках.

Мета роботи є актуальною, оскільки вона спрямована на удосконалення засобів та заходів кіберзахисту веб-сайту підприємства «ТОВ НОВА ПЕЙ».

При виконанні роботи автор продемонстрував високий рівень теоретичних знань і практичних навичок. На основі аналізу існуючих систем кіберзахисту та вимог веб-сайту були сформульовані конкретні завдання, розглянуті рішення та рекомендації щодо удосконалення заходів кіберзахисту. Особлива увага приділена практичній реалізації запропонованих заходів, що підвищують рівень безпеки веб-сайту.

Практична цінність роботи полягає в її можливості негайного впровадження запропонованих заходів кіберзахисту на практиці, що сприятиме покращенню безпеки веб-сайту і зменшенню ризиків витоку інформації.

Рівень запозичень у кваліфікаційній роботі не перевищує встановлених норм.

В цілому робота відповідає усім вимогам, а її автор заслуговує на оцінку «добре» та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,