Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Пономаренко Анатолій Сергійовича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи захисту корпоративного веб-сайту виробничого підприємства на базі системи керування контентом WordPress*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.
«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Пономаренко Анатолію Сергійовичу*** **академічної групи** ***125м-20-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Методи захисту корпоративного веб-сайту виробничого підприємства на базі системи керування контентом WordPress***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 №1036-с

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати стан інформаційної безпеки корпоративного веб сайту виробничого підприємства на базі системи керування контентом WordPress.	01.11.2021
Розділ 2	Виконати обстеження архітектури типового корпоративного веб сайту, аналіз інформації яка обробляється в ОІД, аналіз загроз та вразливостей, розробка та впровадження методів захисту корпоративного веб сайту.	15.12.2021
Розділ 3	Розрахувати кономічну доцільність впровадження запропонованих методів захисту корпоративного веб сайту, розрахунок витрат та ефекта впровадження методів захисту.	10.01.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 01.09.2021р.

Дата подання до екзаменаційної комісії: 20.01.2022р.

Прийнято до виконання _____ _Пономаренко А.С._
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 12 рис. 15 табл., 4 додатків, 18 джерел.

Об’єкт дослідження: корпоративний веб сайт типового виробничого підприємства на базі системи керування контентом WordPress.

Предмет дослідження: методи захисту веб сайтів на базі WordPress.

Мета роботи: забезпечення достатнього рівня захищеності корпоративного сайту на базі системи керування контентом WordPress.

Методи розробки: спостереження, порівняння, аналіз, дослідження.

Актуальність теми визначається необхідністю захисту інформації в корпоративних веб сайтах типового виробничого підприємства на базі системи керування контентом WordPress.

В першому розділі кваліфікаційної роботи надано загальний аналіз проблем забезпечення безпеки інформації України на веб ресурсах, розглянуто стан інформаційної безпеки на веб ресурсів промислових підпремств, які для роботи використовують систему керування конетнтом на базі WordPress.

В другому розділі кваліфікаційної роботи виконана реалізація меттодів захисту веб сайту на базі систем керування контенту WordPress. Наведено загальні відомості про об’єкт інформаційної діяльності. Проведено обстеження об’єкту інформаційної діяльності, визначені основні загрози та вразливості, проаналізований стан типового корпоративного веб сайту.

В третьому розділі кваліфікаційної роботи розраховано доцільність впровадження та використання запропонованих методів захистту корпоративного веб-сайту , економічну ефективність впровадження її елементів в інформаційно-телекомунікаційну систему на об’єкті інформаційної діяльності.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ОБ`ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АНАЛІЗ ЗАГРОЗ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, WORDPRESS, СИСТЕМА КЕРУВАННЯ КОНТЕНТОМ

РЕФЕРАТ

Объяснительная записка: 73 с., 12 рис. 15 табл., 4 приложений, 18 источников.

Объект исследования: корпоративный веб-сайт типового производственного предприятия на базе системы управления контентом WordPress.

Предмет исследования: методы защиты веб-сайтов на базе WordPress.

Цель работы: обеспечение достаточного уровня защищенности корпоративного сайта на базе системы управления контентом WordPress.

Методы разработки: наблюдение, сравнение, анализ, исследование.

Актуальность темы определяется необходимостью защиты информации в корпоративных веб-сайтах типового производственного предприятия на базе системы управления контентом WordPress.

В первом разделе квалификационной работы представлен общий анализ проблем обеспечения безопасности информации Украины на веб ресурсах, рассмотрен состояние информационной безопасности на веб ресурсов промышленных предприятий, которые для работы используют систему управления конетнтом на базе WordPress.

Во втором разделе выполнена реализация методов защиты веб сайта на базе систем управления контента WordPress. Приведены общие сведения об объекте информационной деятельности. Проведены обследования объекта информационной деятельности, определены основные угрозы и уязвимости, проанализировано состояние типичного корпоративного веб-сайта.

В третьем разделе квалификационной работы рассчитана целесообразность внедрения и использования предложенных методов защиты корпоративного веб-сайта, экономическая эффективность внедрения ее элементов в информационно-телекоммуникационную систему на объекте информационной деятельности.

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, АНАЛИЗ УГРОЗ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШНИКА, WORDPRESS, СИСТЕМА УПРАВЛЕНИЯ КОНТЕНТОМ

ABSTRACT

Explanatory note: 73 p., 12 fig. 15 tables, 4 annexes, 18 sources.

Object of research: corporate website of a typical manufacturing enterprise based on the WordPress content management system.

Subject of research: methods of protecting websites based on WordPress.

Purpose: to ensure a sufficient level of security of the corporate site of a typical manufacturing enterprise based on the WordPress content management system.

Development methods: observation, comparison, analysis, research.

The relevance of the topic is determined by the need to protect information in the corporate websites of a typical manufacturing enterprise based on the WordPress content management system.

The first section of the qualification work provides a general analysis of the problems of information security of Ukraine on web resources, the state of information security on the web resources of industrial enterprises that use a content management system based on WordPress.

In the second section of the qualification work the implementation of web site protection methods based on WordPress content management systems is implemented. General information about the object of information activities is given. A survey of the object of information activities was conducted, the main threats and vulnerabilities were identified, and the status of a typical corporate website was analyzed.

The third section of the qualification work calculates the feasibility of implementing and using the proposed methods of protection of the corporate website, the cost-effectiveness of implementing its elements in the information and telecommunications system at the object of information activities.

INFORMATION AND TELECOMMUNICATIONS SYSTEM, OBJECT OF INFORMATION ACTIVITY, THREAT ANALYSIS, THREAT MODEL, THREAT MODEL, INFRINGEMENT MODEL, WEBSITE, WORDPRESS, CONTENT MANAGER SYSTEM

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

В роботі використовуються такі позначення і скорочення:

АС - автоматизована система;

ІзОД — інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КС — комп'ютерна система;

КСЗІ — комплексна система захисту інформації;

НД — нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД — несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС — обчислювальна система;

ПЗ — програмне забезпечення;

CMS - система керуванням конттенту

БД - база даних

HTTP - протокол передачі гіпертексту

CRM - управління взаємовідносинами з клієнтами

ЗМІСТ

ВСТУП

Кожне підприємство використовує корпоративний веб-сайт для тих чи інших цілей: презентація компанії, налагодження роботи між працівниками компанії, автоматизація процесів та багато іншого. Така вбудованість корпоративного веб сайту в бізнес процеси підприємства викликають дуже великий інтерес у конкурентів.

Сьогодні будь-який злом використовується виключно з комерційною метою. Інтерес становлять не лише великі портали, а й невеликі сайти, блоги — загроза може торкнутися будь-якого ресурсу. Тому метою роботи було - забезпечення достатнього рівня захищеності корпоративного сайту типового виробничого підприємства, а саме: на базі системи керування контентом WordPress.

Адже реалізація атаки на веб ресурс підприємства несе за собою великі фінансові втрати та часткову бездіяльність підприємства. До наслідків, які за собою тягне хакерська атака, входять основні і критичні для сайту проблеми:

- Втрата контролю над сайтом.
- Витік даних користувачів.
- Витік комерційної інформації.
- Спам-розсилки.
- Фішингові сторінки.
- Масові атаки.
- Переадресація.
- Зниження чи повна втрата пошукових позицій.
- Репутаційні втрати.

Об'єктом дослідження був корпоративний веб сайт виробничого підприємства на базі системи керування контентом WordPress. Вибір CMS системи був обумовлений її великою популярністю на ринку та низьким рівнем захищеності веб ресурсів на цій CMS системі. Результатом проведення роботи стала

Предметом дослідження були методи захисту веб сайтів, впровадження яких підвищило рівень захищеності ресурсу.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Аналіз проблеми забезпечення захищеності корпоративних веб ресурсів.

Дослідники з компанії Sucuri узагальнили статистику зі зламів сайтів, засновану на інформації з більш ніж 25 тисяч звернень до служби розбору інцидентів та протидії шкідливій активності компаній GoDaddy та Sucuri.

90% звернень для усунення наслідків зламів були пов'язані з платформою WordPress, 4.6% – Magento, 4.3% – Joomla, 3.6% – Drupal. Слід зазначити, що значна перевага WordPress обумовлена популярністю даної CMS (застосовується на 30% з десяти мільйонів найбільших сайтів) та спеціалізацією Sucuri у вирішенні проблем з WordPress.

Вибір для досліджень саме WordPress обумовлен його популярністю. Саме на цій платформі розроблено вебсайт об’єкту мого дослідження.

Для точного аналізу треба обумовити поняття. WordPress — система керування вмістом(надалі СКВ або CMS) з відкритим кодом, яка через свою простоту в установленні та використанні широко застосовується для створення вебсайтів. Сфера використання — від блогів до складних вебсайтів. Вбудована система тем і плагінів у поєднанні з вдалою архітектурою дозволяє конструювати на основі WordPress практично будь-які вебпроекти. Через низький порог входу, його обираються переважна більшість корисстувачей.

Але така популярність CMS має і свої недоліки. Фахівці Wordfence звернули увагу, що якийсь хак-гурт розгорнув масштабну кампанію проти сайтів на WordPress. Використовуючи різні відомі вразливості, зловмисники спробували атакувати майже мільйон ресурсів за минулий тиждень.

Атаки розпочалися 28 квітня 2020 року та призвели до тридцятикратного збільшення обсягу шкідливого трафіку, що відстежується компанією. Угруповання використовує для атак понад 24 000 різних IP-адрес і вже спробувало зламати понад 900 000 сайтів під керуванням WordPress. Атаки досягли свого піку минулої неділі, 3 травня 2020 року, коли хакери зробили більше 20 000 000 спроб зламування 500 000 різних доменів.

За статистикою на 2021 рік:

- 80% сайтів на WordPress раніше були зламані;
- Близько 30% сайтів на цьому движку зараз знаходяться під керуванням сторонніх осіб;
- 90% власників сайтів не знають про злом 3 місяці і більше.
- На момент взлому 56% сайтів було оновлено до актуального випуску CMS;
- 44% використали застарілі версії.

За рік помічено тенденцію до збільшення з 69.8% до 87.50% числа неоновлених уразливих установок CMS Joomla на момент злому. Для WordPress ситуація зворотна і частка використання застарілих версій під час взлому знижується (атакують переважно через уразливості у плагінах та темах оформлення).

Найбільш популярною (68%) шкідливою активністю після злому залишається впровадження бекдору для отримання доступу до системи. Частка шкідливої активності на зламаних сайтах, пов'язаної з поширенням шкідливого програмного забезпечення, збільшилася за рік з 47% до 56.4%, а пов'язаної з розміщенням SEO-спаму зросла з 44% до 51.3%. Число виявлених скриптів для розсилки спаму скоротилося з 19% до 12.5%.

1.2. Аналіз типового об’єкта

Для початку треба визначитись з поняттям корпоративного веб сайту. Корпоративний веб сайт - це інтернет-ресурс компанії/підприємства, на якому містяться дані про компанію, керівника, послуги, товари, системи ведення бізнесу, здобутки компанії та інше. Він — важлива складова іміджу компанії. Корпоративний сайт потрібен для середнього чи великого бізнесу, який постійно розвивається в інтернеті і в оффлайн.

1.2.1 Призначення корпоративного веб сайту

Призначення корпоративного веб сайту безпосередньо залежить від типу бізнесу та цілей компанії. Далі розглянемо лише основні пункти:

- Формування та підвищення іміджу компанії.
- Розширення клієнтської та партнерської бази.
- Можливість продажу товарів та послуг.

- Залучення нових працівників.
- Функціонування CRM системи для ведення бізнесу між співробітниками.
- Функціонування ресурсів для автоматизації процесів.

1.2.2 Типова реалізація

Розробка корпоративного веб сайту вже давно стала доступною для кожного. Існує велика кількість платформ для розробки, сервісів, інструментів та методик. За статистикою агентства W3Tech більше половини компаній користуються найпопулярнішим та найпростішим методом розробки веб сайту - використання Систем Керування Контентом(надалі CMS).

CMS - це веб-додаток, в якому люди створюють та обслуговують сайти. Основна перевага CMS – щоб створити сайт та працювати з ним не обов'язково знати програмування.

На сьогоднішній день можна виділити 8 найпопулярніших CMS систем: WordPress, Joomla, Drupal, Typo3, Serendipity, Dotclear, ImpressPages, Chamilo;

Процес реалізації CMS систем повністю співпадає зі звичайною моделлю реалізації веб сайту та представлений на рисуноку 1.1.

CMS дозволяє спростити пункт “КОДУВАННЯ”. Це говорить про те, що всі підготовчі процеси залишають однаковими, а саме:

- орендування доменного імені;
- аналіз потреб;
- визначення технічних характеристик хостінгу;
- арендування хостіну;
- процесс розробки;
- тестування;
- кінцева експлуатація;

Кожну CMS систему треба встановити на свій сервер, для подальшої роботи з ресурсом. Для цього на сайтах виробників завантажуються файли інсталювання,

встановлюються файли на хостінгу, робиться первинне налаштування CMS системи.

Рисунок 1.1. Типова модель реалізації веб ресурсу

1.2.3 Архітектура корпоративного веб сайту

Архітектура корпоративного веб сайту— структура сторінок та програмної частини сайту. Архітектура допомагає візуально подати всі розділи сайту, що дуже важливо в процесі розробки. Власнику сайту відразу видно, які саме розділи включені у веб-сайт, дизайнеру видно, які сторінки треба розробити та зверстати, райтер знає, яким контентом наповнювати конкретні розділи.

Надалі представлена типова архітектура веб сайту, яка характерна з використанням CMS систем представлений на рисуноку 1.2.

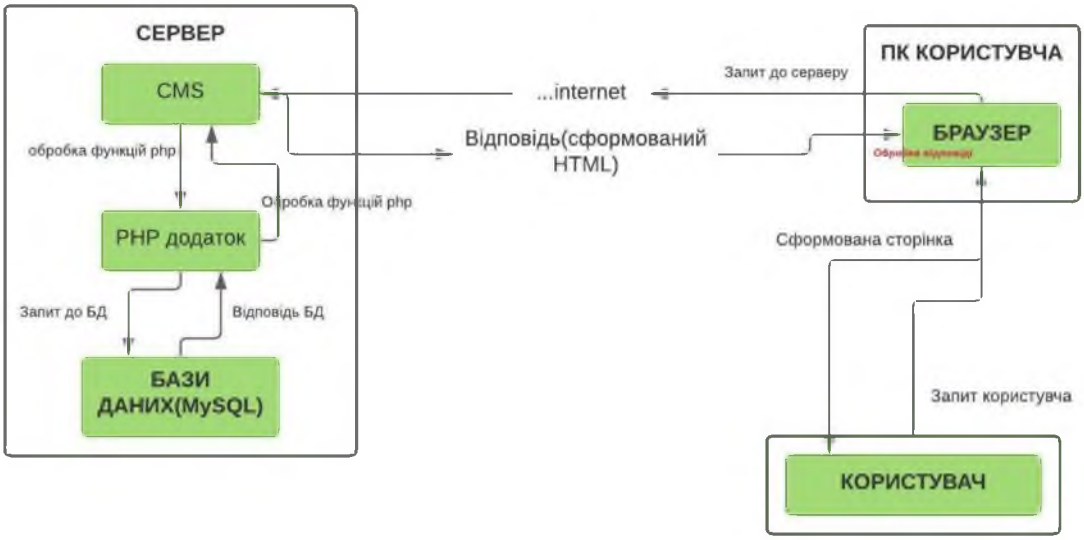


Рисунок 1.2 Типова архітектура веб сайту з використанням CMS.

Для типової CMS системи наявні певні особливості та послідовності завантаження ресурсів для відображення контенту. До особливостей можна віднести:

- послідовність завантаження файлів;
- типи підключення файлів;
- назви підключених файлів;
- особливості побудови функції;

На рисунку 1.3 представлена типова архітектура сторінки CMS системи, на якому видно послідовність завантаження файлів та ресурсів на сторінці.

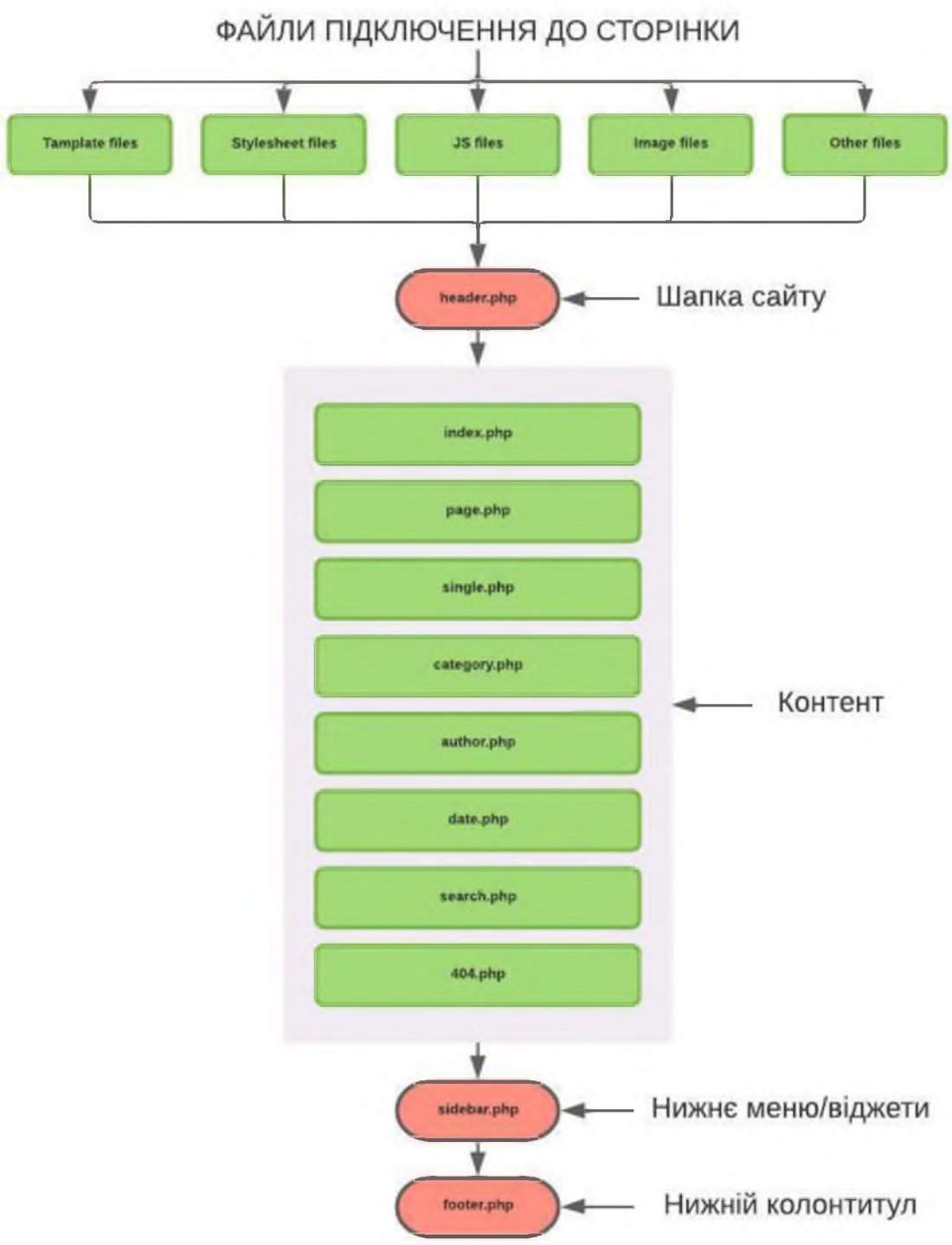


Рисунок 1.3 Архітектура сторінки веб сайту на базі CMS системи.

Згідно схеми (рис. 1.3) видно порядок підключення файлів, та їх структурна особливість. Для CMS системи характерні підключення наступних файлів:

- файлів шаблону сторінки, які формують структуру сторінки;
- файли стилів сторінки;

- файли HEADER та FOOTER;

1.3 Аналіз типових загроз та вразливостей корпоративного веб сайту

При керуванні сайтом важливо знати найбільш значущі вразливості та загрози безпеці веб сайту. Для аналізу загроз та вразливостей задіяно матрицю MITRE ATT&CK, список OWASP TOP 10. Саме на цих ресурсах представлені актуальні данні про загрози та вразливості, та методи усунення цих загроз.

Фахівці з інформаційної безпеки використовують матриці Mitre Att&ck для вирішення наступних завдань:

- Аналіз існуючого захисту на предмет відповідності реальним загрозам та підвищення безпеки інфраструктури компанії. За допомогою матриць Mitre Att&ck можна визначити, до яких технік уразливі ресурси організації, щоб у перспективі усунути найкритичніші проблеми.
- Своєчасне реагування на інциденти. За допомогою матриць Mitre Att&ck можна встановити, на якому етапі розвитку знаходиться атака і які заходи необхідно вжити насамперед.
- Розслідування кіберінцидентів. Матриці Mitre Att&ck дозволяють оперативно визначити, на якому етапі виявлено атаку і де варто в першу чергу шукати сліди вторгнення.
- Атрибуція атак. За переліком технік, використаних зловмисниками, можна визначити імовірного виконавця.
- Аналіз діяльності кіберзлочинців. Матриці Mitre Att&ck дозволяють відслідковувати еволюцію тактик та технік, які застосовують відомі APT-угруповання.
- Обмін інформацією із колегами. Єдина структурована система опису кібератаки дозволяє фахівцям із різних областей знаходити спільну мову.

Наступним інструментом для аналізу був список OWASP.

OWASP (розшифровується як Open Web Application Security Project) - це онлайн-спільнота, яка випускає статті на тему безпеки веб-застосунків, а також документацію, різні інструменти та технології.

Надалі представлені типові загрози та вразливості які базуються на знаннях двох БД. Аналізувалась БД сервісів виключно для організаціх безпеки корпоративного веб сайту. Спочтаку розглянемо матрицю MITRE ATT&CK.

1.3.1. Аналіз матриці типових загроз

ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) – Тактики, техніки та загальновідомі знання про зловмисників) спосіб опису та категоризації поведінки зловмисників, заснований на аналізі реальних атак.

Матриця дозволяє будувати моделі загроз для різних типів компаній та показувати, які із відомих загроз можна закрити конкретними рішеннями. Теоретично це виглядає так: компанія, що вибирає рішення для захисту своєї інфраструктури, проектує можливості зловмисника на матрицю ATT&CK і дивиться, які актуальні загрози залишилися не закритими.

Для аналізу MITRE використовує набори TTP (техніки, тактики та процедури) розшифровуються наступним чином:

тактика – як зловмисник діє на різних етапах своєї операції, яка мета чи завдання зловмисника на певному кроці, наприклад: TA0002 Execution – це коли зловмисник намагається запустити свій шкідливий код.

техніка - як зловмисник досягає мети або поставленого завдання, які використовує інструменти, технології, код, експлоїти, утиліти тощо. Приклад: T1059.001 PowerShell – використання PowerShell під час атаки;

процедура – як ця техніка виконується і для чого. Наприклад: шкідлива програма, використовуючи PowerShell, завантажує пейлоад, який у свою чергу завантажує Cobalt Strike для спроби запуску на віддалених хостах.

В таблиці 1.1 представлено основні загрози та методи реалізації вразливостей актуальні на основі матриці ATT&CK.

Таблиця 1.1 Матриця загроз ATT&CK

Тактика	Техніка	Процедура
Початковий доступ	Експлуатування публічної програми T1190	Зловмисники можуть спробувати скористатися слабкістю комп'ютера або програми з Інтернетом, використовуючи програмне забезпечення, дані або команди, щоб викликати ненавмисне або непередбачувану поведінку. Слабкою стороною системи може бути помилка, збій або вразливість дизайну. Ці програми часто є веб-сайтами, але можуть включати бази даних (наприклад, SQL), стандартні служби (наприклад, SMB або SSH), протоколи адміністрування та керування мережевими пристроями (наприклад, SNMP та Smart Install), та будь-які інші програми з відкритими сокетами, доступними в Інтернет, наприклад, веб-сервери та супутні служби. Залежно від використовуваного недоліку це може включати експлуатацію для ухилення від оборони.
Виконання	Інтерпретатор команд та сценаріїв T1059	Зловмисники можуть зловживати інтерпретаторами команд і сценаріїв для виконання команд, сценаріїв або двійкових файлів. Ці інтерфейси та мови забезпечують способи взаємодії з комп'ютерними системами і є спільною ознакою для багатьох різних платформ. Більшість систем мають деякий вбудований інтерфейс командного рядка та можливості написання сценаріїв, наприклад, дистрибутиви macOS та Linux включають Unix Shell, тоді як інсталяції Windows включають командну оболонку Windows та PowerShell.

Продовження таблиці 1.1 Матриця загроз ATT&CK

Тактика	Техніка	Процедура
Налаштування	Змінити процес аутентифікації	Зловмисники можуть змінювати механізми та процеси аутентифікації, щоб отримати доступ до облікових даних користувачів або дозволити іншим чином необґрунтований доступ до облікових записів. Процес аутентифікації обробляється такими механізмами, як локальний сервер аутентифікації безпеки (LSASS) і менеджер облікових записів безпеки (SAM) у Windows, підключаються модулі аутентифікації (PAM) у системах на базі Unix та плагіни авторизації в системах MacOS, відповідальні для збору, зберігання та перевірки облікових даних. Змінюючи процес аутентифікації, зловмисник може пройти аутентифікацію в службі або системі без використання дійсних облікових записів.
	Завантаження Pre-OS	Зловмисники можуть зловживати механізмами попереднього завантаження ОС як способом встановити стабільність у системі. Під час процесу завантаження комп'ютера прошивка та різні служби завантаження завантажуються до операційної системи. Ці програми контролюють потік виконання до того, як операційна система візьме контроль.

Продовження таблиці 1.1 Матриця загроз ATT&CK

Тактика	Техніка	Процедура
Ухилення від оборони	Послабити захист	Зловмисники можуть змінювати компоненти середовища жертви, щоб перешкодити або вимкнути захисні механізми. Це не тільки передбачає погіршення засобів захисту, таких як брандмауери та антивіруси, але й можливості виявлення, які захисники можуть використовувати для перевірки діяльності та виявлення шкідливої поведінки. Це також може охоплювати як власні засоби захисту, так і додаткові можливості, встановлені користувачами та адміністраторами.
	Змінити процес аутентифікації	Зловмисники можуть змінювати механізми та процеси аутентифікації, щоб отримати доступ до облікових даних користувачів або дозволити іншим чином необґрунтований доступ до облікових записів. Процес автентифікації обробляється такими механізмами, як локальний сервер аутентифікації безпеки (LSASS) і менеджер облікових записів безпеки (SAM) у Windows, підключаються модулі аутентифікації (PAM) у системах на базі Unix та плагіни авторизації в системах MacOS, відповідальні для збору, зберігання та перевірки облікових даних. Змінюючи процес аутентифікації, зловмисник може пройти автентифікацію в службі або системі без використання дійсних облікових записів.

Продовження таблиці 1.1 Матриця загроз ATT&CK

Тактика	Техніка	Процедура
	Змінити образ системи	Зловмисники можуть вносити зміни в операційну систему вбудованих мережевих пристроїв, щоб послабити захист і надати собі нові можливості.
	Мережеве мостове з'єднання	Зловмисники можуть подолати межі мережі, порушивши периметр мережевих пристроїв. Порушення цих пристроїв може дозволити зловмисникові обійти обмеження на маршрутизацію трафіку, які в іншому випадку розділяють надійні та ненадійні мережі.
	Зміна трафіку	Зловмисники можуть використовувати зміну трафіку, щоб приховати відкриті порти або інші шкідливі функції, які використовуються для командування та контролю. Зміна трафіку передбачає використання певного значення або послідовності, яку необхідно надіслати в систему, щоб викликати спеціальну відповідь, наприклад, відкриття закритого порту або виконання шкідливого завдання. Це може мати форму відправки серії пакетів з певними характеристиками, перш ніж буде відкритий порт, який зловмисник може використовувати для командування та контролю. Зазвичай ця серія пакетів складається із спроб підключення до попередньо визначеної послідовності закритих портів (тобто Port Knocking), але може включати незвичайні прапорці, певні рядки або інші унікальні характеристики.

Продовження таблиці 1.1 Матриця загроз ATT&CK

Тактика	Техніка	Процедура
Доступ до облікових даних	Захоплення введення даних T1056	Зловмисники можуть використовувати методи фіксації введених користувачів для отримання облікових даних або збору інформації. Під час нормального використання системи користувачі часто надають облікові дані в різних місцях, наприклад на сторінках входу/порталах або системних діалогових вікнах. Механізми захоплення вхідних даних можуть бути прозорими для користувача.
	Змінити процес аутентифікації	Зловмисники можуть змінювати механізми та процеси аутентифікації, щоб отримати доступ до облікових даних користувачів або дозволити іншим чином необґрунтований доступ до облікових записів. Процес автентифікації обробляється такими механізмами, як локальний сервер аутентифікації безпеки (LSASS) і менеджер облікових записів безпеки (SAM) у Windows, підключаються модулі аутентифікації (PAM) у системах на базі Unix та плагіни авторизації в системах MacOS, відповідальні для збору, зберігання та перевірки облікових даних. Змінюючи процес аутентифікації, зловмисник може пройти автентифікацію в службі або системі без використання дійсних облікових записів.

Продовження таблиці 1.1 Матриця загроз ATT&CK

Тактика	Техніка	Процедура
	Перегляд мережі	Зловмисники можуть перевіряти мережевий трафік, щоб отримати інформацію про середовище, включаючи матеріал аутентифікації, що передається по мережі. Перегляд мережі відноситься до використання мережевого інтерфейсу в системі для моніторингу або захоплення інформації, надісланої через дротове або бездротове з'єднання. Зловмисник може перевести мережевий інтерфейс у безладний режим для пасивного доступу до даних, що передаються по мережі, або використовувати порти span для захоплення більшої кількості даних.
Відкриття	Перегляд мережі	Зловмисники можуть перевіряти мережевий трафік, щоб отримати інформацію про середовище, включаючи матеріал аутентифікації, що передається по мережі. Перегляд мережі відноситься до використання мережевого інтерфейсу в системі для моніторингу або захоплення інформації, надісланої через дротове або бездротове з'єднання. Зловмисник може перевести мережевий інтерфейс у безладний режим для пасивного доступу до даних, що передаються по мережі, або використовувати порти span для захоплення більшої кількості даних.

Продовження таблиці 1.1 Матриця загроз ATT&CK

Тактика	Техніка	Процедура
Збирання	Дані сховища конфігурації T1602	Зловмисники можуть збирати дані, пов'язані з керованими пристроями, зі сховищ конфігурації. Репозиторії конфігурації використовуються системами керування для налаштування, керування та контролю даних у віддалених системах. Репозиторії конфігурації можуть також полегшити віддалений доступ та адміністрування пристроїв.
	Захоплення введення	Зловмисники можуть використовувати методи фіксації введених користувачів для отримання облікових даних або збору інформації. Під час нормального використання системи користувачі часто надають облікові дані в різних місцях, наприклад на сторінках входу/порталах або системних діалогових вікнах. Механізми захоплення вхідних даних можуть бути прозорими для користувача.
Командування та контроль	Проксі	Зловмисники можуть використовувати проксі-сервер з'єднання для спрямування мережевого трафіку між системами або виступати посередником у мережевому зв'язку з сервером командування та управління, щоб уникнути прямих з'єднань зі своєю інфраструктурою. Існує багато інструментів, які дозволяють перенаправляти трафік через проксі-сервери або порти, включаючи HTRAN, ZXProxy і ZXPortMap. [1]

Продовження таблиці 1.1 Матриця загроз ATT&CK

Тактика	Техніка	Процедура
Ексфільтрація	Автоматизована ексфільтрація T1020	Зловмисники можуть вилучити дані, такі як конфіденційні документи, за допомогою автоматизованої обробки після того, як вони були зібрані під час збору.
	Зміна трафіку	Зловмисники можуть використовувати зміну трафіку, щоб приховати відкриті порти або інші шкідливі функції, які використовуються для командування та контролю. Зміна трафіку передбачає використання певного значення або послідовності, яку необхідно надіслати в систему, щоб викликати спеціальну відповідь, наприклад, відкриття закритого порту або виконання шкідливого завдання. Це може мати форму відправки серії пакетів з певними характеристиками, перш ніж буде відкритий порт, який зловмисник може використовувати для командування та контролю. Зазвичай ця серія пакетів складається із спроб підключення до попередньо визначеної послідовності закритих портів (тобто Port Knocking).

Надалі розглянемо рейтинг вразливостей веб сайту за базою даних OWASP TOP 10.

1.3.2. Аналіз бази даних актуальних загроз

OWASP (розшифровується як Open Web Application Security Project) - це онлайн-спільнота, яка випускає статті на тему безпеки веб-застосунків, а також документацію, різні інструменти та технології.

В останній версії OWASP можна виділити 8 основних вразливостей:

- Ін'єкційні атаки (Injections)

- Порушена автентифікація (Broken Authentication)
- Незахищеність критичних даних (Sensitive Data Exposure)
- Зовнішні об'єкти XML (XXE) (XML External Entities (XXE))
- Порушення контролю доступу (Broken Access control)
- Небезпечна конфігурація (Security misconfigurations)
- Міжсайтовий скриптинг (XSS) (Cross Site Scripting (XSS))
- Використання компонентів з відомими вразливістю (Using Components with known vulnerabilities)

Ін'єкційна атака. При ін'єкційній атаці зловмисник впроваджує неприпустимі дані у веб-додаток із наміром змусити його зробити щось, для чого програма не була розроблена/запрограмована.

Можливо, найпоширенішим різновидом цієї вразливості системи безпеки є використання коду через SQL-запит, що використовує ненадійні дані, наприклад: String query = "SELECT * FROM accounts WHERE custID = '" + request.getParameter("id") + "'";

Один приклад SQL-впровадження, що торкнулося понад півмільйона сайтів, на яких було встановлено плагін YITH WooCommerce Wishlist для WordPress, яке показано на рисунку 1.4.

```
function deleteQuery($conn)
{
    if (isset($_POST['deleteProductId']))
    {
        $strsql = "DELETE FROM PRODUCT WHERE id = ?";
        if ($stmt = $conn->prepare($strsql))
        {
            // bind
            $stmt->bind_param("s", $_POST['deleteProductId']);
            $stmt->execute();
            $stmt->close();
            echo "Delete succeed!<br>";
        }
```

Рисунок 1.4 Приклад SQL впровадження.

Зазначене вище SQL-використання може призвести до серйозного витоку конфіденційних даних.

Порушена автентифікація. Некоректна автентифікація може дозволити зловмиснику використовувати ручні та/або автоматичні методи, щоб спробувати отримати контроль над будь-яким обліковим записом у системі або, що ще гірше, повний контроль над системою.

Незахищеність критичних даних. Незахищеність критичних даних є однією з найпоширеніших вразливостей. Йдеться насамперед про конфіденційні дані, які вимагають особливої уваги та захисту.

Приклади конфіденційних даних:

- Номери кредитних карток,
- Медична інформація,
- Інформація, що дозволяє ідентифікувати особистість (PII),
- Інша особиста інформація.

Зовнішні об'єкти XML. Атака зовнішнього об'єкта XML - це тип атаки на програму за допомогою аналізу введення XML. Ця атака відбувається, коли введення XML, що містить посилання на зовнішній об'єкт, обробляється погано налаштованим синтаксичним аналізатором XML.

Більшість синтаксичних аналізаторів XML за умовчанням уразливі для XXE-атак. Відповідальність за те, щоб програма не містила цієї вразливості, лежить в основному на розробнику.

Порушення контролю доступу. У сфері безпеки сайтів контроль доступу – це обмеження доступу відвідувачів до окремих розділів або сторінок. Тобто порушення контролю доступу - це несанкціонований доступ до розділу, доступу до якого у користувача немає. У наші дні це проблема майже всіх основних систем керування вмістом (CMS). За промовчанням доступ до сторінки входу адміністратора надається всім.

Небезпечна конфігурація. Сучасні програми CMS, будучи простими у використанні, можуть бути небезпечними для кінцевих користувачів. Більшість атак хакерів, безумовно, повністю автоматизовані, і зловмисники покладаються на те, що у користувачів виставлені налаштування за замовчуванням. Це означає, що

велику кількість атак можна запобігти, змінивши при установці CMS налаштування за замовчуванням.

Найпоширенішими помилками є:

- Не виправлені недоліки;
- Конфігурації за замовчуванням;
- Наявність сторінок, що не використовуються;
- Не захищені файли та каталоги;
- Непотрібні служби.

Міжсайтовий скриптинг. Міжсайтовий скриптинг - це поширена вразливість, атаки якої складаються з впровадження шкідливих клієнтських скриптів на сайт з подальшим використанням сайту як розповсюджувача.

Ризики, пов'язані з XSS, полягають у тому, що він дозволяє зловмиснику впроваджувати контент на сайт та змінювати спосіб його відображення, змушуючи тим самим браузер жертви виконувати під час завантаження сторінки код, наданий зловмисником.

Використання компонентів з відомими вразливістю. У наші дні навіть прості сайти, такі як особисті блоги, мають багато залежностей.

Нездатність оновити кожну частину програмного забезпечення на серверній та клієнтській стороні сайту, без сумніву, рано чи пізно створить серйозні ризики для безпеки.

Наприклад, у 2019 році 56% усіх програм CMS на момент їх зараження були застарілими.

1.4 Аналіз нормативно-правової бази у сфері захисту інформації

Під час розробки систем захисту для корпоративного веб сайту було проаналізовано нормативно-правові документи, серед яких можна виділити:

- Закон України "Про інформацію»;
- Закон України "Про захист інформації в автоматизованих системах";
- НД ТЗІ 1.1-002-99: Загальні положення з захисту інформації в комп’ютерних системах від НСД;

- НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22);
- НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».;
- ДСТУ ISO/IEC 27001:2015 - Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)- На заміну ДСТУ ISO/IEC 27001:2010
- ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).
- ISO 27017 – Зведення практичних правил із засобів контролю інформаційної безпеки для хмарних служб.
- ISO 27018 – Зведення практичних правил захисту персональних даних у загальнодоступних хмарних середовищах, що діють як процесори персональних даних.
- НД ТЗІ 2.5-004-99 специфікаціями. Встановлює мінімально необхідний перелік послуг безпеки інформації та рівнів їх реалізації у комплексах засобів захисту інформації WEB-сторінки від несанкціонованого доступу.
- НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

1.5 Постановка задачі

Згідно статистики CMS систем, яку проводила Microsoft у 2021 році, був сформований наступний список найпопулярніших систем керуванням контентом представлені на рисунку 1.5.

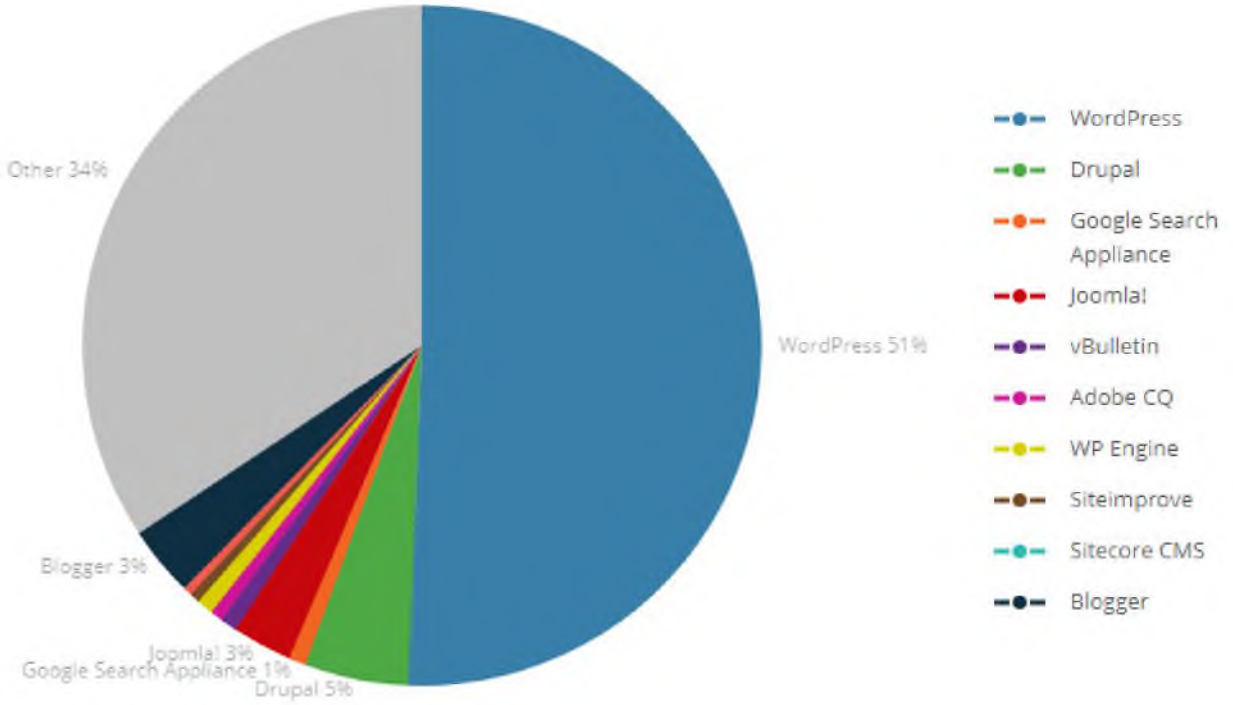


Рисунок 1.5 Статистика використання CMS систем.

З списку видно - найпопулярніші CMS системою є WordPress, він займає 51% від всього ринку світу.

Саме через велику популярність даної CMS ми будемо розглядати корпоративний веб сайт виробничого підприємства, сформований на базі WordPress.

На основі проаналізованих проблем у пункті 1.1, пункті 1.2 та на основі аналізу статистик використання CMS систем, у якому були встановлені основні проблеми використання корпоративних веб сайтів типового виробничого підприємства, ставимо задачу впровадити методи захисту в розділі 2.

Для побудови системи захисту потрібно:

- Проаналізувати архітектуру типового корпоративного веб сатйу виробничого підприємства;

- Проаналізувати особливості використання веб сатйу;
- Проаналізувати логічну характеристику об’єкту;
- Проаналізувати види інформації та особливості взаємодії інформації на об’єкті;
- Побудувати модель загроз;
- Оцінити рівень захищеності корпоративного веб сайту до впровадження методів захисту;
- Підібрати методи захисту та впровадити на запропоновану систему.
- Оцінити рівень захищеності корпоративного веб сайту після впровадження методів захисту.

1.6 Висновки до першого розділу

У першому розділі кваліфікаційної роботі було описано стан інформаційної захищенності в CMS системах, наведені основні проблеми використання CMS систем, проаналізована нормативно-правова база, що регулюють відносини у сфері інформаційних відносин, поставлена задача для подальшої роботи кваліфікаційної роботи.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Архітектура мережі типового об'єкта інформаційної діяльності

Основна інформація про корпоративний веб сайта представлена у таблиці 2.1.

Таблиця 2.1.Параметри хостінгу корпоративного веб сайту.

CMS WordPress	5.8.2
Версія PHP	7.2.34
Домен	agroprom.shop
Хостінг	Hosting Ukraine
Об’єм сховища	1 Тб
Оперативна пам’ять	32 Гб
Кількість сторінок	21 + Сторінки товару
Кількість сайтів на хостінгу	3
Зайнятий об’єм	324 мб

Шаблони системи слугують для створення особливого дизайну веб сайту. Це певний набір плагінів, стилів, CSS, JS, PHP скриптів, які створюють особливий візуальний стиль. На тестовому веб сайті використовується преміальний шаблон The7. Інформація про шаблон представлена в таблиці 2.2.

Таблица 2.2. Використанні шаблони.

Назва	Версія	Потреба в оновленні
The7	9.17.2	Потребує

Також для спрощення процесу програмування у CMS системах використовують плагіни. Плагін - це набір скриптів, які виконують певну

специфічну задачу, яку не може виконати CMS система. Надалі представлена таблиця 2.3 з інформацією про використані плагіни на сайті.

Таблиця 2.3 Використані плагіни.

Назва	Версія	Потреба в оновленні
Google Ads & Marketing by Kliken	1.0.7	Потребує
Google Analytics for WordPress by MonsterInsights	8.0.1	Потребує
WPForms Lite	1.6.9	Не потребує
WPBakery Page Builder	6.7.0	Потребує
WooCommerce	5.7.1	Потребує
WC Ukr Shipping	1.8.2	Потребує
Ultimate Addons for WPBakery Page Builder	3.19.11	Потребує
The7 Elements	2.5.7.1	Потребує
Slider Revolution	6.5.8	Не потребує
Safe SVG	1.9.9	Потребує
Revision Control	2.3.2	Не потребує

Для кожного корпоративного сайту, які надають якісь послуги або продають товари, прослідковується характерна типова схема. На схемі представлені основні розділи веб-сайту та шляхи доступу до сторінок та розділів.

Дана схема представлена на рисунку 2.2

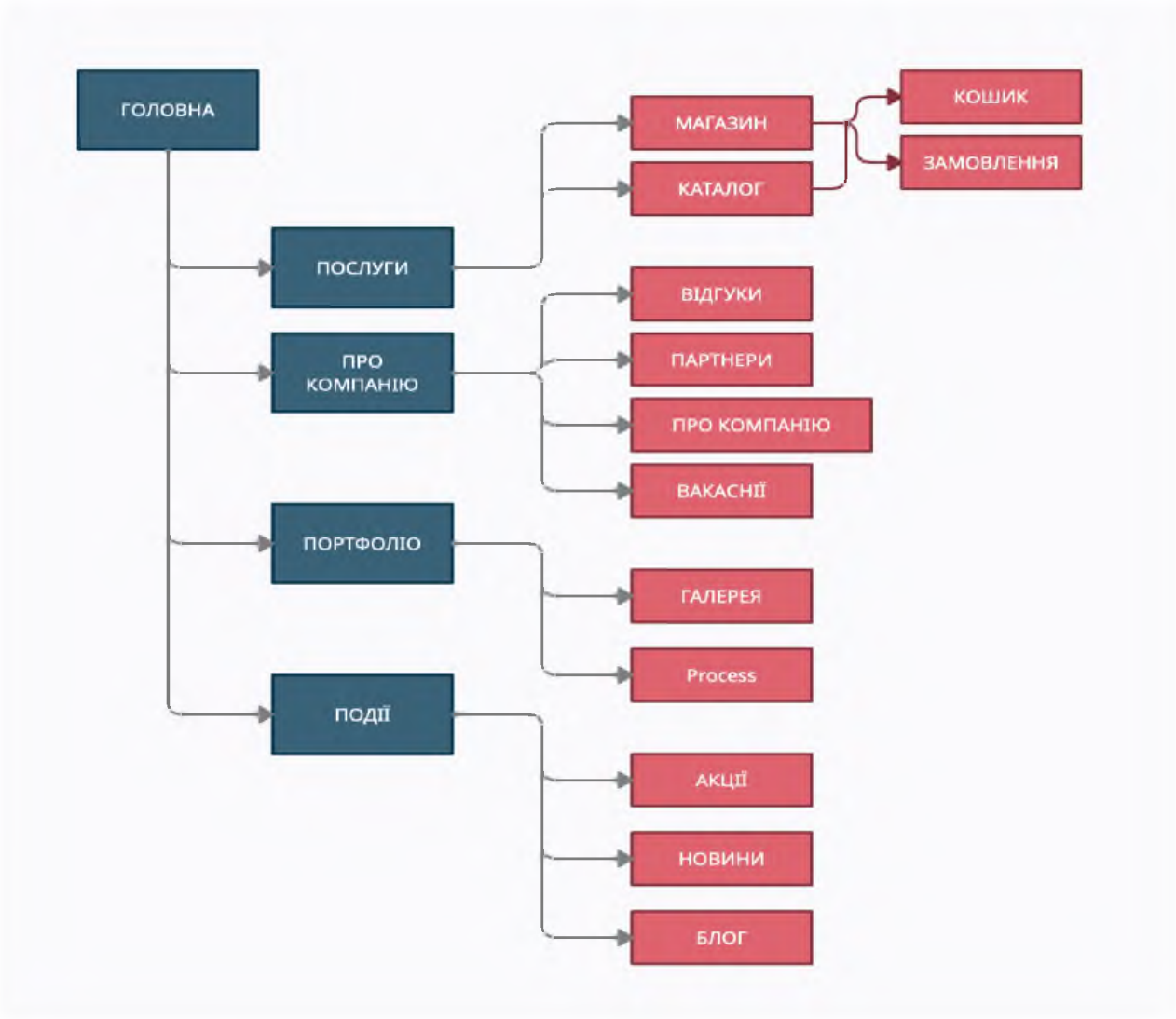


Рисунок 2.2 Типова схема корпоративного веб сайту

2.2 Опис інформації, яка обробляється на веб ресурсах типового підприємства

Детальний перелік інформації, правовий режим, вид зберігання та вимогу до захисту наведено у таблиці 2.4.

К – вимоги до конфіденційності

Ц – вимога до цілісності

Д – вимога до доступності

Таблиця 2.4 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
1	Розробки планів оптимізації виробництва	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
2	Звіти закупівель	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
3	Документація зборки	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
4	Інженерні моделі	Електронний	ІЗоД	Комерційна таємниця	КЦД
5	Креслення	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
6	Програмні коди для програмування обладнання	Електронний	ІЗоД	Комерційна таємниця	КЦД
7	Технології обробки	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД

Продовження таблиці 2.4 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
8	Документація з технології зварювання	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
9	Норми виробництва	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
10	Стратегічний план розвитку	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
11	Звітність з дифіциту	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
12	Звідність з складів матеріалу	Електронний, паперовий	ІЗоД	Комерційна таємниця	Д
13	Технічні завдання інженерам	Електронний, паперовий	ІЗоД	Комерційна таємниця	ЦД

Продовження таблиці 2.4 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
14	Технічні завдання технологам	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
15	Технічні завдання	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦ
16	Документи постачання	Електронний, паперовий	ІЗоД	Комерційна таємниця	КД
17	Інформація про діяльність відділів	Електронний, паперовий	Відкрита	-	Ц
18	Прайс продукції	Електронний, паперовий	Відкрита	-	ЦД

Продовження таблиці 2.4 Перелік основної інформації

№	Інформація	Вид зберігання	Режим доступу	Правовий режим	Вимоги до захисту
19	Каталоги продукції	Електронний, паперовий	Відкрита	-	ЦД
20	Медіатека	Електронний	Відкрита	-	ЦД
21	Сертифікати на продукцію	Електронний, паперовий	ІЗоД	Комерційна таємниця	КЦД
22	Облікові дані дилерів	Електронний	ІЗоД	Комерційна таємниця	КЦД
23	Облікові дані клієнтів	Електронний	ІЗоД	Комерційна таємниця	КЦД

2.3 Аналіз загроз та вразливостей

2.3.1. Модель порушника

Порушником є особа, яка здійснює спробу несанкціонованого доступу до об'єктів захисту (ознайомлення, модифікація, знищення, зміна режимів використання чи функціонування тощо).

Категорії порушників, що використовуються при створенні моделі, наведено в таблиці 2.5. У таблицях наведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ІТС, за показником можливостей використання засобів ІТС для реалізації загроз, за часом та місцем дії. Сукупність цих характеристик визначає профіль порушника.

Таблиця 2.5 Рейтингова оцінка рівня загроз:

Рейтінгова оцінка	Опис
1	незначний
2	низький
3	середній
4	високий
5	неприпустимо високий

Виходячи із результатів аналізу характеристики інформації, яка обробляється, категорій порушників, які мають потенційну можливість порушення

конфіденційності та цілісності інформації вважаються найбільш: небезпечними, доступності - менш небезпечними, а спостережності - найменш небезпечними.

Таблиця 2.6 Категорії порушників

Позначення	Визначення категорії	Потенціальний рівень загроз
П1	Авторизовані користувачі, яким надано право доступу до ІзОД (клієнти/ дилери/ менеджери)	5
П2	Авторизовані користувачі, яким надано повноваження контролювати дії користувачів та персоналу та забезпечувати управління веб сайту (менеджери/ модератори/ райтери/ SEO спеціалісти)	4
П3	Особи, які забезпечують працездатність веб сайту (адміністратори)	5
П4	Авторизовані користувачі, яким не надано право доступу до ІзОД (клієнти/зареєстровані користувачі)	2
П5	Не авторизовані користувачі, яким не надано право доступу до ІзОД (не зареєстровані клієнти/зловмисники/ конкуренти та інші)	5

Таблиця 2.7 Специфікація моделі порушника за місцем дії

Позначення	Визначення категорії	Потенціальний рівень загроз
Д1	з робочих місць персоналу ІТС, але без доступу до місць розміщення обладнання ІТС	3
Д2	З робочих місць персоналу ІТС, а також місць розміщення обладнання ІТС, де обробляється інформація, яка підлягає захисту	4
Д3	Без доступу до приміщень, в тому числі з зовнішніх каналів зв'язку, з можливістю застосування технічних засобів здобуття інформації оптичними, акустичними каналами.	2

Таблиця 2.8 Специфікація моделі порушника за рівнем кваліфікації та обізнаності

Позначення	Визначення категорії	Потенціальний рівень загроз
К1	Не володіє знаннями та інформацією про порядок функціонування ІТС, не має навичок щодо користування штатними засобами обробки інформації системи та захисту інформації	1
К2	Має навички щодо користування ПК на рівні користувача	3
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення і операційних систем, а також практичними навичками роботи з засобами обробки інформації	4
К4	Володіє знаннями щодо: функціонування засобів та механізмів обробки інформації та її захисту, що використовуються на ІТС та їх недоліків.	5

Таблиця 2.9 Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз

Позначення	Визначення категорії	Потенціальний рівень загроз
З1	Має фізичний доступ до компонентів ІТС, але не є авторизованим користувачем ІТС (адміністратор хостінгу)	2
З2	Має можливість запуску програм, що реалізують функції обробки інформації	3
З3	Має можливість керування функціонуванням ІТС, тобто конфігурує програмне забезпечення ІТС. (адміністратор веб сайту/ адміністратор хостінгу)	4

Таблиця 2.10 Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Визначення категорії	Потенціальний рівень загроз
М1	Безвідповідальність (недбалість, ненавмисне порушення)	3
М2	Корислива цілеспрямованість (зловмисне порушення)	5

Таблиця 2.11 Специфікація моделі порушника за часом дії

Позначення	Визначення категорії	Потенціальний рівень загроз
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час)	3
Ч2	Під час функціонування ІТС	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	2

Профілі порушників всіх категорій наведено в таблиці, у колонці «Рівень загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 2.12 Профілі можливостей порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Адміністратор веб сайту	П2	М2	К1	З1	Ч3	Д2	18
Адміністратор хостінгу	П2	М2	К2	З1	Ч3	Д2	20
Менеджер магазину	П2	М2	К2	З1	Ч3	Д2	20
Райтер компанії	П1	М1/М2	К2	З1	Ч3	Д2	21
Клієнт компанії	П2	М1/М2	К3	З3	Ч3	Д3	21

Продовження таблиці 2.12 Профілі можливостей порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума
Клієнт з особистим кабінетом	П1	М1/М2	К2	З1	Ч3	Д2	21
Дилер компанії	П1	М1/М2	К2	З1	Ч3	Д2	21
Представник конкурентів/зловмисник/хакер	П4	М1/М2	К4	З3	Ч3	Д3	20

З таблиці 2.12 видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становлять: адміністратор хостінгу, адміністратор веб ресурсу, хакери, дилери.

Тому організація роботи цих особ повинна бути найбільш контрольованою, оскільки вони є основними потенційними порушниками безпеки інформації.

2.3.2. Модель загроз

За результатами впливу на інформацію та систему її обробки, загрози поділяються на:

1) Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам розмежування доступу до інформації.
2) Порушення цілісності інформації (Ц) - повне або часткове знищення, викривлення, модифікація інформації, нав'язування хибної інформації тощо.
3) Порушення доступності інформації (Д) - часткова або повна втрата працездатності системи, блокування доступу до інформації в результаті некоректних дій адміністраторів, технічного обслуговуючого персоналу.

Таблиця 2.13 Шкала оцінки ймовірності реалізації загрози

Оцінка ймовірності	Характеристика
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Зроблено якісну оцінку ймовірності реалізації загрози та визначено сукупний рівень загрози. Результати аналізу викладені в таблиці 2.14

Таблиця 2.14. Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
1	Ін'єкційні атаки	Відсутність перевірки введених полів форм.	3	КЦ	3	Зовнішня	3
		Відсутність перевірки завантажувальних файлів	2	ЦК	3	Зовнішня	2,5
2	Порушена автентифікація	Відкрита сторінка автентифікації адміністратора, такі як: - /administrator в Joomla!, - /wp-admin/ в WordPress, - /index.php/admin в Magento, - /user/login в Drupal.	5	КЦД	3	Зовнішня	4

		Дозвіл користувачам використовувати підбір комбінації імені користувача та пароля для цих сторінок;	3	КЦД	4	Зовнішня	3,5
		Використання стандартних, слабких або добре відомих паролів, таких як Password1 або admin/admin;	5	КЦД	5	Зовнішня	5
		Слабкі або неефективні процеси відновлення облікових даних та забутих паролів, у тому числі «відповіді на основі знань»;	5	КЦД	4	Зовнішня /Внутріш ня	4,5
		Не використовує багатофакторну автентифікацію;	4	КЦД	3	Зовнішня /Внутріш ня	3,5
		Надає ідентифікатори сеансу в URL.	3	КД	2	Внутріш ня	2,5

Продовження таблиці 2.14 Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
		Дозвіл користувачам використовувати підбір комбінації імені користувача та пароля для цих сторінок;	3	КЦД	4	Зовнішня	3,5
		Використання стандартних, слабких або добре відомих паролів, таких як Password1 або admin/admin;	5	КЦД	5	Зовнішня	5
		Слабкі або неефективні процеси відновлення облікових даних та забутих паролів, у тому числі «відповіді на основі знань»;	5	КЦД	4	Зовнішня/Внутрішня	4,5

Продовження таблиці 2.14 Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
		Використання стандартних, слабких або добре відомих паролів, таких як Password1 або admin/admin;	5	КЦД	5	Зовнішня	5
		Слабкі або неефективні процеси відновлення облікових даних та забутих паролів, у тому числі «відповіді на основі знань»;	5	КЦД	4	Зовнішня/Внутрішня	4,5
		Не використовує багатофакторну автентифікацію;	4	КЦД	3	Зовнішня/Внутрішня	3,5
		Надає ідентифікатори сеансу в URL.	3	КД	2	Внутрішня	2,5

Продовження таблиці 2.14 Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
3	Незахищеність критичних даних	Програма автоматично шифрує номери кредитних карток у базі даних. Однак при отриманні ці дані автоматично розшифровуються, що дозволяє вразливості SQL-впровадження отримувати номери кредитних карток у вигляді відкритого тексту	3	К	4	Зовнішня/Внутрішня	3,5
		Программа зовсім не шифрує дані	5	К	5	Зовнішня/Внутрішня	5
		База даних паролів використовує прості хеші для зберігання паролів усіх користувачів.	4	К	3	Внутрішня	3,5

Продовження таблиці 2.14 Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
4	Зовнішні об'єкти XML	Зловмисники можуть завантажувати XML або включати шкідливий вміст у документ XML	3	КЦД	5	Зовнішня	4
5	Порушення контролю доступу	Доступ до панелі керування хостингом/адміністративної панелі.	5	КЦД	5	Зовнішня/Внутрішня	5
		Доступ до сервера через FTP/SFTP/SSH.	2	КЦД	5	Зовнішня/Внутрішня	3,5
		Доступ до адміністративної панелі.	3	КЦД	4	Зовнішня/Внутрішня	3,5
		Доступ до інших програм на сервері.	2	КЦД	3	Внутрішня	2,5

Продовження таблиці 2.14 Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
		Доступ до бази даних	2	КЦД	4	Зовнішня/Внутрішня	3
6	Небезпечна конфігурація	Невиправлені недоліки	5	КЦД	3	Зовнішня/Внутрішня	4
		Конфігурації за замовчуванням	5	КЦД	4	Внутрішня	4,5
		Наявність сторінок, що не використовуються	5	КЦД	3	Внутрішня	4
		Непотрібні служби	4	КЦД	3	Внутрішня	3,5
7	Міжсайтовий скриптинг	Ресурс або API включає в себе неперевірене і неекрановане введення користувача як частина виводу HTML	3	КЦД	3	Зовнішня/Внутрішня	3

Продовження таблиці 2.14 Аналіз загроз та вразливостей

№	Загроза	Вразливість	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка
8	Використання компонентів з відомими вразливістю	Програмне забезпечення не підтримується або застаріло	5	КЦД	4	Внутрішня	4,5
		Не знання версії всіх використовуваних вами компонентів	5	КЦД	2	Внутрішня	3,5
		Не своєчасно оновлена базову платформу	5	КЦД	2	Внутрішня	3,5
		Розробники програмного забезпечення не перевіряють сумісність оновлених чи виправлених бібліотек	3	КЦД	3	Внутрішня	3

Згідно аналізу в таблиці 2.14 Аналіз загроз та вразливостей можна виділити основний список загроз, які мають найбільшу загальну оцінку небезпеки.

2.4 Основні методи та засоби оцінки рівня захищеності корпоративного веб сайту

Аналіз захищеності умовно можна розділити такі способи його проведення:

- інструментальне обстеження(використання спеціальних алгоритмів, які в автоматичному режимі проводять аналіз та тестування на проникнення);
- ручний аналіз захищеності;

2.4.1 Інструментальне обстеження

При проведенні інструментального обстеження web-сайтів в першу чергу використовуються сканери безпеки (а в більшості випадків ними і обмежуються), що дозволяють шляхом здійснення перевірок об'єкта досліджуваного виявити його схильність до всіляких вразливостей.

Інструментальне обстеження є найпростішим і, як наслідок, найпоширенішим способом проведення аналізу захищеності. Через те, що автоматизований аналіз використовує шаблонні методи, то якість аналізу значно падає. Подібна ситуація обумовлена насамперед функціональними обмеженнями автоматизованих засобів.

Сервіси, які призначені для аналізу рівня захищенності:

- Netsparker
- Acunetix
- Core Impact
- Nessus
- Burpsuite
- Zed Attack Proxy (ZAP)

2.4.2. Ручний аналіз захищеності

Порівняно з попереднім способом ручний спосіб пошуку вразливостей у web-сайтах дозволяє виявити більше вразливостей, дозволяє провести перевірки, які неможливо було виконати під час проведення інструментального обстеження. Однак варто відзначити, що на його виконання було витрачено набагато більше часу, ніж під час проведення аналогічних робіт з використанням інструментальних засобів.

Цей спосіб часто застосовується в тому випадку, коли щодо веб-сайту неможливо або дуже важко провести інструментальне сканування. Прикладом подібних web-сайтів можуть бути ресурси, що використовують продуману модель захисту від вразливостей.

Для ручного тестування була використана операційна система
Kali Linux, на яку встановлені фреймворки:

- w3af
- Wireshark
- Metasploit

2.5 Порівняння результатів аналізу рівня захищеності

Аналіз рівня захищеності виконавця згідно з керівництвом методології OSSTMM.

OSSTMM - документ, досить складний для читання та сприйняття.

Але він містить велику кількість актуальної та дуже докладної інформації з безпеки. Це також найвідоміший посібник з безпеки на планеті з приблизно пів мільйоном завантажень щомісяця. Причина такої популярності в наступному: ці інструкції приблизно на десятиліття випереджають решту документів в індустрії безпеки. Ціль OSSTMM — у розвитку стандартів перевірки безпеки Інтернету. Цей документ призначений для формування найбільш детального основного плану для тестування, що, у свою чергу, забезпечить досконале та всебічне випробування на проникнення. Незалежно від інших організаційних особливостей, таких як корпоративний профіль постачальника послуг із тестування на проникнення, це випробування дозволяє клієнту переконатись у рівні технічної оцінки.

2.5.1 Аналіз рівня захищеності корпоративного веб сайту інструментальним обстеженням

OWASP Zed Attack Proxy (ZAP) - сканер вразливостей веб-застосунків, створений проектом OWASP і має велику функціональність.

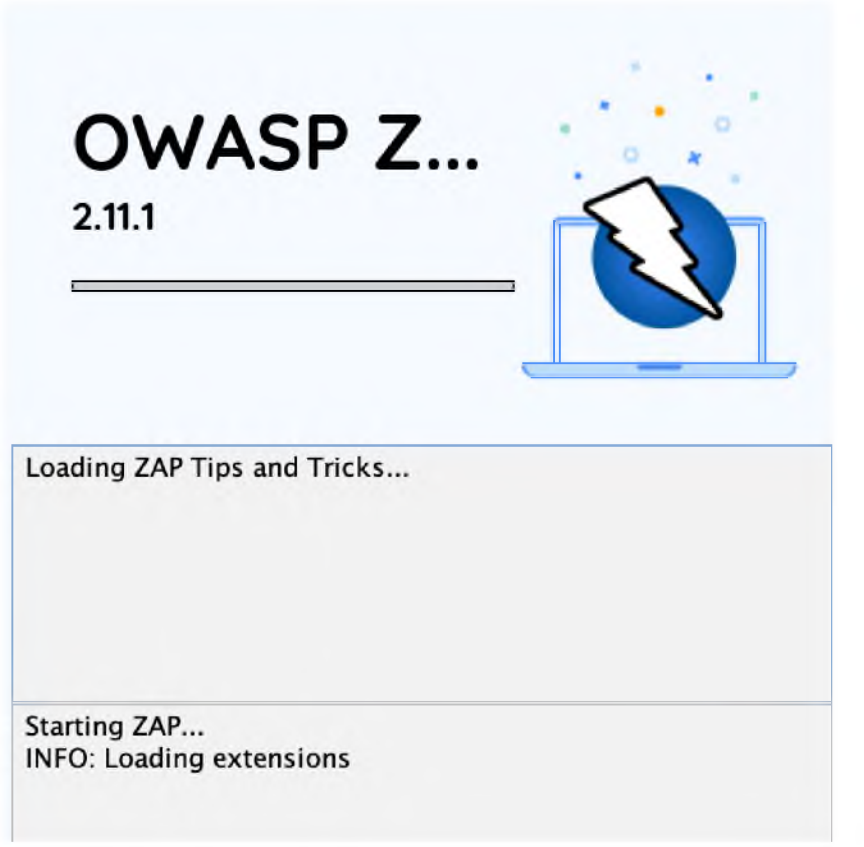


Рисунок 2.3 Запуск OWASP ZAP.

Після обходу сайту ZAP проводить низку різних перевірок на наявність загальних вразливостей веб сайту. Вони вказані на вкладці Alerts (Оповідання) у нижньому лівому куті. Наприклад, на Рисунку 2.4 наведено уразливості, виявлені ZAP у додатку DVWA.

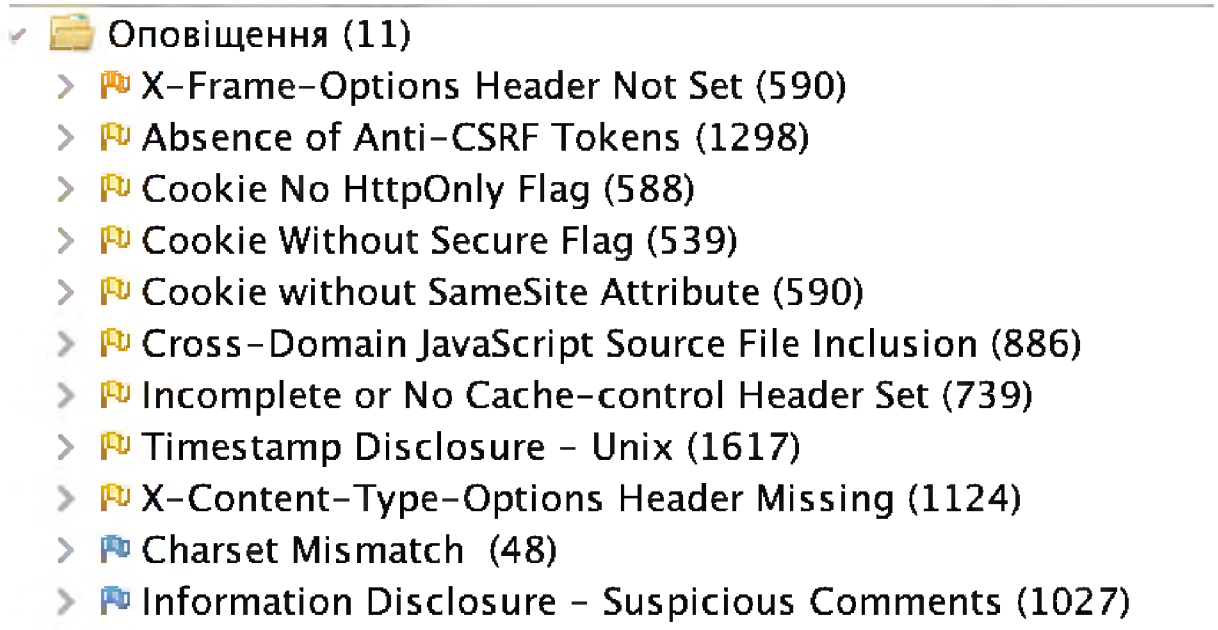


Рисунок 2.4 Результати аналізу OWASP ZAP

Надалі розглянемо знайдені вразливості на основі аналізу за допомогою.

2.5.2 Аналіз рівня захищеності корпоративного веб сайту ручним обстеження

Для цього розділу вам знадобиться :

- Kali Linux;
- OWASP Broken Web Applications (BWA).

OWASP BWA – попередньо налаштована віртуальна машина OWASP із колекцією вразливих веб-застосунків. Ми будемо працювати на віртуальній машині з одним з таких додатків – Damn Vulnerable Web App, DVWA.

У цьому розділі ми розглянемо інструменти, призначені для виявлення можливих вразливостей у веб-застосунках. Деякі з цих інструментів, зокрема Burp Suite та OWASP ZAP, виходять за рамки оцінки вразливостей для веб- та хмарних програм і надають можливість атакувати ці вразливості, про що ми також поговоримо.

На основі інформації, яку ми отримуємо з результатів роботи різних інструментів, ми можемо визначити напрямок нашої атаки для отримання доступу до системи. Це стосується і атак на паролі, і вилучення даних з баз даних або самої системи.

Надалі проведемо сканування за допомогою nikto - базовий сканер безпеки веб-сервера, який представлено на рисунку 2.5.

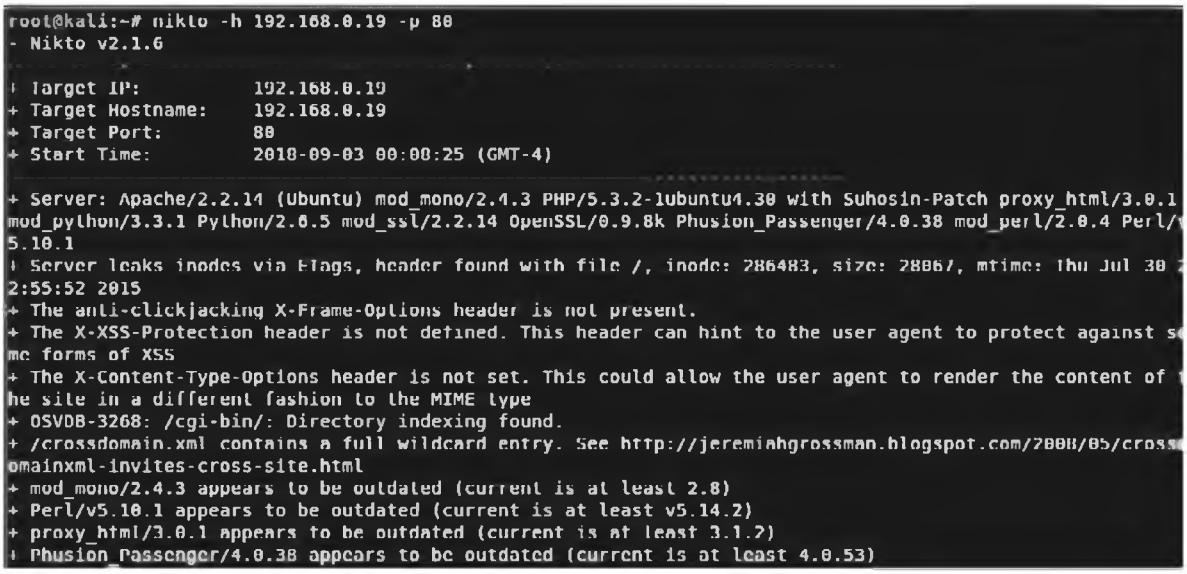


Рисунок 2.5 Сканування веб сайту за допомогою nikto.

Далі у результатах відображає коди OSVDB. OSVDB – це абревіатура бази даних вразливостей з відкритим вихідним кодом, який представлено на рисунку 2.6.

CVE Reference Map for Source OSVDB

Source	OSVDB
Description	Open Source Vulnerability Database (OSVDB) entry
URL	http://osvdb.org/
Notes	

This reference map lists the various references for OSVDB and provides the associated CVE entries or candidates. It uses data from CVE version 20061101 and candidates that were active as of 2019-06-11.

Note that the list of references may not be complete.

OSVDB:100007	CVE-2013-6796
OSVDB:10001	CVE-2004-2516
OSVDB:100030	CVE-2013-6936
OSVDB:1001	CVE-1999-0417
OSVDB:100106	CVE-2013-6374
OSVDB:100113	CVE-2013-4164
OSVDB:100191	CVE-2013-6795
OSVDB:10023	CVE-2004-1689
OSVDB:100342	CVE-2013-4212
OSVDB:100363	CVE-2013-4558
OSVDB:100364	CVE-2013-4505
OSVDB:10037	CVE-2004-2475

Рисунок 2.6 Результат сканування nikto.

Також був використаний ручний аналіз файлів з програмним кодом.

Корпоративний веб сайт використовує наступні доповнення:

- створений на замовлення файловий менеджер;

- додано плагіни для роботи з файлами;
- додані плагіни для роботи з API “Нова Пошта”;

Аналіз файлів з програмним кодом файлового менеджера показало наступні загрози:

- немає функції аналізу завантажених файлів;
- GET параметр передаєть у URL заголовку;
- в кінці сторінки виводиться результати запросу до БД MYSQL;
- розмежування доступом діє тільки на звичайних користувачів;
- до опису файлу можна записати SQL ін’єкцію(перевірки на правильність вводу немає);
- паролі користувачів зберігаються не в зашифрованому вигляді;
- немає обмежень завантаженого файлу;
- менеджер не шифрує файли для передачі на сервер;

Аналіз файлів плагіну для роботи з файлами показало наступні загрози:

- плагін не може вивести кирилицю в назві файлу;
- плагін не шифрує файли для передачі на сервер;

Аналіз файлів плагіну для роботи з Новою Поштою не показало критичних загроз.

2.6 Побудова системи захисту для систем керування контентом

З проробленої роботи у розділі 2.5 було виділено наступний перелік загроз, для яких буде будуватись система захисту корпоративного веб сайту.

Для побудови комплексу захисту системи керування контентом треба охопити загальні правила, які слід виконати для всіх користувачів WordPress та персональні рекомендації для особливих задач.

2.6.1 Загальні способи організації захисту

До загальних способів організації захисту можна віднести:

1. Використовуйте добрий логін.

Захист сайту на WordPress починається з елементарного створення гарного логіну. Встановлюючи WordPress, користувачі часто використовують логін, який програма установки пропонує за замовчуванням, а саме admin. Це те, що перевіряють боти, що шукають дірки у безпеці вашого сайту, в першу чергу. Використовуючи цей логін, ви надаєте половину необхідної інформації для хакерів, і їм залишається тільки підібрати пароль.

2. Використовуйте складний та унікальний пароль.

Захист адмінки WordPress, звичайно, неможливий без складного доброго пароля. Важливо, щоб він був унікальним і включав цифри, літери різних регістрів, знаки пунктуації, символи та інше. Паролі типу: pass, 1q2w3e4r5t6y, 87654321, qwerty, abc123, 111111, 1234, дата вашого народження і т.д. - Не є надійними, але багато користувачів продовжують їх використовувати. Приклад хорошого пароля: pcVaOF8r39. Звичайно, вам складно буде запам'ятати такий пароль, але для цього існує ряд програм, які зберігають і генерують паролі, а також можуть бути інтегровані в інтерфейс браузера (наприклад, Password Agent, KeyPass, Roboform і т.д.)

3. Оновлювати версію WordPress.

WordPress дбає про своїх користувачів, і тому в адміністративній панелі управління ви можете знайти повідомлення про вихід нової версії. Рекомендуємо здійснити оновлення, як тільки ви побачите його, оскільки одним із найпоширеніших проломів у захищеності вашого сайту є використання застарілої версії платформи.

4. Приховувати WordPress.

WordPress за замовчуванням додає номер поточної версії у вихідний код файлів і сторінок. І оскільки часто не завжди вдається оновлювати версію WordPress, це може стати слабким місцем вашого сайту. Знаючи, яка у вас версія WordPress, хакер може завдати багато шкоди.

За допомогою файлу functions.php можна заборонити виведення інформації про версію платформи. Для цього вам необхідно відкрити файл functions.php,

розташований у кореневій папці поточної теми вашого сайту (wp-content/themes/поточна_тема_wordpress), та додати наступний код:

```
remove_action('wp_head', 'wp_generator');
```

Або ж можна додати наступний код у файл functions.php:

```
/* Hide WP version strings from scripts and styles
* @return {string} $src
* @filter script_loader_src
* @filter style_loader_src
*/
function fjarrett_remove_wp_version_strings( $src ) {
global $wp_version;
parse_str(parse_url($src, PHP_URL_QUERY), $query);
if ( !empty($query[‘ver’]) && $query[‘ver’] === $wp_version ) {
$src = remove_query_arg('ver', $src);
}
return $src;
}
add_filter( 'script_loader_src', 'fjarrett_remove_wp_version_strings');
add_filter( 'style_loader_src', 'fjarrett_remove_wp_version_strings');

/* Hide WP version strings from generator meta tag */
function wpmudev_remove_version() {
return”;
}
add_filter('the_generator', 'wpmudev_remove_version');
```

Крім вищесказаного, у папці будь-якої теми WordPress, ви знайдете файл header.php. У ньому також вказується версія вашої установки, що для хакера дуже цікавим, як згадувалося раніше. Видаливши наступний рядок з файлу, ви позбавитеся цієї зайвої інформації:

```
<meta name=”generator” content=”WordPress <?php bloginfo ('version'); ?>” />
```

5. Завантажуйте теми та плагіни з надійних ресурсів.

WordPress є настільки поширеним, що все більше розробників створюють для нього готові теми та плагіни. У той час як більшість з них полегшать роботу з вашим сайтом і розширять його функціональність, деякі можуть приховувати в собі дуже неприємні наслідки у вигляді вірусів та відчиняти хакерські двері. Використовуйте лише перевірені ресурси для завантаження тем і плагінів, наприклад, wordpress.org, а також звертайте увагу на всі попередження про шкідливість файлів. Як і у випадку із самим WordPress, важливо вчасно оновлювати плагіни до останніх версій.

6. Регулярно перевіряйте ваш локальний комп'ютер на наявність вірусів.

Здійснення різних кроків із забезпечення безпеки сайту на WordPress – це добре, але за комп'ютером необхідно стежити. У вас повинен бути встановлений антивірус, що постійно оновлюється. В іншому випадку ви ризикуєте заразити ваш веб-сайт, завантаживши на нього вірусні файли.

7. Робіть резервні копії сайту.

Не всі атаки зловмисників можна попередити, але лише одна успішна атака може знищити всі зусилля по роботі над вашим сайтом. Рекомендуємо робити регулярні резервні копії веб-сайту. Багато хостингових компаній надають опцію серверних резервних копій і в разі чого ви зможете відновити сайт з копії, яка доступна на сервері.

Але рекомендуємо не обмежуватись такими серверними резервними копіями, оскільки важливо подбати про бекапи і з вашого боку. Ви можете вручну створювати копії вашого сайту з певною періодичністю або важливими оновленнями, але також існує ряд плагінів, які допоможуть автоматично створювати копії WordPress.

8. Використовуйте захищене з'єднання.

Якщо ви хочете завантажувати файли за допомогою FTP-клієнта, використовуйте захищений протокол з'єднання до сервера SFTP.

9. Створіть файл .htaccess.

.htaccess файл – це головний конфігураційний файл веб-сервера, який знаходиться у кореневій папці вашого веб-сайту. Якщо ви не маєте цього файлу, просто створіть його за допомогою текстового редактора.

Розширення файлу немає, тому вам достатньо буде назвати новий файл .htaccess.

Додаючи в цей файл різні варіації коду, можна значно убезпечити ваш сайт:

Код, що блокує доступ до вашого wp-config.php файлу, який містить важливу інформацію, необхідну для з'єднання з сервером MySQL та базою даних:

```
<Files wp-config.php>
order allow, deny
deny from all
</Files>
```

Код, який обмежить доступ до самого .htaccess файлу:

```
<files .htaccess>
order allow, deny
deny from all
</files>
```

Так само можна захистити будь-який інший файл, просто замінивши в коді «.htaccess» на назву необхідного файлу.

Код, який обмежує доступ користувачів з певною IP-адресою до вашого сайту:

```
order allow,deny
allow from all
deny from X.X.X.X
```

Так ви можете заборонити доступ підозрілих користувачів, спамерів та ботів, оскільки їх IP-адреси часто повторюються. Тим самим ви також зменшите навантаження на сервер.

Код, який дає доступ до вашого сайту лише користувачам з певною IP-адресою:

```
order deny,allow
```

deny from all

allow from X.X.X.X

Код, який обмежує доступ до адмін-панелі управління вашого сайту (це зручно, якщо у вас статична IP-адреса, і ви можете встановити доступ тільки для себе):

AuthUserFile /dev/null

AuthGroupFile /dev/null

AuthName “Access Control”

AuthType Basic

order deny, allow

deny from all

allow from X.X.X.X

10. Змініть префікс таблиці бази даних.

Захист WordPress від хакерів також посилиться, якщо усунути початковий префікс wp_ - це ускладнить пошук для зловмисників.

11. Обмежуйте кількість спроб доступу.

Найчастіше зловмисники роблять безліч спроб входу на ваш сайт, підбираючи пароль. Ви можете налаштувати систему таким чином, щоб IP-адреса була заблокована на кілька годин після певної кількості невдалих спроб входу.

Для цього ви можете використовувати додаткові плагіни, наприклад Login LockDown або Limit Login Attempts. У налаштуваннях цих плагінів, ви можете самостійно встановити кількість спроб входу та час блокування.

12. Видаліть readme.html та license.txt.

Файли readme.html і license.txt є в кореневій папці будь-якої установки WordPress. Вам ці файли ні до чого, а хакерам вони можуть надати їх злочину. Наприклад, щоб з'ясувати поточну версію вашого WordPress і багато чого іншого корисного для злому веб-сайту. Рекомендуємо видалити їх відразу після встановлення WordPress.

2.6.2 Особливі способи організації захисту

До особливого способу організації можна віднести:

- організація захисту для ділянки коду, який написан розробником власноруч;
- організація захисту для самописних плагінів/або плагінів які розробили на замовлення;
- організація захисту для зв'язків між сервісами, які підключені до сайту;

Додати методи перевірки завантаженого файлу. Для цього в запропонованому веб сайті використаємо структуру:

```
// Path to vendor directory.
$Vendor = __DIR__ . DIRECTORY_SEPARATOR . 'vendor';

// Composer's autoloader.
require $Vendor . DIRECTORY_SEPARATOR . 'autoload.php';

$Loader = new \phpMussel\Core\Loader();
$Scanner = new \phpMussel\Core\Scanner($Loader);
$Web = new \phpMussel\Web\Web($Loader, $Scanner);
$Loader->Events->addHandler('sendMail', new
\phpMussel\PHPMailer\Linker($Loader));

// Scans file uploads (execution terminates here if the scan finds anything).
$Web->scan();

// Fixes possible corrupted file upload names (Warning: modifies the content of
$_FILES).
$Web->demojibakefier();

// Cleanup.
unset($Web, $Scanner, $Loader);
```

яка відноситься до бібліотеки phpMussel.

Для передачі GET параметрів можна зробити декілька варіантів. 1 варіант - перейти на POST передачу даних, 2 варіант - використовувати $_SESSION.

Закрити виводи службової інформації з сторінок веб сайту.

видалити структури:

- echo $ArrResult;
- echo “<pre>”;
  print_r[$ArrResult];
  echo “</pre>”;

Додати перевірку введення даних в поля(додати валідацію форм).

Для цього можна використовувати структуру:

```
if(IsPost && Validation.IsValid()){
   // Process form submit
}
```

Додати методи шифрування паролів. Для цього використаємо структуру шифрування md5() або sha1(). Але функції для хешірування не стійки до брут-форсу, тому рекомендовано використовувати функцію crypt(), структура:

```
<?php
// пароль
$password = 'mypassword';

// получение хеша, соль генерируется автоматически; не рекомендуется
$hash = crypt($password);
?>
```

Також потрібно обмежити розміри завантажуваного файлу. Для цього відредагуйте файл init.php за допомогою структури:

```
ini_set('post_max_size', 'FILE SIZE');
ini_set('upload_max_filesize', FILE SIZE);
```

Де FILE SIZE - максимальний розмір завантажуваного файлу.

Для передачі файлів між клієнтом та сервером використовується HTTPS (TLS 1.2). Все, крім адресної частини URL - зашифровано.

Щоб уникнути будь-яких атак MITM, ви можете закріпити сертифікат сервера клієнта.

2.7 Оцінка ефективності запропонованого рішення

Після проробленої роботи у пункті 2.6, було зроблено повторний аналіз рівня захищеності корпоративного веб-сайту.

Результати проведення повторного аналізу представлені в польдальших звітах.

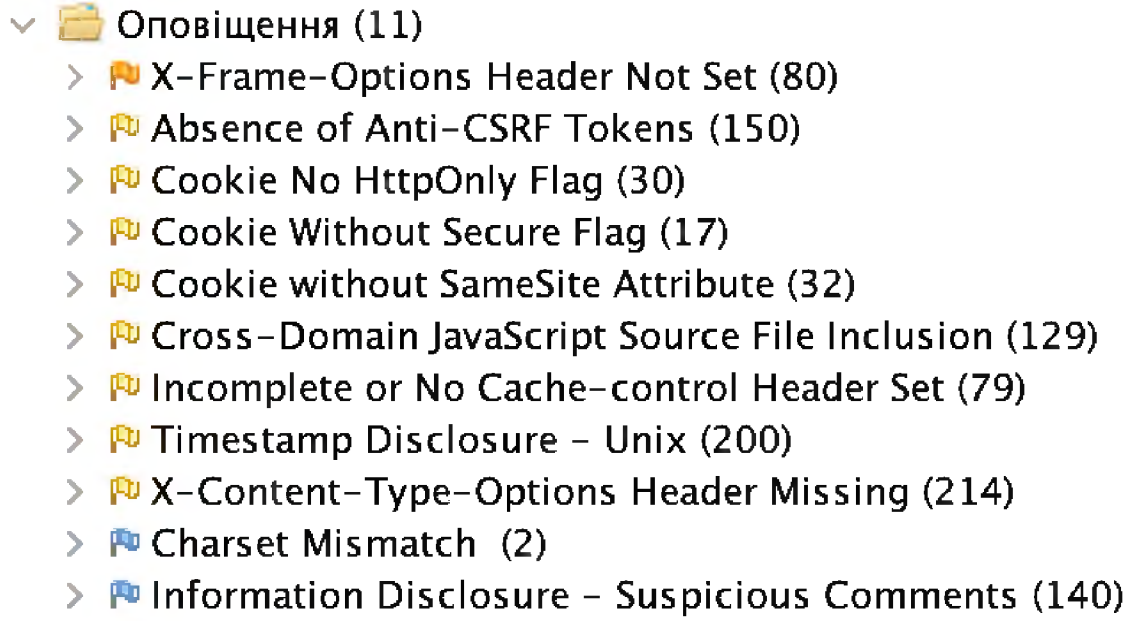
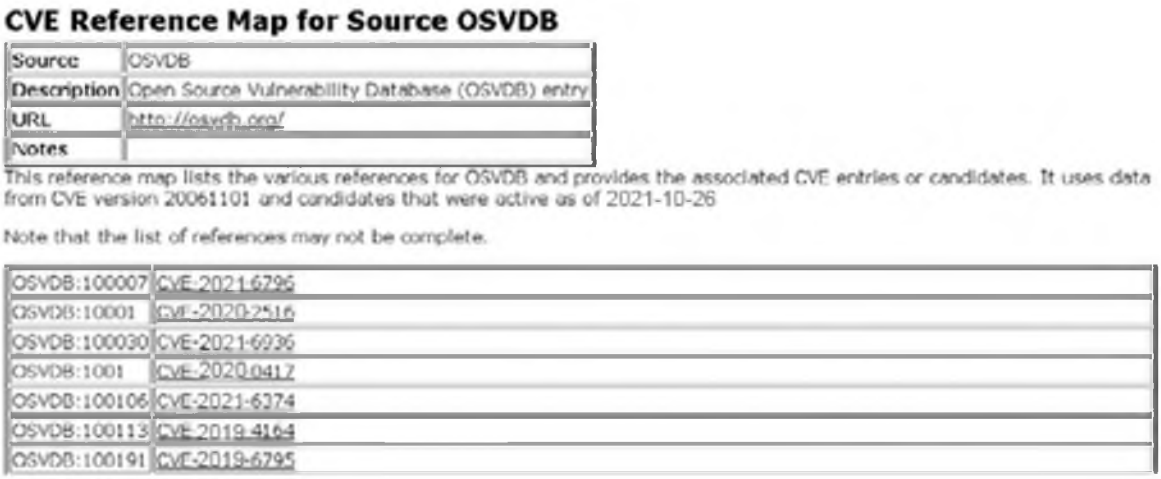


Рисунок 2.7 Результати сканування OWASP ZAP.

Результати ручного аналізу та сканування за допомогою nikto показані на рисунку 2.8.



CVE Reference Map for Source OSVDB

Source	OSVDB
Description	Open Source Vulnerability Database (OSVDB) entry
URL	http://osvdb.org/
Notes	

This reference map lists the various references for OSVDB and provides the associated CVE entries or candidates. It uses data from CVE version 20061101 and candidates that were active as of 2021-10-26

Note that the list of references may not be complete.

OSVDB:100007	CVE-2021-6796
OSVDB:10001	CVE-2020-2516
OSVDB:100030	CVE-2021-6936
OSVDB:1001	CVE-2020-0417
OSVDB:100106	CVE-2021-6374
OSVDB:100113	CVE-2019-4184
OSVDB:100191	CVE-2019-6795

Рисунок 2.8 Результат сканування nikto.

2.8 Висновки до розділу 2

У рамках другого розділу роботи було виконано обстеження на ОІД, розглянуто: архітектура мережі типового об'єкта інформаційної діяльності, аналіз інформації яка обробляється веб сайтом, модель загроз та вразливостей, основні методи та засоби оцінки рівня захищеності веб сайту. Проведено аналіз та оцінку загроз інформаційної безпеки і виділено значущі загрози. За результатами обстеження та аналізу загроз та вразливостей, визначено недосконалості використання систем керування контентом корпоративного веб сайту. Недоліки можуть стати причинами появи вразливостей системи та завдати збитків підприємству.

За результатами з проведеним аналізом, запропоновані до впровадження методи та засоби захисту інформації для забезпечення ефективної роботи всіх складових системи.

Аналіз загроз та вразливостей після впровадження запропонованих методів вказує на зниження рівня ризиків на систему через виявлені загрози.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Економічне обґрунтування доцільності впровадження методів забезпечення захисту веб сайтів на базі системи керування контентом WordPress.

Метою розрахунків є економічне обґрунтування доцільності впровадження методів забезпечення захисту веб сайтів. Для цього визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребують впроваджені методи;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження методів захисту.

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість впровадження методів захисту веб сайту визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

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

де $t_{тз}$ - тривалість складання ТЗ для впровадження методів захисту = 45 години;

$t_{в}$ - тривалість розробки концепції безпеки веб сайту = 32 години;

$t_{а}$ - тривалість процесу аналізу загроз та вразливостей = 80 години;

$t_{вз}$ - тривалість визначення вимог заходів, методів та засобів захисту = 70 години

$t_{озб}$ - тривалість виробу основних рішень з забезпечення безпеки веб сату = 135 години;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування корпоративного веб сайту = 213 години;

$t_{д}$ - тривалість документального оформлення результатів тестування на проникнення = 23 години;

t=45+32+80+70+135+213+23 = 598 години

3.1.2 Розрахунок витрат на впровадження систем захисту

Витрати на впровадження методів захисту корпоративного веб-сайту на базі CMS WordPress Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для впровадження методів захисту Змч.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 203\ 320 + 2517{,}58 = 205837{,}58 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 598*340 = 203\ 320 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для впровадження методів захисту корпоративного веб сайту визначається за формулою:

$$З_{мч} = t*С_{мч} = 598*4{,}21 = 2517{,}58 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0{,}7* 4 * 1{,}44 + ((5713*0{,}4)/1920) + ((9980*0{,}1)/1920) = 4{,}21 \text{ грн.}$$

Відповідно до розроблених рекомендації щодо застосування методів захисту веб сайту планується використання програмні засоби, які вже встановлені на підприємстві та додатково використовувати нові програмні засоби, які зазначені в таблиці 3.1.

Таблицця 3.1. Використанні програмні засоби

Програмний засіб	Вартість, грн	Тип ліцензії
Avast Business	980	1 раз на рік

Продовження таблиці 3.1 Використанні програмні засоби

Програмний засіб	Вартість, грн	Тип ліцензії
File Manager Plugin	2480	1 раз на рік
WordPress support +	1240	1 раз на рік
UpDate Manager WP	4300	1 раз на рік
Check File Plugin WP	980	1 раз на весь час
Всього	9980	

Таким чином, капітальні (фіксовані) витрати на впровадження систем захисту корпоративного веб сайту складає:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 226417{,}58 \text{ грн.}$$

де $К_{рп}$ – вартість впровадження методів захисту та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 0 грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, 3780 грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 0 грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 16800 грн.

Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad грн.$$

$$С = 9000 + 69453,27 + 0 = 78453,27$$

де $С_в$ - вартість відновлення й модернізації системи $С_в = 9000$;

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки = $С_{ак} = 0$ грн.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються $= С_н = 38000$ грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$С_з = З_{осн} + З_{дод}$, грн.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 26500 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо налаштувань інфраструктури безпечних підключень мобільних користувачів до інтрамережі підприємства потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (26500*12 + 26500*12*0,1)*0,25 = 87450 \text{ грн.}$$

З 01.01.2022 р. Ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 87450 * 0,22 = 19239 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \quad грн.,$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,7 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,44 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0,7*1920*1,44 = 1935,36 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%

$$С_{тос} = 226417,58*0,01=2264,17 \text{ грн}$$

Витрати на керування системою інформаційної безпеки визначаються:

$$С_к = 38000+87450+27588+1935,36+2264,17 = 157237,53 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 157237,53 грн.

3.2. Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку:

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 5 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує веб сайт , 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованного вузла або сегмента корпоративної мережі, 3 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 21500 грн./міс.;

$З_с$ – заробітна плата співробітників атакованного вузла, 18000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 16 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 2350000 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 2;

N – середнє число атак на рік, 13.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

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

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, 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 = ((18000 *12)/176)*5 = 6136,36 грн,

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережівключають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне введення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента

корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = ((21500 *12)/176)*2 = 2931,81 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{вп} = ((18000 *1)/176)*3 = 204,54 \text{ грн.}$$

Витрати на заміни встаткування або запасних частин можуть скласти 1450,50 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 2931,81 + 204,54 + 1450,50= 4586,85 \text{ грн.}$$

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

$$V = (2350000/2080)* (3+5+3) = 12427,88 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 6136,36 + 4586,85 + 12427,88 = 23151,09 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$В = 2 * 13 * 23151,09 = 601928,34 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці = 57%;

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 601928,34 * 0,57 - 78453,27 = 72028,815 \text{ грн.}$$

3.3 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:

$$ROSI = E/K, \quad \text{частки одиниці,}$$

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

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = 72028,815 / 226417,58 = 0,31 \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (10%);

$N_{інф}$ – річний рівень інфляції, (9%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,31 > (10 - 9)/100 = 0,31 > 0,01.$$

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

$$T = 1/0,31 = 3,2 \text{ роки.}$$

3.4 Висновок:

Розробка та впровадження запропонованих методів захисту веб сайтів на базі системи керування контентом WordPress є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 0,31 грн./грн., що означає отримання 0,31 грн. економічного ефекту на кожну гривню капітальних вкладень на впроваджені методи безпеки. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 3,2 років (біля 38,4 місяців). Капітальні витрати складають 226417,58 грн.

ВИСНОВКИ

У першому розділі кваліфікаційної роботі було описано стан інформаційної захищенності веб сайтів на базі систем керування контентом, наведені основні проблеми використання CMS систем, проаналізована нормативно-правова база, поставлена задача для подальшої роботи кваліфікаційної роботи.

У рамках другого розділу роботи було виконано обстеження типового ОІД, розглянуто: архітектуру типового веб сайту, особливості використання CMS системи, типову реалізацію корпоративного веб сайту на базі WordPress. Проведено аналіз ризиків інформаційної безпеки і виділено значущі загрози.За результатами обстеження та аналізу інформаційних ризиків, виділено недосконалості корпоративного сайту на базі системи керування контентом WordPress. Недоліки можуть стати причинами появи вразливостей системи та завдати збитків підприємству.

Згідно з проведеним аналізом, запропоновані до впровадження методів захисту інформації для забезпечення ефективної роботи всіх складових системи.

Згідно з отриманими даними під час розрахунку економічної частини - капітальні затрати становлять 226417,58 грн, експлуатаційні - 78453,27 грн. Згідно з підрахунками, впроваджені методи захисту є доцільними з економічної точки зору.

Загальний збиток від атаки на корпоративний веб сайту виробничого підприємства склав 740834,88 грн. Загальний ефект від впровадження системи інформаційної безпеки склав 72028,815 грн. Згідно с коефіцієнтом ROSI який становить 0,31 - впроваджені методи захисту є цілком доцільними. Термін окупності впровадження методів захисту веб сайту становить 3,2 років (біля 38 місяців).

ПЕРЕЛІК ПОСИЛАНЬ

1. Common Vulnerabilities and Exposures (CVE) [Электронный ресурс].// http://www.cve.mitre.org/about/.
2. National Vulnerability Database [Электронный ресурс].// https://nvd.nist.gov/general/nvd-dashboard/.
3. CWE – Common Weakness Enumeration [Электронный ресурс].// http://cwe.mitre.org/data/index.html.
4. OSVDB: Open Sourced Vulnerability Database [Электронный ресурс].// http://osvdb.org/
5. Common Attack Pattern Enumeration and Classification (CAPEC) [Электронный ресурс]. // http://capec.mitre.org/data/index.html
6. Луан Дж., Ван Дж., Сюе М. Автоматизоване моделювання вразливостей та перевірка для тестування на проникнення з використанням мереж Петрі [Текст] / Дж. Луан, Дж. Ван, М. Сюе // ICCCS (2). – 2016. – С.71-82.
7. Ву Д., Ліан Ю.-Ф., Чен К., Лю Ю.-Л. Метод ідентифікації та аналізу загроз безпеки на основі графіка атак [Текст] / Д. Ву, Ю.-Ф. Лянь, К. Чен, Ю.-Л. Лю // Jisuanji Xuebao (Китайський журнал комп'ютерів). – 2012. - вип. 35, н. 9. – С. 1938–1950.
8. Jha, S., Sheyner, O., Wing, J.M. Two Formal Analyses of Attack Graphs [Текст] / S. Jha, O. Sheyner, J.M. Wing // Proceedings of the 15th IEEE workshop on Computer Security Foundations. – 2002. – С. 49-63.
9. Гомер, Дж., Чжан, С., Оу, Х. Агрегування показників вразливості в корпоративних мережах за допомогою графіків атак [Текст] / Дж. Гомер, С. Чжан, Х. Оу та ін. // Журнал комп'ютерної безпеки. – 2013. – вип. 21, № 4. – С. 561–597.
10. Ноель С., Джаджодіа С., Ванг Л., Сінгхал А. Вимірювання ризику безпеки мереж за допомогою графіків атак [Текст] / С. Ноель, С. Джаджодіа, Л. Ванг, А. Сінгхал // Міжнародний журнал обчислень нового покоління. – 2010. – вип. 1, № 1.

11. Абрамов Є.С., Кобилев М.А., Крамаров Л.С., Мордвин Д.В. Використання графа атак для автоматизованого розрахунку мер протидія угрозам інформаційної безпеки мережі [Текст] / Е.С. Абрамов, М.А. Кобилев, Л.С. Крамаров, Д.В. Мордвин // Известия ЮФУ. Технические науки. – 2014. – No 2 (151). – С. 92-100.
12. Shandilya, V., Simmons, C. B., Shiva, S. Use of Attack Graphs [Текст] / Vivek Shandilya, Chris B. Simmons, Sajjan Shiva // Security Systems, Journal of Computer Networks and Communications. – 2014. – вип. 2014 р., ідентифікатор статті 818957, 13 стор.
13. Jajodia S., Noel S., O'Berry B. Topological analysis of network attack vulnerability [Текст] / S. Jajodia, S. Noel, B. O'Berry // Managing Cyber Threats: Issues, Approaches and Challenges. – 2005. – С.247-266.
14. Муньос-Гонсалес Л., Сгандурра Д., Баррере М., Лупу Е. Методи точного висновку для аналізу байєсівських графіків атак [Текст] / Л. Муньос-Гонсалес, Д. Сгандурра, М. Барре , Е. Lupu // IEEE Transactions on Dependable and Secure Computing. – 2017. – С. 1-14.
15. Лю, Ю., Ман, Х. Оцінка вразливості мережі з використанням байєсівських мереж [Текст] / Ю. Лю, Х. Ман // Data Mining, Intrusion Detection, Inform. Гарантія та безпека мереж даних. – 2005. – вип. 5812. – С. 61–71.
16. Frigault, M., Wang, L., Singhal, A., Jajodia, S. Measuring network security using dynamic Bayesian network [Текст] / M. Frigault, L. Wang, A. Singhal, S. Jajodia // Procs. 4-й семінар з якості захисту. – 2008. – С. 23– 30.
17. Пулсаппасіт Н., Дьюрі Р., Рей І. Динамічне управління ризиками безпеки з використанням байєсівських графіків атак [Текст] / Н. Пулсаппасіт, Р. Деурі, І. Рей // IEEE Transactions on Dependable and Secure Computing. – 2012. – вип. 9, № 1. - С. 61–74.
18. Aguessy, F., Bettan, O., Blanc, G., Conan, V., Debar, H. Hybrid Risk Assessment Model Based on Bayesian Networks [Текст] / F. Aguessy, O. Bettan, G. Blanc, V. Конан, Х. Дебар // 11-й міжнародний семінар з безпеки, матеріали. – 2016. – С.21-40

Додаток А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	22	
6	А4	2 Розділ	40	
7	А4	3 Розділ	9	
8	А4	Висновки	1	
9	А4	Список посилань	2	
10	А4	Додаток А. Відомість матеріалів кваліфікаційної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгуки керівників розділів	1	
13	А4	Додаток Г. Відгук керівника кваліфікаційної роботи	1	

Додаток Б. Перелік документів на оптичному носії

1.Пояснювальна_записка_Пономаренко.docx

2.Пояснювальна_записка_ Пономаренко.pdf

3.Презентація_ Пономаренко.pptx

Додаток В. Відгуки керівників розділів

Відгук керівника економічного розділу: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

Додаток Г. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу

студента групи 125м-20-2

Пономаренко Анатолія Сергійовича

на тему: «Методи захисту корпоративного веб-сайту виробничого підприємства на базі системи керування контентом WordPress»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 82 сторінках та 4 додатків.

Метою кваліфікаційної роботи є забезпечення достатнього рівня захищеності корпоративного веб сайту на базі системи керування контентом WordPress.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в роботі вирішуються наступні задачі: аналіз стану інформаційної безпеки, особливості організації захисту корпоративних сайтів типових виробничих підприємств, аналіз нормативно-правової бази у сфері захисту інформації, аналіз загроз та вразливостей після впровадження запропонованих методів захисту.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності захисту інформації корпортаивних веб.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Пономаренко А.С. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки 90 «відмінно».

Керівник кваліфікаційної роботи :

д.ф-м.н., проф. Кагадій Т.С. _____

Керівник спеціальної частини:

ст. викл. Тимофєєв Д.С. _____