

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

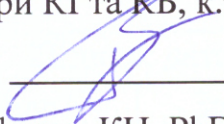
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту web-сайту на базі
CMS WordPress»

Виконав студент 3-го курсу групи КБк-22-1
спеціальності 125 «Кібербезпека»

 Роман ТОМАСОВ

Керівник доцент кафедри КІ та КБ, к.т.н.

 Олександр ПІРОГ

Рецензент завідувач кафедри КН, PhD, доцент

 Марина ГРАФ

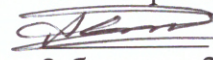
Житомир – 2025

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Томасов Роман Олегович

Тема роботи: «Проект підсистеми захисту web-сайту на базі CMS WordPress»

затверджена Наказом університету від 3 березня 2025 р. №80/с

Термін здачі студентом закінченої роботи 18 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Методи, інструменти та технології забезпечення захисту вебзастосунків,
розгорнутого на базі CMS WordPress.

Обладнання та програмне забезпечення:

1. CMS WordPress
2. Плагін Wordfence

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх
стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

Студент  Роман ТОМАСОВ

Керівник  Олександр ПІРОГ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Пошук теоретичної інформації	26.03.2025	Виконано
3	Вибір програмного забезпечення	01.04.2025	Виконано
4	Проведення дослідження CMS	15.04.2025	Виконано
5	Налаштування WordFence	01.05.2025	Виконано
6	Тестування WordFence	15.05.2025	Виконано
7	Написання пояснювальної записки	01.06.2025	Виконано
8	Захист	18.06.2025	Виконано

Студент  Роман ТОМАСОВ

Керівник  Олександр ПРОГ

АНОТАЦІЯ

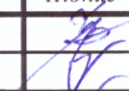
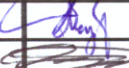
Метою кваліфікаційної роботи є розробка підсистеми захисту вебзастосунку, розгорнутого на базі MS WordPress. Особлива увага приділяється захисту від фішингових атак, контролю активності користувачів, аналізу трафіку, виявленню вразливостей та запровадженню багаторівневого захисту.

У роботі визначено основні завдання для забезпечення захисту вебресурсів на базі CMS WordPress та підвищення загального рівня кібербезпеки шляхом впровадження плагіна Wordfence Security. Проаналізовано ключові принципи та методи забезпечення безпеки вебсайтів, включаючи виявлення вразливостей, блокування шкідливого трафіку та запобігання несанкціонованому доступу. Розглянуто функціональні можливості Wordfence, зокрема сканування системи на наявність шкідливого коду, ведення журналу подій (Audit Log), застосування двофакторної автентифікації, контроль вхідного трафіку, блокування IP-адрес та реалізацію географічного блокування. Змодельовано процес впровадження технічних заходів захисту та налаштування параметрів плагіна для досягнення максимальної ефективності в підвищенні рівня безпеки сайту.

Наведено результати тестування безпекових механізмів плагіна Wordfence на базі CMS WordPress. Виявлено низку уразливостей у конфігурації системи та типових діях користувачів, що можуть бути використані зловмисниками, що підкреслює важливість впровадження додаткових заходів кібербезпеки.

Дипломна робота має обсяг 92 сторінки, містить 66 рисунків та 33 літературних джерела.

Ключові слова: WORDPRESS, WORDFENCE, CMS, ЗАХИСТ, БЕЗПЕКА, ПЛАГІНИ.

					ККІКБ.КР.Б – 125 – 49 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту web-сайту на базі CMS WordPress	Літ.	Арк.	Аркушів
Розроб.		Томасов Р.О.		17.06.25				
Керівник		Пірог О.В.		17.06.25			4	92
Реценз.		ГрафМ.С.		17.06.25		ФІКТ, Гр. КБк-22-1		
Н. контр.		Пірог О.В.		17.06.25				
Затверд.		Єфіменко А.А.		17.06.25				

ANNOTATION

The aim of the qualification work is to develop a security subsystem for a web application deployed on the WordPress CMS platform. Special attention is given to protection against phishing attacks, user activity monitoring, traffic analysis, vulnerability detection, and the implementation of multi-layered security.

The study defines the main tasks for ensuring the protection of web resources based on the WordPress CMS and improving the overall level of cybersecurity through the implementation of the Wordfence Security plugin. Key principles and methods of website security are analyzed, including vulnerability detection, malicious traffic blocking, and prevention of unauthorized access. The functional capabilities of Wordfence are examined, particularly system scanning for malicious code, event logging (Audit Log), implementation of two-factor authentication, incoming traffic control, IP address blocking, and geographic blocking. The process of implementing technical security measures and configuring plugin parameters has been modeled to achieve maximum efficiency in enhancing the security level of the website.

The results of testing the security mechanisms of the Wordfence plugin on the WordPress CMS platform are presented. A number of vulnerabilities were identified in the system configuration and in typical user behavior, which could be exploited by malicious actors. This highlights the importance of implementing additional cybersecurity measures.

The thesis consists of 92 pages, includes 66 figures, and references 33 literary sources.

Keywords: WORDPRESS, WORDFENCE, CMS, SECURITY, PROTECTION, PLUGINS.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пироз О.В.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ВЕБЗАСТОСУНКІВ	10
1.1 Важливість захисту вебзастосунків на базі CMS WordPress.....	10
1.2 Поняття інформаційної безпеки у вебзастосунках.....	12
1.3 Основні загрози інформаційної безпеки вебзастосунків	17
РОЗДІЛ 2 ВИБІР ТА НАЛАШТУВАННЯ ПЛАГІНА ЗАХИСТУ WORDPRESS .	25
2.1 Огляд архітектури CMS WordPress.....	25
2.2 Методи та засоби захисту WordPress-застосунків.....	30
2.3 Підбір плагіна	39
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ.....	46
3.1 Налаштування плагіну	46
3.2 Тестування WordFence.....	71
ВИСНОВКИ.....	87
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	89

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CMS – Content Management System

XSS – Cross Site Scripting

HTTP – HyperText Transfer Protocol

HTTPS – HyperText Transfer Protocol Secure

SSL – Secure Sockets Layer

RBAC – Role-Based Access Control

TLS – Transport Layer Security

WAF – Web Application Firewall

SDLC – Software Development Life Cycle

Jetpack – Jetpack Security

CSRF – Cross-Site Request Forgery

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному цифровому середовищі, де вебресурси відіграють важливу роль у діяльності компаній, установ та приватних користувачів, забезпечення безпеки вебсайтів стає одним із ключових аспектів кіберзахисту. Системи управління контентом, зокрема WordPress, завдяки своїй популярності, стають привабливою мішенню для кіберзлочинців. Атаки на вебсайти можуть призвести до витоку конфіденційної інформації, компрометації доступу, блокування сервісів або навіть повної втрати контролю над ресурсом.

Метою кваліфікаційної роботи є розробка підсистеми захисту web-сайту, розгорнутого на базі CMS WordPress.

Визначена мета обумовлює наступні завдання:

- дослідити загрози, характерні для CMS WordPress;
- проаналізувати сучасні типи атак на вебресурси, зокрема фішинг, brute-force та SQL-ін'єкції;
- розглянути можливості вибраного плагіна та обґрунтувати його вибір;
- налаштувати основні компоненти безпеки у вибраному плагіні;
- провести тестування ключових функцій плагіна;
- надати рекомендації для користувачів щодо захисту від атак;
- оцінити ефективність плагіна у виявленні та запобіганні фішинговим спробам і технічним загрозам.

Об'єктом дослідження є інформаційна безпека вебресурсів, побудованих на CMS WordPress.

Предметом дослідження є методи, інструменти та технології забезпечення захисту web-сайту, розгорнутого на базі CMS WordPress

Методологія дослідження. У роботі застосовано загальнонаукові методи дослідження, зокрема: аналіз, синтез, порівняння, моделювання, систематизація. Практичну частину проведено на основі експериментального методу – налаштування та тестування плагіна Wordfence у реальному середовищі WordPress. Оцінювання результатів здійснювалось шляхом спостереження за логами подій,

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ефективністю сканування, блокуванням підозрілих IP-адрес та країн, а також перевіркою функцій двофакторної автентифікації.

Практичне значення одержаних результатів. У ході виконання роботи було розроблено практичні рекомендації для підвищення рівня кіберзахисту вебсайтів, що функціонують на базі CMS WordPress. У межах дослідження проведено повноцінне тестування плагіна Wordfence Security, що включало сканування системи на наявність шкідливого коду, контроль дій користувачів через журнал подій (Audit Log), налаштування двофакторної автентифікації (2FA), аналіз та обмеження вхідного трафіку, блокування підозрілих IP-адрес, а також впровадження функції географічного блокування (Country Blocking) для обмеження доступу з окремих країн. Отримані результати мають практичну цінність і можуть бути використані адміністраторами сайтів, власниками вебресурсів та фахівцями з кібербезпеки як рекомендаційна основа для підвищення інформаційної безпеки.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних літературних джерел та додатку. Основний зміст роботи викладено на 93 сторінках друкованого тексту. Робота містить 66 рисунки. Список використаної літератури налічує 33 джерел, що викладені на 4 сторінках.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ВЕБЗАСТОСУНКІВ

1.1 Важливість захисту вебзастосунків на базі CMS WordPress

WordPress став однією з найпопулярніших систем керування контентом (CMS) у світі, керуючи понад 40% усіх вебсайтів в Інтернеті. Його гнучкість, простота використання та широкий набір тем і плагінів роблять його привабливим вибором для власників вебсайтів.

Забезпечення швидкого та легкого доступу для користувачів без технічного досвіду в Інтернеті стало однією з ключових причин популярності блогінгу по всьому світу. Ведення блогів сьогодні стало не лише популярним явищем, а й засобом комунікації для постійних користувачів мережі, а також для великих корпорацій, новинних організацій та освітніх установ. Ідея, що відсутність вебсайту організації означає відсутність самої організації, особливо актуальна для блогів.

Спочатку WordPress здобув популярність як платформа для ведення блогів [2]. Однак з часом все більше користувачів почали усвідомлювати широкі можливості цього інструменту. Завдяки активній спільноті, до якої входили розробники, програмісти та дизайнери, WordPress еволюціонував у потужну платформу для створення повноцінних вебсайтів, зокрема корпоративних. Важливу роль у цьому відіграв і вибір надійного хостингу, що забезпечував стабільну та ефективну роботу сайтів.

Також WordPress є найбільш популярним скриптом з системою управління вмістом, завдяки його простоті у встановленні та можливості швидко та легко змінювати зовнішній вигляд. Крім того, WordPress є безкоштовною технологією, що дозволяє використовувати її для створення як комерційних, так і приватних вебсайтів.

На сьогодні існує можливість вибору однієї з декількох програм та платформ для керування блогами та вебсайтами загалом. WordPress виокремлюється серед провідних платформ, пропонуючи широкий функціонал для ефективного

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

управління контентом. Відмінною особливістю WordPress є його здатність створювати вебсайти навіть без значних технічних знань.

Однак навіть найсучасніша система управління контентом не гарантує повної безпеки Інтернет-ресурсу без належної конфігурації та заходів забезпечення безпеки.

WordPress не є винятком серед систем керування вмістом блогів, адже вона володіє найбільшою популярністю та функціональністю. Проте, разом із своєю популярністю приходить і ризик безпеки, з якими необхідно рахуватися. Ось кілька причин, чому WordPress може бути уразливим:

- Типові файли для паролів і налаштувань: WordPress використовує стандартні файли для зберігання паролів та налаштувань, що розташовані у відомих каталогах. Це може зробити їх легкодоступними для злоумисників у випадку отримання часткового доступу.

- Панель адміністратора та кодова база: Панель адміністратора WordPress працює на тому ж домені та використовує ту саму кодову базу, що й решта вебсайту. Це може створити ризики безпеки, оскільки злоумисники, які мають доступ до панелі адміністратора, можуть отримати доступ до усіх ресурсів вебсайту.

- Плагіни та теми: Користувачі-адміністратори можуть інсталиувати плагіни та теми, які можуть мати вразливості або небажану функціональність. Неофіційні теми чи плагіни, а також ті, які не були оновлені або перевірені на безпеку, можуть стати джерелом потенційних загроз для веб-сайту.

Важливо бути уважними і вживати заходів безпеки, таких як регулярне оновлення платформи та плагінів, використання надійних паролів, а також перевірка безпеки та аудит коду для виявлення можливих вразливостей.

Таким чином з'ясовано, що WordPress є найбільш популярною системою управління вмістом. Однак вона не гарантує повної безпеки Інтернет-ресурсу без належної конфігурації та заходів забезпечення безпеки. Основними причинами вразливостей WordPress є: використання WordPress стандартних файлів для зберігання паролів та налаштувань, що розташовані у відомих каталогах; робота

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

панелі адміністратора WordPress на тому ж домені, що й решта вебсайту; можливість інсталювання плагінів та тем, які можуть мати вразливості або небажану функціональність.

1.2 Поняття інформаційної безпеки у вебзастосунках

Безпека вебзастосунків (Web AppSec) – це концепція, яка полягає в забезпеченні стабільної та безпечної роботи вебсайтів навіть у разі кібернападів. Йдеться про створення таких умов, за яких додаток здатен протистояти потенційним загрозам та зловмисним діям з боку третіх осіб.

Ця концепція включає впровадження комплексу засобів захисту, вбудованих у саму архітектуру вебзастосунку, що дозволяє зберігати його ресурси та дані в безпеці. Слід враховувати, що як і будь-яке інше програмне забезпечення, веб-додатки можуть містити помилки або недоліки. Частина з них є критичними вразливостями, якими можуть скористатися хакери, ставлячи під загрозу цілісність та функціональність системи.

Захист вебзастосунків передбачає системний підхід [3]: застосування принципів безпечної розробки, дотримання найкращих практик безпеки та впровадження відповідних механізмів захисту на всіх етапах життєвого циклу програмного продукту (SDLC). Це дозволяє виявляти і усувати слабкі місця ще на етапі проєктування, а також запобігати помилкам під час реалізації та впровадження додатку.

Основна суть інформаційної безпеки полягає в захисті організаційних даних від несанкціонованого доступу, спотворення, втрати або знищення. Також вона сприяє оптимізації інформаційних систем і підвищенню їх надійності. Її завдання – мінімізувати ризики порушення конфіденційності, некоректного видалення даних, помилок у зберіганні чи обробці інформації.

Принцип конфіденційності полягає в тому, щоб забезпечити доступ до інформації лише тим особам, які мають на це відповідні повноваження. Для досягнення цього необхідно впроваджувати ефективні системи контролю доступу

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

– як у цифровому середовищі (наприклад, використання паролів і шифрування), так і в фізичному (наприклад, персональні перепустки або системи ідентифікації).

Щоб уникнути ненавмисного розголошення конфіденційних даних, варто обмежувати обсяг інформації, якою обмінюються між співробітниками, а також регламентувати, хто має доступ до певної інформації. Надзвичайно важливим є також навчання персоналу: кожен працівник має володіти базовими знаннями з інформаційної безпеки та дотримуватися встановлених правил і стандартів.

Цілісність даних може бути порушена як випадково, так і навмисно. До ненавмисних причин належать збої в роботі систем, помилки під час введення інформації або недбале ставлення до збереження актуальних резервних копій. Водночас існують і навмисні загрози, наприклад, дії зловмисників, які змінюють чи підробляють дані. Одним із прикладів може бути фішингова атака, спрямована на зміну реквізитів банківських рахунків у системах фінансових виплат, що ставить під загрозу достовірність критичних даних.

З метою збереження цілісності даних користувачам рекомендується використовувати захищені канали для створення резервних копій і обміну інформацією виключно з авторизованими особами. Наприклад, спеціалізовані хмарні сервіси надають змогу не лише зберігати файли в захищеному середовищі, а й встановлювати права доступу, відслідковувати зміни, створювати історії версій та швидко відновлювати попередні версії файлів у разі потреби.

Такі інструменти є значно безпечнішими, ніж звичайний обмін файлами через електронну пошту або зберігання на знімних носіях, як-от USB-накопичувачі. Крім того, сучасні хмарні платформи дозволяють вести журнал активності, що полегшує моніторинг змін і вчасне виявлення можливих спроб порушити цілісність інформації.

Ключові методи підтримки цілісності даних охоплюють кілька важливих практик:

– Валідація даних: використання механізмів перевірки даних дозволяє вчасно виявляти помилки або спроби несанкціонованих змін. Такі перевірки забезпечують логічну узгодженість інформації та підтримують її достовірність.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

– Контроль змін: впровадження формалізованих процедур для фіксації та затвердження будь-яких змін у даних або системах гарантує, що всі модифікації відбуваються під наглядом і в межах дозволених повноважень. Це дозволяє уникнути випадкових чи навмисних спотворень інформації.

– Хешування: застосування криптографічних алгоритмів хешування дає змогу створити унікальний цифровий «відбиток» для кожного набору даних. У разі навіть незначної зміни вмісту даних хеш-код змінюється, що служить сигналом про потенційне порушення цілісності.

Доступність інформації є одним із ключових аспектів ефективної роботи будь-якої організації. Вона означає, що необхідні дані та системи мають бути доступними для авторизованих користувачів у потрібний момент часу. В умовах сучасного цифрового середовища, де багато бізнес-процесів автоматизовано, забезпечення безперебійного доступу до інформаційних ресурсів набуває особливого значення.

Підтримка доступності базується на кількох важливих практиках. По-перше, це резервування – створення копій важливих систем або даних, що дозволяє оперативно відновити доступ у разі відмови основного ресурсу. По-друге, застосовуються механізми відмовостійкості, наприклад, системи балансування навантаження або автоматичне перемикання на резервні сервери, які забезпечують продовження роботи без простоїв.

Ще одним важливим елементом є планування аварійного відновлення, що передбачає чітко прописані дії на випадок критичних ситуацій – таких як кібератаки, технічні несправності або природні катастрофи. Наявність подібного плану дозволяє швидко відновити працездатність систем і звести до мінімуму втрати для бізнесу.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				14
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.1 – Схема інформаційної безпеки

Уразливості вебзастосунків слабкі місця в програмній архітектурі чи налаштуваннях, які можуть бути використані зловмисниками для порушення безпеки системи. Такі вразливості нерідко виникають через недосконале опрацювання вхідних даних користувача, неправильну конфігурацію серверного середовища або загальні помилки в логіці побудови веб-програми.

На відміну від загальних мережових або системних уразливостей, ті, що пов'язані з вебзастосунками, виникають саме через постійну взаємодію користувача з інтерфейсом у багатокористувацькому середовищі. Така відкритість і доступність вебресурсів – ключовий фактор, яким активно користуються зловмисники для реалізації атак.

Щоб ефективно захистити вебдодаток, важливо не обмежуватись лише стандартними засобами, як-от звичайні сканери уразливостей. Потрібні спеціалізовані інструменти для аналізу програмної логіки, динамічного тестування та моделювання реальних атак. Розуміння найпоширеніших типів кіберзагроз –

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

таких як SQL-ін'єкції, XSS, CSRF тощо – дозволяє краще підготувати веб-додаток до потенційних викликів.

У сучасному середовищі інформаційної безпеки варто комбінувати автоматизовані засоби перевірки з ручним тестуванням, щоб виявити глибші, нетипові вразливості. Це допомагає не лише зміцнити захист, а й усвідомити реальні ризики, що можуть загрожувати бізнесу.

З поширенням веб-сайтів зросла і увага з боку кіберзлочинців. Чим більше людей використовують певне програмне забезпечення, тим більше з'являється потенційних мішеней, а отже, зловмисники витрачають більше зусиль і ресурсів на пошук уразливостей. Однак, вразливості є не лише у CMS – жодне програмне забезпечення не може бути абсолютно безпечним. Окрім того, розробники постійно додають нові функції, і кожен новий рядок коду збільшує не тільки можливості програми, але й потенційні ризики, адже зростає ймовірність появи вразливих місць.

Щоб зменшити кількість атак на CMS, необхідно регулярно встановлювати оновлення безпеки. Крім того, існують й інші заходи, що можуть підвищити рівень захищеності CMS.

Таким чином, безпека вебзастосунків є критично важливою складовою сучасного цифрового середовища, що потребує системного підходу та впровадження надійних механізмів захисту на всіх етапах життєвого циклу програмного продукту. Забезпечення конфіденційності, цілісності та доступності інформації досягається шляхом впровадження практик безпечної розробки, контролю доступу, резервного копіювання, моніторингу активності та регулярного оновлення CMS. Урахування типових уразливостей вебзастосунків і засобів протидії їм дає змогу суттєво знизити ризики, пов'язані з кібератаками, і сформувати надійну основу для створення ефективної підсистеми захисту.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Основні загрози інформаційної безпеки вебзастосунків

Вебзастосунки постійно стикаються з численними ризиками безпеки, які можуть призвести до серйозних наслідків, таких як витоки даних, тривалі простої систем, а також втрату довіри з боку користувачів.

Атаки типу «ін'єкція» виникають [7], коли зловмисники використовують вразливості в програмному забезпеченні для того, щоб впровадити шкідливий код у систему. Цей вид атаки дозволяє атакуючим виконувати несанкціоновані команди, отримувати доступ до конфіденційних даних або змінювати поведінку системи. Оскільки ін'єкційні атаки можуть мати серйозні наслідки і часто використовуються злочинцями, вони є однією з найбільших загроз для кібербезпеки в сучасному світі.

Ін'єкційні атаки здійснюються шляхом введення шкідливого коду в програмне забезпечення, що може призвести до несанкціонованого виконання команд, витоку або зміни даних. Ці атаки можуть проявлятися в різних формах, але серед основних типів виділяються:

- SQL-ін'єкція: Зловмисники використовують вразливості в запитах до бази даних для вставлення шкідливих SQL-інструкцій, що можуть порушити цілісність даних або призвести до їх витоку.
- Ін'єкція команд: Цей тип атаки дозволяє виконувати небажані команди на рівні операційної системи хоста, що дає можливість повного контролю над системою.
- XML-ін'єкція: Під час цієї атаки зловмисники маніпулюють XML-документами або їх обробкою, що може призвести до витоку даних або некоректної обробки інформації.

Крім того, ін'єкційні атаки можуть використовуватися для більш складних зловмисних цілей, таких як встановлення шкідливих скриптів чи програм на сервері, що забезпечує зловмисникам тривалий доступ до системи без виявлення. Враховуючи їх потенціал для серйозних порушень безпеки, запобігання таким атакам є критично важливим аспектом захисту інформаційних систем.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Атаки, що використовують ін'єкції, можуть мати катастрофічні наслідки. Коли зловмисники успішно експлуатують ці вразливості, вони можуть отримати доступ до конфіденційної інформації, такої як особисті дані, фінансові записи та чутливі бізнес-дані. Такий несанкціонований доступ до даних не лише представляє безпосередню загрозу для осіб і організацій, а й серйозно підриває довіру. У разі витоку даних ці відомості можуть бути використані для подальших атак, продані на чорному ринку або використані для шантажу через спеціалізовані сайти, контрольовані злочинцями.

Крім витоків інформації, атаки ін'єкціями можуть спричинити збої в роботі системи, перевантажуючи її або пошкоджуючи її функціональність. Перерви в обслуговуванні можуть мати серйозні наслідки, оскільки це може призвести до зупинки операцій і навіть продажів, що потребує тривалого відновлення та виправлення пошкоджень. Це призводить до фінансових втрат, зниження рівня задоволення клієнтів та можливих довготривалих репутаційних проблем.

Міжсайтовий скриптинг (XSS)

Також є загрози які називаються міжсайтовий скриптинг (XSS) – вразливість веб-безпеки, яка дозволяє зловмисникам маніпулювати взаємодією користувачів з вразливою веб-програмою. Ця вразливість дає можливість атакуючим обходити політику походження, що зазвичай запобігає взаємодії між різними веб-сайтами. Атаки XSS дають зловмисникам змогу діяти від імені користувача, виконувати дії, доступні для жертви, а також отримувати доступ до її даних. Якщо жертва має високі привілеї в системі, атакуючий може отримати повний контроль над усіма функціями та даними програми.

Міжсайтовий скриптинг (XSS) реалізується шляхом маніпулювання вразливим вебсайтом так, щоб він відправляв користувачам шкідливий JavaScript. Коли цей код виконується в браузері жертви, зловмисник отримує можливість повністю скомпрометувати взаємодію користувача з веб-програмою. Це може призвести до крадіжки конфіденційних даних, таких як сесійні куки або паролі, а також дозволити атакуючому виконувати дії від імені користувача, змінюючи налаштування, дані чи взаємодію з іншими сервісами. Зловмисник також може

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

використовувати XSS для подальших атак, наприклад, для поширення шкідливих посилань серед інших користувачів або для отримання доступу до системи, що має привілеї в додатку.

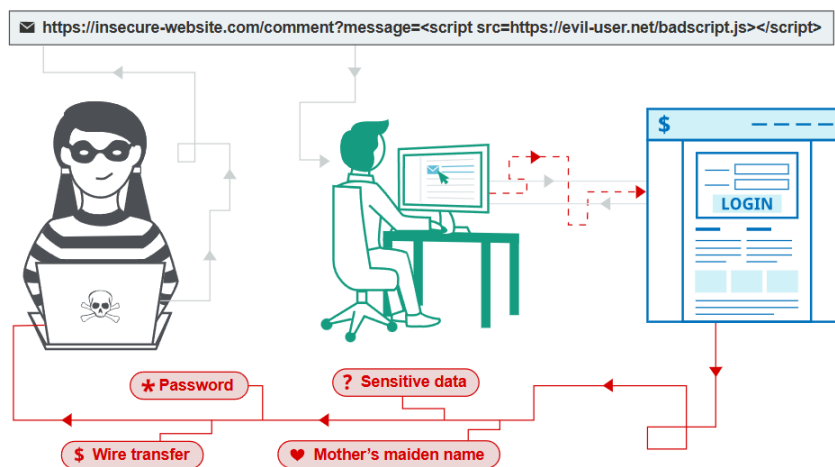


Рисунок 1.2 – Приклад схеми XSS

Існує три основні типи атак XSS:

- Відображена XSS – шкідливий скрипт надходить безпосередньо з поточного HTTP-запиту.
- Збережена XSS – шкідливий код зберігається в базі даних вебсайту і виконується при доступі до певної сторінки.
- XSS на основі DOM – вразливість полягає в коді на стороні клієнта, а не на сервері, що дозволяє атакувати через маніпуляцію з документом веб-сторінки в браузері.

Відображений XSS – це один з найпростіших типів міжсайтового скриптингу. Він виникає, коли веб-програма отримує дані в HTTP-запиті і безпосередньо включає ці дані у відповідь, не виконуючи належної перевірки чи санітарії. Такий підхід дозволяє зловмисникам вставити шкідливий JavaScript-код, який буде виконано в браузері користувача, коли він отримає відповідь від сервера. Це може призвести до крадіжки інформації, змінювання налаштувань облікових записів або виконання інших небажаних дій від імені користувача. Важливо зазначити, що відображений XSS часто використовується в фішингових атаках, коли зловмисник

створює спеціальні URL-адреси, що спрямовують жертв до скомпрометованих сторінок.

Збережений XSS (також відомий як постійний XSS або XSS другого порядку) виникає, коли веб-програма отримує дані з ненадійного джерела і небезпечним чином включає їх у свої подальші HTTP-відповіді.

Ці дані можуть надходити через різні канали, наприклад, через коментарі до дописів у блозі, нікнейми користувачів у чатах або контактні дані в замовленнях клієнтів. Інколи інформація може надходити з інших ненадійних джерел, таких як програма веб-пошти, що відображає повідомлення через SMTP, маркетингові платформи, які інтегрують дописи з соціальних мереж, або програми моніторингу мережі, які працюють з пакетами даних із мережевого трафіку.

При збереженому XSS шкідливий код зберігається на сервері і стає доступним для інших користувачів, що взаємодіють із скомпрометованими частинами сайту. Це може призвести до постійного виконання шкідливих скриптів для кожного, хто відвідує відповідну сторінку, що підвищує ризик масових атак. Оскільки код зберігається на сервері, він може залишатися активним навіть після перезапуску сервера, що робить його дуже небезпечним для користувачів і складним для виявлення без спеціалізованих засобів захисту.

XSS на основі DOM (також відомий як DOM XSS) виникає, коли вебпрограма використовує клієнтський JavaScript, який обробляє дані з ненадійного джерела небезпечним способом, зазвичай шляхом запису цих даних назад у DOM (Document Object Model) сторінки без належної перевірки чи санітарії.

У цьому випадку вразливість не пов'язана з серверною частиною програми, а з тим, як клієнтський код (JavaScript) взаємодіє з даними, які надходять від користувача або з інших ненадійних джерел, наприклад, через параметри URL, дані з форм або навіть через локальне сховище браузера. Якщо ці дані без перевірки вставляються в DOM, зловмисник може впровадити шкідливий JavaScript, який виконується в браузері жертви.

На відміну від інших типів XSS, DOM XSS відбувається виключно на стороні клієнта, і зловмисник використовує вразливості в JavaScript, щоб маніпулювати

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

DOM-елементами без участі сервера. Це робить такі атаки складними для виявлення та захисту за допомогою традиційних серверних методів безпеки. Наслідки таких атак можуть включати крадіжку сесійних куків, маніпуляції з інтерфейсом користувача або навіть виконання довільних дій від імені користувача без його відома.

Кросс-сайтове підроблення запитів (CSRF):

Міжсайтова підробка запитів (CSRF) – це атака, яка змушує автентифікованого користувача веб-застосунку виконувати небажані або шкідливі дії. За допомогою технік соціальної інженерії, таких як надсилання шкідливих посилань через електронну пошту або чат, зловмисник може маніпулювати користувачем і змусити його виконати дії, які вигідні атакуючому. Якщо жертвою є звичайний користувач, успішна CSRF-атака може призвести до виконання запитів на зміну стану, таких як переведення коштів або зміна контактної інформації. Однак якщо жертвою є адміністратор, атака може скомпрометувати весь веб-застосунок, дозволивши зловмиснику отримати повний контроль над системою.

CSRF дозволяє зловмиснику здійснювати небажані дії від імені жертви, використовуючи її привілеї та автентифікацію. Це відбувається, коли браузер автоматично додає до запитів всі облікові дані, пов'язані з сайтом, такі як куки сесії, IP-адреса або облікові дані домену. Тому, якщо користувач вже авторизований на сайті, система не може відрізнити підроблений запит, надісланий зловмисником, від легітимного запиту користувача.

Атаки зазвичай орієнтовані на зміни стану сервера, такі як зміна пароля, адреси електронної пошти або здійснення покупок. Оскільки зловмисник не отримує відповіді від сайту, атака має сенс лише тоді, коли вона змінює дані або ініціює дії, вигідні для атакуючого.

Зловмисник може також застосувати CSRF для отримання особистих даних жертви, використовуючи специфічну форму атаки, відому як CSRF для входу. В цьому випадку зловмисник змушує неавтентифікованого користувача увійти в обліковий запис, що дозволяє додавати або переглядати особисту інформацію, таку

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

як платіжні дані. Якщо жертва не підозрює про атаку, вона може безпечно заповнити ці дані, а зловмисник згодом скористається ними для своїх цілей.

Іноді CSRF-атаки можуть бути збережені на самому сайті, створюючи так звані "збережені CSRF-вади". Це можна досягти, вставивши шкідливі теги, такі як IMG або IFRAME, в поля, що приймають HTML, або використовуючи складніші методи, як міжсайтові скриптингові атаки. Якщо атака зберігається на сайті, вона стає набагато небезпечнішою, оскільки жертва, ймовірно, відвідає скомпрометовану сторінку, будучи вже авторизованою. Це підвищує ймовірність успіху атаки.

Соціальна інженерія

Соціальна інженерія сама по собі не є безпосередньо пов'язаною з конкретними платформами, такими як WordPress, але вона може бути використана як частина атак на сайти, які працюють на WordPress або будь-якому іншому веб-сервісі.

Соціальна інженерія – техніка маніпуляції, яка використовує людську довірливість або неуважність для отримання конфіденційної інформації, доступу або цінних ресурсів. У кіберзлочинності ці шахрайські методи, які можна вважати своєрідним "хакерством людей", зазвичай спрямовані на те, щоб підштовхнути довірливих користувачів до розкриття своїх даних, поширення шкідливих програм або надання доступу до обмежених систем. Такі атаки можуть відбуватися не тільки онлайн, а й особисто чи через інші види взаємодії.

Шахрайства, засновані на соціальній інженерії, ґрунтуються на розумінні людської поведінки та психології. Це дозволяє зловмисникам маніпулювати людьми, змушуючи їх робити дії, які вони зазвичай не виконували б. Якщо хакер розуміє, які фактори мотивують користувача, він може ефективно використовувати ці знання для обману.

Крім того, кіберзлочинці часто користуються відсутністю знань у користувачів щодо новітніх загроз. Оскільки технології швидко розвиваються, багато споживачів та працівників не мають достатнього уявлення про потенційні ризики, такі як випадкові завантаження або фішинг. Крім того, багато користувачів

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

недооцінюють цінність особистих даних, таких як номер телефону чи адреса електронної пошти. Через це багато людей не знають, як належним чином захистити себе та свою інформацію від зловмисників.

Більшість атак соціальної інженерії базуються на безпосередньому спілкуванні між зловмисником і жертвою. Замість того, щоб застосовувати методи грубої сили для отримання ваших даних, зловмисник намагається переконати користувача самотійно розкрити конфіденційну інформацію.

Однією з найбільших загроз соціальної інженерії є те, що атаки не завжди спрямовані на всіх користувачів. Одна обдурена жертва може надати достатньо інформації, щоб розпочати атаку, яка вплине на всю організацію.

З часом методи соціальної інженерії стали набагато складнішими. Фальшиві вебсайти або електронні листи тепер виглядають настільки реалістично, що легко можуть обдурити користувачів і змусити їх розкрити інформацію, яка може бути використана для крадіжки особистих даних. Соціальна інженерія стала одним з найпоширеніших способів, якими зловмисники обходять початкові заходи безпеки організацій, що дає їм змогу завдати подальших збитків та порушень.

Таким чином, вебзастосунки стикаються з численними загрозами, серед яких атаки типу ін'єкцій, міжсайтовий скриптинг (XSS), кросс-сайтове підроблення запитів (CSRF) та соціальна інженерія є одними з найбільш небезпечних. Ці загрози можуть призвести до серйозних наслідків, таких як витоки конфіденційних даних, збої в роботі системи, значні фінансові втрати, а також втрату довіри з боку користувачів. Враховуючи еволюцію методів атак і їх складність, критично важливо для організацій вживати заходів безпеки для запобігання таким інцидентам. Це включає в себе регулярне оновлення програмного забезпечення, впровадження відповідних фільтрів для введених даних, а також підвищення обізнаності користувачів про потенційні загрози, щоб мінімізувати ризики від атак і зберегти безпеку інформаційних систем.

Висновок до першого розділу

WordPress є найбільш популярною системою управління вмістом, однак її безпека без належної конфігурації та заходів захисту не може бути гарантована.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Основними причинами вразливостей WordPress є використання стандартних файлів для зберігання паролів і налаштувань у відомих каталогах, а також спільне розміщення панелі адміністратора з іншими частинами вебсайту, що може створювати додаткові можливості для зловмисників. Крім того, наявність плагінів та тем з потенційними уразливостями також сприяє зниженню рівня безпеки.

Забезпечення безпеки вебзастосунків є критично важливим для сучасного цифрового середовища, і вимагає системного підходу. Основним завданням є забезпечення конфіденційності, цілісності та доступності інформації через впровадження практик безпечної розробки, контролю доступу, резервного копіювання, моніторингу активності та регулярного оновлення системи управління вмістом. Потрібно враховувати типові уразливості вебзастосунків і застосовувати засоби протидії їм для значного зниження ризиків, пов'язаних з кібератаками, що дозволить створити надійний захист інформаційних систем.

Основними загрозами для безпеки є атаки типу ін'єкцій, міжсайтовий скриптинг (XSS), кросс-сайтове підроблення запитів (CSRF) і соціальна інженерія. Такі загрози можуть призвести до серйозних наслідків, включаючи витоки конфіденційних даних, збої в роботі системи, фінансові втрати та втрату довіри користувачів. Враховуючи еволюцію методів атак і їх складність, для організацій критично важливо вживати заходів безпеки, включаючи регулярне оновлення програмного забезпечення, впровадження фільтрів для введених даних і підвищення обізнаності користувачів. Це допоможе мінімізувати ризики від атак і забезпечити безпеку інформаційних систем.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 2 ВИБІР ТА НАЛАШТУВАННЯ ПЛАГІНА ЗАХИСТУ WORDPRESS

2.1 Огляд архітектури CMS WordPress

CMS (система керування вмістом) – це потужне програмне забезпечення, яке дає змогу будь-якому користувачеві, навіть без технічних знань, створювати, редагувати та керувати вебсайтами. Важливість таких платформ зростає, оскільки вони дозволяють значно спростити процес розробки сайту та зекономити час. WordPress, зокрема, є однією з найбільш популярних CMS у світі, займаючи понад 43% глобального ринку. Завдяки своїй простоті та великій кількості доступних плагінів, ця платформа стала вибором номер один для багатьох бізнесів і приватних осіб.



Рисунок 2.1 – WordPress

WordPress має велику спільноту розробників і користувачів, що завжди готові допомогти. Величезний вибір ресурсів для навчання, форумів і блогів забезпечує безперервний доступ до корисних порад і рішень для різних проблем. Це робить платформу ідеальним варіантом як для новачків, так і для професіоналів.

За останніми даними, WordPress використовується для роботи понад 43% усіх вебсайтів, що вражає. Однак така популярність має і зворотний бік – вона автоматично привертає увагу злоумисників.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Оскільки велика кількість сайтів побудована саме на WordPress, хакери часто намагаються знаходити та використовувати вразливості в його системі. Плагіни й теми, хоч і розширюють функціональність, часто можуть містити недоліки в безпеці. Це створює додатковий ризик, адже не всі розробники приділяють достатньо уваги захисту свого коду.

На офіційній сторінці безпеки WordPress чесно визнається, що найбільш вразливими є саме сторонні плагіни та теми, які можуть стати слабкою ланкою в системі.

Щоб мінімізувати ризики, важливо не лише користуватись надійними розширеннями, а й бути обізнаним у найпоширеніших уразливостях. Складання чіткого переліку таких вразливостей допоможе користувачам краще захищати свої сайти та уникати потенційних атак у майбутньому.



Рисунок 2.2 – WordPress

У період з 2023 по 2024 рік було зафіксовано 5948 вразливостей у WordPress [10], і цікаво, що аж 97% з них були пов'язані саме з плагінами. Теми спричинили 3% проблем, а от ядро WordPress виявилося майже бездоганим – лише 0,2% вразливостей походили звідти, і ті не мали критичного характеру. Ці дані чітко демонструють, що найбільша загроза безпеці сайтів криється не в самому WordPress, а в додаткових розширеннях. Це ще раз підтверджує, наскільки важливо уважно підходити до вибору плагінів і тем, встановлювати лише перевірені продукти й не забувати регулярно оновлювати їх.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Найчастіші типи вразливостей у WordPress

SQL-ін'єкція, виникає тоді, коли дані, введені користувачем, не проходять належної перевірки або фільтрації, і потрапляють до бази даних у сирому вигляді. Це може статися, якщо не використовуються підготовлені запити або якщо розробник застосовує невідповідні методи очищення даних. Подібні атаки можливі й у WordPress, особливо коли функції безпеки застосовуються неправильно або взагалі ігноруються.

```
$variable = $_REQUEST['id'];

// Vulnerable, user input variable used directly in SQL query.
$wpdb->get_var("SELECT * FROM wp_users WHERE id = " . $variable);

// Vulnerable, esc_sql variables must be enclosed within quotes.
$wpdb->get_var("SELECT * FROM wp_users WHERE id = " . esc_sql($variable));

// Vulnerable, sanitize_text_field does not remove quotes or escape values.
$wpdb->get_var("SELECT * FROM wp_users WHERE id = " . sanitize_text_field($variable));
```

Рисунок 2.3 – Користувач передає певну змінну через параметри запиту в URL або за допомогою форми на сайті

Міжсайтовий скриптинг (XSS) в JavaScript, цей тип вразливості є однією з найпоширеніших загроз у сфері веб-безпеки й становить серйозну небезпеку як для користувачів, так і для компаній. Завдяки впровадженню шкідливих скриптів у веб-додатки, зловмисники можуть отримати доступ до конфіденційної інформації, перехопити користувацькі сесии або навіть діяти від імені жертв без їхнього відома. Саме тому для веб-розробників критично важливо не просто знати, що таке XSS (міжсайтове скриптування), а й активно впроваджувати методи захисту, щоб запобігти таким атакам.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

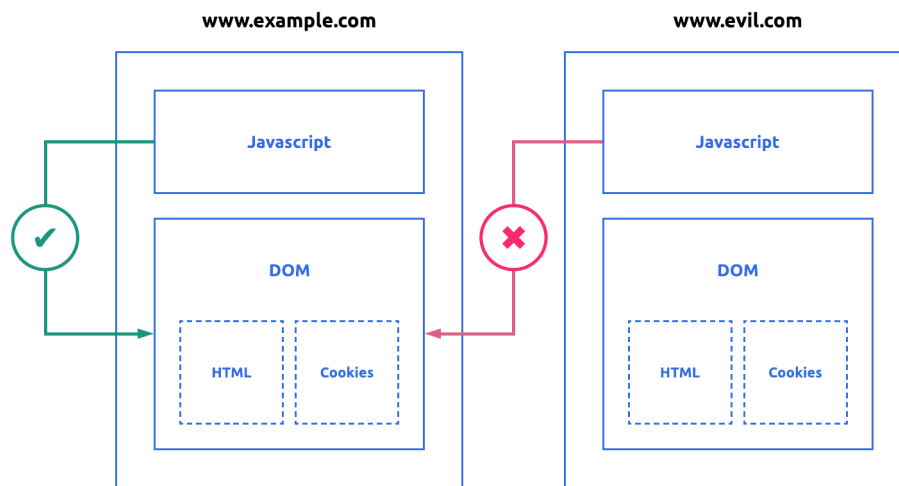


Рисунок 2.4 – Приклади XSS-атак

XSS-атаки відбуваються, коли зломисник вдається вставити шкідливі скрипти у веб-сторінки, що переглядаються іншими користувачами. Ці скрипти можуть виконуватись під час сеансу користувача, що дає можливість атакуючим викрадати файли cookie, токени доступу або навіть іншу конфіденційну інформацію, що відображається на сайті. Це може призвести до серйозних наслідків для безпеки користувачів і сайтів загалом.

Типи XSS-атак:

Зберігається XSS: Шкідливий скрипт постійно зберігається на сервері і виконується кожного разу, коли користувач отримує доступ до зараженої сторінки.

Відображений XSS: Скрипт вставляється у відповідь сервера, наприклад, через повідомлення про помилку або результат пошуку, де частина або всі введені дані користувача передаються назад у браузер.

XSS на основі DOM: Уразливість виникає в коді на стороні клієнта, де шкідливий скрипт виконується без взаємодії з сервером, через маніпуляції з документом HTML безпосередньо в браузері користувача.

Атака Cross-Site Request Forgery (CSRF) є однією з основних загроз для безпеки WordPress. Вона маніпулює браузером користувача, змушуючи його виконувати небажані операції на іншому сайті, де користувач уже автентифікований.

Як це відбувається? Ось три основні етапи атаки CSRF:

Міжсайтовий: атака включає взаємодію між різними веб-сайтами, де один сайт може отримувати дані або запити від іншого.

Запит: браузер користувача автоматично відправляє запит на сервер, наприклад, через методи GET або POST.

Підробка: зловмисник створює неправдивий запит, який має на меті виконання шкідливих дій на сайті.

Атака CSRF використовує активний сеанс користувача для відправлення підроблених запитів, що виглядають як запити від автентифікованого користувача. Це може призвести до виконання несанкціонованих дій, таких як зміна налаштувань облікового запису, витік конфіденційних даних чи виконання адміністративних завдань без відома користувача.

Користувач входить у свій обліковий запис на сайті WordPress «exampleforum.com». Тим часом він відвідує інший веб-сайт – «malicioussite.com», де ховається зловмисний скрипт. Цей скрипт надсилає запит на «exampleforum.com», намагаючись змінити електронну адресу користувача на адресу, якою контролює хакер.

Оскільки користувач вже автентифікований на «exampleforum.com», сервер вважає цей запит легітимним і обробляє його, хоча він насправді є зловмисним.

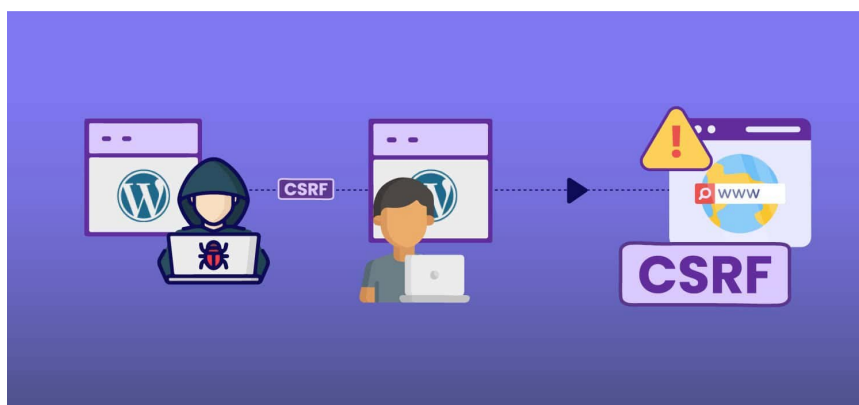


Рисунок 2.5 - Приклад Атака CSRF

Файли cookie сеансу є важливим елементом для автентифікації користувачів і управління сеансами на сайтах WordPress. Під час входу користувача на сайт сервер генерує унікальний ідентифікатор сеансу і зберігає його у вигляді cookie в

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

браузері користувача. Цей файл cookie потім надсилається разом із кожним запитом, що дозволяє серверу ідентифікувати та підтримувати сеанс.

Проте атака CSRF може використати цей механізм, подібно до атак на крадіжку cookie або захоплення сеансу. Зловмисники обманом змушують користувачів відправляти небажані запити, які автоматично включають ці сеансові cookie. Це дозволяє зловмисникам робити запити, які виглядають як дії від легітимного користувача, хоча насправді вони є шкідливими.

Існує безліч різноманітних атак на WordPress, таких як DDoS, файлові включення, Backdoor, а також інші методи, які значно погіршують безпеку веб-сайту. Кожна з цих атак несе серйозну загрозу, оскільки вони можуть призвести до втрати конфіденційної інформації, пошкодження даних, несанкціонованого доступу до адмін-панелі, а також до повної втрати контролю над сайтом.

Атаки, як DDoS (атаки на відмову в обслуговуванні) можуть перевантажити сервер і зробити сайт недоступним для користувачів, тоді як файлові включення дозволяють зловмисникам завантажувати та виконувати шкідливі скрипти на сервері. Використання задніх дверей (Backdoor) дозволяє хакерам отримувати доступ до сайту навіть після того, як інші вразливості були виправлені.

Ці та інші атаки часто спричиняють серйозні наслідки для безпеки, включаючи втрату довіри з боку користувачів, зниження позицій у пошукових системах, а також фінансові витрати на відновлення та виправлення пошкоджень. Тому важливо регулярно оновлювати платформу, використовувати надійні плагіни та теми, а також приймати інші заходи для захисту, щоб знизити ризик таких атак

2.2 Методи та засоби захисту WordPress-застосунків

У наш час, коли цифрова безпека набуває все більшого значення, кожен власник вебсайту має розуміти: захист – це не розкіш, а необхідність. Особливо це стосується сайтів на WordPress, адже ця платформа є найпопулярнішою у світі, обслуговуючи понад 40% усіх ресурсів в Інтернеті. Таке широке використання робить її привабливою цілью для кіберзлочинців.

Неналежно захищений сайт WordPress – це відкриті двері для зловмисників. Наслідки можуть бути серйозними: витік даних, втрата довіри користувачів,

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

проблеми з SEO, а іноді й прямі фінансові втрати. Саме тому, кожен адміністратор сайту повинен інвестувати час і ресурси в безпеку.

Витік даних – це одна з найсерйозніших загроз для будь-якого онлайн-проекту. Особливо небезпечно це для сайтів на WordPress, адже там часто зберігається чутлива інформація користувачів: електронні адреси, платіжні дані, особисті повідомлення тощо. Як тільки сторонні особи отримують до них доступ, наслідки можуть бути дуже серйозними.

Втрата довіри користувачів – це чи не найболючіше, що може статися. Люди перестають довіряти платформі, а повернути їхню впевненість – справа довга й витратна. До того ж, юридичні проблеми та можливі штрафи – це додатковий тягар для компанії. Іноді витік даних здатен підірвати весь бізнес.

Інвестувати в безпеку потрібно з перших днів розробки сайту. Профілактика проблем завжди краща за боротьбу з їхніми наслідками.

Якщо зловмисники отримають контроль над сайтом, вони можуть не лише вкрати облікові дані та особисту інформацію користувачів, а й використовувати платформу для поширення вірусів або шкідливих програм. У підсумку – постраждають ваші клієнти, а отже й ваша репутація.

Втрати прибутку також цілком реальні: недоступність сайту, блокування пошуковими системами, зменшення довіри клієнтів – усе це може негативно вплинути на доходи. А відновлення після такого удару часто вимагає значних зусиль і ресурсів.

Один із найефективніших способів убезпечити сайт WordPress без використання сторонніх плагінів – це грамотне налаштування прав доступу на основі ролей (RBAC) у поєднанні із зворотним проксі. Це рішення дозволяє створити гнучку систему управління дозволами, де кожен користувач має доступ лише до тих частин сайту, які відповідають його ролі.

Зворотний проксі, як проміжна ланка між клієнтом і сервером, може фільтрувати запити та додатково контролювати доступ до ресурсів. Разом із правильною файловою структурою та правами доступу це дає потужний захист від небажаних дій або вторгнень.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Правильне налаштування прав доступу до файлів WordPress – це основа безпеки сайту. Вони визначають, хто і що може робити з конкретними файлами чи папками, виходячи з ролі користувача. Якщо все налаштовано грамотно, кожен учасник команди працює в межах своїх повноважень, не маючи доступу до конфіденційних або критично важливих файлів.

Наприклад, співробітники, які мають базовий доступ, не зможуть втручатися в системні або адміністративні файли, які зарезервовані для користувачів із вищим рівнем доступу. Це можливо завдяки впровадженню контрольованого доступу на основі ролей (RBAC), що забезпечує зрозумілу і безпечну структуру управління файлами всередині WordPress.

Такий підхід не лише підвищує рівень безпеки, а й допомагає уникнути випадкових помилок, які можуть зашкодити роботі сайту.

Контроль доступу на основі ролей (RBAC) – це один із найзручніших і найнадійніших способів організації доступу до ресурсів у WordPress. Суть цього підходу полягає в тому, що користувачі отримують доступ до певних розділів сайту або файлів залежно від тієї ролі, яку їм призначено в системі.

Такий підхід дозволяє чітко розмежувати повноваження між учасниками команди або користувачами сайту: кожен має лише ті права, які йому необхідні для роботи. У результаті забезпечується не тільки зручне адміністрування, а й підвищений рівень безпеки, оскільки зменшується ризик несанкціонованого доступу до важливої інформації.

RBAC допомагає зберігати порядок і контроль у великій системі, де багато користувачів виконують різні функції. Це важливо і для внутрішньої ефективності, і для захисту даних.

Серед таких рішень особливу увагу заслуговує **Jetpack Security**, який часто очолює списки найкращих плагінів завдяки своїй надійності та широкому функціоналу.

Універсальні плагіни зазвичай поєднують одразу кілька ключових функцій – від ведення журналів аудиту та сканування на наявність шкідливого коду до вбудованих брандмауерів і засобів захисту при вході в систему. Це дозволяє

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

власникам сайтів забезпечити захист на всіх рівнях без необхідності встановлювати десятки додаткових модулів.

Jetpack Security – це комплексне рішення, яке автоматизує ключові аспекти захисту WordPress-сайтів. Завдяки поєднанню безкоштовних і преміальних функцій, він забезпечує базовий рівень безпеки навіть для невеликих проектів, водночас пропонуючи потужні інструменти для більш вимогливих користувачів.

Цей плагін охоплює як профілактичні засоби, так і засоби для реагування на інциденти, допомагаючи як запобігти загрозам, так і швидко відновитися після зламу. Серед основних можливостей:

- захист від атак методом перебору пароля (brute force),
- веб-додатковий брандмауер (WAF),
- фільтрація спаму,
- антивірусне сканування сайту,
- моніторинг часу простою,
- автоматичне створення резервних копій,
- ведення журналів активності користувачів,
- підтримка двофакторної автентифікації.

Хоча основні заходи безпеки можна реалізувати вручну, використання таких рішень, як Jetpack Security, значно полегшує процес налаштування та управління захистом.

Один із ефективних способів підвищення безпеки сторінки входу до WordPress – зробити її менш помітною для сторонніх. Стандартна адреса доступу до панелі адміністратора (наприклад, www.yoursite.com/wp-admin) є загальновідомою і часто використовується хакерами для спроб несанкціонованого входу. По суті, це як залишити на видноті ключі від дверей.

Щоб ускладнити завдання зловмисникам, рекомендується змінити URL-адресу сторінки входу. Це дозволяє створити додатковий бар'єр безпеки, знижуючи ймовірність автоматизованих атак. Таку зміну можна зробити як вручну, маючи FTP-доступ до файлів сайту, так і за допомогою спеціального плагіна, який спростить процес.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Захист панелі адміністрації від підбору пароля, простий та ефективний спосіб захистити панель адміністрації від атак на пароль – це плагін Login Lockdown. Плагін можна завантажити з офіційного репозиторію WordPress.org за посиланням: Login Lockdown.

Принцип його роботи полягає в тому, що при досягненні певної кількості невдалих спроб входу з одного IP, цей IP потрапляє до чорного списку, і доступ до сайту блокується. Цей плагін можна використовувати на будь-якому типі сайтів.

Щоб встановити плагін, потрібно завантижити та активувати плагін блокування входу. Налаштування плагіна доступні за адресою: <https://example.com/wp-admin/options-general.php?page=loginlockdown.php>.

Плагін не вимагає додаткових налаштувань, але за потреби можна змінити параметри на ваш розсуд.

Рисунок 2.6 – Налаштування Jetpack Security

Також для захисту вебзастосунку на базі WordPress можна використовувати протоколи SSL або TLS.

SSL (Secure Sockets Layer) – це технологія, яка забезпечує безпеку даних, що передаються між веб-сайтом і його відвідувачами. Ця технологія захищає конфіденційну інформацію, таку як особисті дані, паролі та платіжну інформацію.

Захист веб-сайту WordPress за допомогою SSL є важливим для забезпечення безпеки даних та підвищення довіри користувачів. На всіх наших сайтах

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

використовується SSL, що дає можливість бути впевненими в безпеці даних користувачів.

Сертифікат SSL є необхідним для будь-якого веб-сайту, який обробляє конфіденційну інформацію, оскільки він шифрує дані, що передаються між сайтом та його відвідувачами. Це ускладнює доступ хакерів до цієї інформації.

SSL також додає замок HTTPS в адресний рядок веб-переглядача, що дозволяє відвідувачам переконатися в безпеці сайту, підвищуючи довіру та надійність ресурсу.

Встановлення сертифіката SSL на веб-сайт WordPress є важливим з кількох причин. По-перше, це дозволяє серверу хостингу встановлювати безпечне з'єднання з веб-браузерами, що допомагає уникнути порушень безпеки, які можуть загрожувати як особистій інформації, так і даним клієнтів.

З цієї причини Google тепер штрафує сайти без сертифіката SSL. Наприклад, користувачі, які намагаються отримати доступ до таких сайтів, можуть побачити попередження "незахищене" або "ваше з'єднання не приватне".

TLS розшифровується як **Transport Layer Security**. Це протокол безпеки, який забезпечує захист як веб-сайту, так і його користувачів, шифруючи всі дані під час передачі від кінця до кінця. Згідно з Mozilla Developer Network (MDN):

Захист транспортного рівня (TLS), раніше відомий як рівень захищених сокетів (SSL), – це протокол, який використовується програмами для безпечного обміну даними в мережі, запобігаючи втручанню та прослуховуванню електронної пошти, веб-серфінгу, обміну повідомленнями та інших мережевих протоколів. Як SSL, так і TLS є клієнт/серверними протоколами, що забезпечують конфіденційність передачі даних за допомогою криптографії, гарантуючи безпеку мережевих комунікацій. Коли сервер і клієнт використовують TLS, це забезпечує, що ніхто, включаючи третю сторону, не зможе підслухати чи підробити повідомлення.

Всі сучасні браузери підтримують протокол TLS, вимагаючи від сервера надання дійсного цифрового сертифіката, який підтверджує його автентичність, щоб встановити безпечне з'єднання. Клієнт і сервер можуть також взаємно

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

автентифікувати один одного, якщо кожна сторона надасть власний цифровий сертифікат.

TLS, що є наступником протоколу Secure Sockets Layer (SSL), використовується для веб-браузерів та інших інтернет-програм і процесів, які потребують обміну даними. Як TLS, так і SSL є стандартами безпеки для Інтернету, хоча TLS є останньою версією протоколу. Обидва сертифікати перетворюють незахищений префікс URL-адреси HTTP (протокол передачі гіпертексту) на HTTPS (захищений протокол передачі гіпертексту).

Сертифікат TLS забезпечує захист веб-сайту WordPress і інформації користувачів, гарантуючи, що URL-адреса має префікс HTTPS. Це також підвищує легітимність і безпеку сайту в очах пошукових систем, зокрема Google. TLS використовує процес, званий рукоштовуванням TLS, для безпечного з'єднання користувача з веб-сайтом. Протокол шифрує дані наскрізно, що забезпечує їх захист від втручання з боку третіх осіб. Якщо хакер чи зловмисник намагався б перехопити дані сайту, захищеного TLS, він би побачив лише набір випадкових символів, а не використовувану інформацію. Крім того, TLS автентифікує кожен сеанс між користувачем і сервером, перевіряючи, що всі сторони є законними. Сертифікат TLS також допомагає підтримувати цілісність веб-сайту та покращує його репутацію в пошукових системах.

Наявність сертифіката TLS на веб-сайті забезпечує захист від зловмисних атак, хакерів та витоку даних, що робить його важливим елементом сучасної безпеки в Інтернеті. Це вже стандарт для більшості веб-браузерів. Наприклад, браузери Google Chrome і Mozilla Firefox попереджають користувачів, коли вони намагаються отримати доступ до незахищених HTTP-сайтів, що підвищує ризики для безпеки. Окрім цього, пошукові системи, зокрема Google, знижують рейтинги веб-сайтів, які не мають сертифіката SSL або TLS, що може негативно вплинути на їх видимість у пошукових результатах.

TLS також надає захист від можливих юридичних наслідків, пов'язаних з обробкою конфіденційної інформації. Наприклад, якщо веб-сайт зберігає особисті або платіжні дані користувачів без належного захисту, це може призвести до

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

серйозних юридичних наслідків. Це особливо важливо для бізнесів, які працюють з платіжними даними або зберігають конфіденційні медичні записи, де безпека має критичне значення.

Важливо забезпечити максимальний рівень безпеки для вашого веб-сайту, починаючи від основ. Хоча сертифікат TLS є лише одним з елементів комплексної безпеки сайту, він є одним із найпростіших і найефективніших способів підвищити безпеку вашого ресурсу.

Ще для захисту вебзастосунку можна використовувати плагіни безпеки, такі як iThemes Security або Wordfence

iThemes Security пропонує привабливе рішення всього за 199 доларів США на необмежену кількість сайтів, що робить його вигідним варіантом у сфері безпеки WordPress. Завдяки поєднанню широкого функціоналу та доступної ціни, цей плагін виступає серйозним конкурентом серед провідних рішень для захисту сайтів.

iThemes Security справляє враження одного з найслабших плагінів безпеки для WordPress серед протестованих. Хоча він пропонує кілька корисних функцій, таких як двофакторна автентифікація та підтримка складних паролів, на цьому його сильні сторони закінчуються. У ньому відсутній сканер шкідливого ПЗ, немає можливості автоматичного очищення зараженого сайту, і фактично немає вбудованого брандмауера.

Цікавим є те, що саме iThemes був першим плагіном, який підлягав тестуванню. Спочатку, з огляду на структуру сайту та процес налаштування, склалося враження, що розробники добре розуміються на безпеці WordPress. Проте це враження, на жаль, не підтвердилося на практиці – функціональність плагіна не відповідає очікуванням. Якщо сайт наразі працює з iThemes Security, рекомендується негайно провести перевірку на наявність шкідливого програмного забезпечення за допомогою альтернативних інструментів.

З іншого боку, iThemes Security має чудову функцію двофакторної автентифікації. Нам також сподобалося, як легко було застосувати reCAPTCHA на wp-login. І, нарешті, налаштування керування паролями користувачів були дуже

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

детальними та детальними. Крім того, є кілька пристойних функцій захисту WordPress, як-от блокування виконання PHP у папках. Забезпечення безпеки WordPress вимагає злагодженої роботи команди фахівців, які постійно аналізують новітні типи шкідливого програмного забезпечення та вразливості, що стосуються WordPress. Їх завдання – перетворювати ці загрози на оновлення для брандмауера та сигнатури для виявлення шкідливих кодів, а потім оперативно передавати ці захисні механізми користувачам у режимі реального часу.

Wordfence по праву вважається провідною командою у сфері безпеки WordPress на світовому рівні. Їхній плагін пропонує повноцінний комплекс інструментів для захисту сайтів, і саме постійні глибокі дослідження команди Wordfence лежать в основі тієї надійності, за яку їх цінують мільйони користувачів.

Варто зазначити, що для Wordfence безпека WordPress – це не лише частина бізнесу, а основна спеціалізація. Вони повністю зосереджені саме на цій галузі. Компанія підтримує цілодобову міжнародну команду реагування на інциденти, яка забезпечує оперативну допомогу – пріоритетним клієнтам гарантується відповідь на критичну загрозу протягом однієї години. Завдяки такому підходу Wordfence не просто захищає сайти, а встановлює стандарти безпеки в екосистемі WordPress.

У його арсеналі: брандмауер кінцевої точки, потужний сканер зловмисного ПЗ, захист входу (включаючи двофакторну автентифікацію), а також можливість моніторингу трафіку в реальному часі, що дозволяє швидко виявляти підозрілу активність.

Канал захисту від загроз постійно оновлює систему найсвіжішими правилами брандмауера, сигнатурами шкідливого ПЗ та списками небезпечних IP-адрес, забезпечуючи проактивний рівень безпеки. Окрім базового захисту, Wordfence пропонує гнучкі інструменти для блокування доступу за країнами, обмеження частоти запитів, виявлення змін у файлах ядра WordPress і багато іншого.

Крім основних функцій захисту, **Wordfence Security** надає детальний журнал подій, який дозволяє відстежувати всі дії користувачів і потенційні загрози на сайті – від спроб входу до змін у файлах. Це дає змогу адміністраторам реагувати на інциденти швидко й обґрунтовано.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Також плагін підтримує централізоване керування безпекою для кількох сайтів через **Wordfence Central**, що особливо зручно для розробників, агентств та адміністраторів великих проєктів. Крім того, команда Wordfence регулярно публікує звіти та аналітику щодо нових вразливостей у плагінах та темах, що допомагає користувачам вчасно вживати превентивних заходів.

У результаті Wordfence – це не просто захисний плагін, а справжня екосистема безпеки, яка забезпечує як технічний захист, так і інформаційну підтримку для постійного вдосконалення кібергігієни WordPress-сайтів.

Захист сайту на WordPress це необхідність у сучасному цифровому світі. Впровадження грамотного контролю доступу на основі ролей, використання зворотного проксі та встановлення сертифікатів SSL/TLS суттєво підвищують рівень безпеки. Використання надійних плагінів, таких як Jetpack Security чи iThemes Security, допомагає ефективно запобігти загрозам і зберегти довіру користувачів, що є ключовим для успішного онлайн-бізнесу.

2.3 Підбір плагіна

Забезпечення безпеки WordPress потребує роботи команди спеціалізованих аналітиків, які постійно досліджують новітні загрози, такі як шкідливе програмне забезпечення та експлойти. Вони створюють відповідні правила для брандмауера та сигнатури для виявлення шкідливих програм і оперативно надають ці оновлення клієнтам у режимі реального часу.

Wordfence справді заслужено вважається однією з найкращих команд у сфері безпеки WordPress. Їхній плагін охоплює всі основні аспекти захисту сайту, а основна сила – це глибокі аналітичні дослідження, які постійно оновлюють захисні механізми.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				39
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.7 – Wordfence Security

На відміну від багатьох інших сервісів, для Wordfence безпека – це не просто один із напрямів роботи, а головна спеціалізація. Особливо вражає те, що вони мають цілодобову міжнародну команду реагування, яка здатна вирішувати інциденти буквально за годину, що критично важливо для великих сайтів і серйозних проєктів.

Wordfence Security є потужним інструментом комплексного захисту сайтів на WordPress. Він включає брандмауер кінцевих точок, сканер шкідливого програмного забезпечення, розширені функції захисту під час входу, перегляд трафіку в реальному часі та багато інших можливостей.

Завдяки постійно оновлюваній стрічці загроз, Wordfence забезпечує сайт актуальними правилами брандмауера, сигнатурами шкідливих програм та списками небезпечних IP-адрес, що дозволяє ефективно реагувати на новітні кіберзагрози.

Наявність двофакторної автентифікації (2FA) та широкого набору додаткових функцій робить Wordfence одним із найповніших та найнадійніших рішень для забезпечення безпеки сайтів на платформі WordPress.

Брандмауер Wordfence побудований на основі набору спеціалізованих правил, які виявляють і блокують поширені типи атак, що активно використовуються в реальному середовищі. Ці шаблони атак мають чітко визначену структуру й не потребують складної обробки для аналізу запитів. Крім

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

того, брандмауер застосовує загальні шаблони, що дозволяють виявляти потенційно небезпечні запити навіть без точної відповідності відомим загрозам. Такі загальні правила допомагають запобігти атакам нульового дня (0-day), коли хакери намагаються використати ще не виправлені вразливості.

Оновлення правил брандмауера відбувається автоматично – без потреби в ручному втручанні користувача. Wordfence завантажує актуальні правила безпеки з власного центру мережеских операцій. Для преміум-користувачів це оновлення здійснюється в режимі реального часу: щойно з'являється нова загроза, брандмауер одразу отримує нові правила захисту. Сервери Wordfence «пінгують» сайт, щоб ініціювати миттєве оновлення та забезпечити максимальний захист.

Користувачі безкоштовної версії Wordfence також отримують ці оновлення, але з затримкою в 30 днів, що надає преміум-користувачам додаткову перевагу у швидкості реакції на нові кіберзагрози.

Переваги Wordfence:

- Потужний брандмауер (WAF): захищає сайт ще до завантаження WordPress, виявляє та блокує відомі та нові типи атак.
- Сканер шкідливого ПЗ: перевіряє файли ядра, тем, плагінів і базу даних на віруси та модифікації, порівнює з оригінальними файлами WordPress.
- Моніторинг у реальному часі: відображає активність користувачів, спроби входу, заблоковані IP, підозрілий трафік.
- Двофакторна автентифікація (2FA): додатковий захист облікового запису адміністратора.
- Автоматичні оновлення правил безпеки: преміум-користувачі отримують оновлення миттєво, безкоштовні – із затримкою.
- Глобальна база IP-адрес: автоматичне блокування підозрілих і шкідливих IP-адрес.

Недоліки Wordfence:

- Вплив на продуктивність: може сповільнювати сайт, особливо на слабкому хостингу.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

– Багато функцій тільки у платній версії миттєві: оновлення правил фаєрвола, розширене сканування, підтримка 24/7.

– Вимагає налаштувань: для оптимальної роботи користувачу потрібно розуміти основи безпеки WordPress.

– Велика кількість сповіщень: новачків можуть перевантажити часті повідомлення та попередження.

Wordfence є одним із найефективніших плагінів безпеки для WordPress, особливо якщо ним користується досвідчений адміністратор або сайт розміщено на продуктивному хостингу. Водночас, щоб отримати повний набір функцій, доцільно скористатися преміум-версією.

Якщо не забезпечувати належне обслуговування WordPress сайту, він може стати вразливим до атак шкідливого ПЗ та спаму. Тому для кожного користувача WordPress надзвичайно важливо подбати про захист свого ресурсу. Одним із надійних інструментів для цього є плагін iThemes Security, який виконує перевірку сайту на наявність вразливостей і допомагає вчасно вжити заходів для запобігання атакам.

Однак, якщо потрібно контролювати безпеку кількох сайтів одночасно, процес сканування кожного окремо може стати трудомістким. У такому випадку доповнення **InfiniteWP iThemes Security Addon** дозволяє централізовано переглядати всі знайдені вразливості на кількох сайтах WordPress, що значно економить час і спрощує адміністрування.

iThemes Security – це плагін для захисту WordPress-сайтів, який надає широкий набір інструментів, спрямованих на запобігання різноманітним загрозам і вразливостям безпеки.

iThemes Security позиціонується як плагін для захисту WordPress-сайтів, однак йому не вистачає ключових компонентів повноцінного захисту – зокрема, сканера шкідливого ПЗ, системи очищення заражень і брандмауера. Багато з його функцій більше схожі на формальність, ніж на реальні заходи безпеки.

Наприклад, плагін заявляє про здатність запобігати атакам ще до їх виникнення, відстежуючи вразливості. Проте фактично він не повідомляє

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

користувача в режимі реального часу й обмежується лише щотижневими електронними листами з інформацією про виявлені загрози.



Рисунок 2.8 – iThemes Security

Хоч у плагіні все ж є кілька корисних функцій, які дійсно працюють, їх недостатньо для комплексного захисту. Сам сайт iThemes для власного захисту використовує інший плагін безпеки, що ставить під сумнів ефективність їхнього власного продукту.

Плагін iThemes Security не має повноцінного брандмауера, хоча розробники заявляють про можливість блокування IP-адрес. Насправді ця функція працює нестабільно або зовсім неефективно. Захист від ботів, який пропонується, також є дуже обмеженим – замість фільтрації шкідливого трафіку він просто блокує індексацію сайту пошуковими системами, що може навіть нашкодити видимості ресурсу.

Користувачам дозволяється забороняти доступ для певних IP-адрес або user-agentів вручну, а також використовувати готовий список заборон від hackrepair.com. Проте ці функції реалізуються через редагування конфігураційних файлів сервера, таких як `.htaccess` чи `nginx.conf`. Ці файли дійсно дуже потужні, але складні у використанні, особливо для недосвідчених користувачів. Управління білими або чорними списками IP у таких файлах може бути незручним, трудомістким і призвести до помилок у роботі сайту.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Переваги iThemes Security

- Простий у використанні: інтуїтивно зрозумілий інтерфейс, підходить навіть для новачків, швидке налаштування за допомогою майстра конфігурації.
- Базовий набір функцій безпеки: захист від brute-force атак (підбір пароля), обмеження кількості спроб входу, приховування сторінки входу (login page), виявлення змін у файлах сайту.
- Підтримка двофакторної автентифікації (2FA): додає додатковий рівень захисту для входу в адмінку
- Email-сповіщення: Повідомлення про важливі події безпеки (зміни файлів, підозрілі входи тощо).
- Інтеграція з InfiniteWP: зручно керувати кількома сайтами WordPress з єдиного інтерфейсу.

Недоліки iThemes Security

- Відсутність вбудованого брандмауера: немає повноцінного фаєрвола для захисту на рівні сервера, як у Wordfence.
- Немає сканера та очищення шкідливого ПЗ: плагін не може виявити чи видалити віруси або шкідливий код.
- Обмеженість функцій у безкоштовній версії: багато корисних можливостей доступні лише в Про-версії.
- Деякі функції працюють через .htaccess/nginx.conf: для зміни чорного/білого списку IP потрібно редагувати серверні конфігураційні файли, що складно для початківців.
- Захист від ботів – слабкий: реалізований поверхнево, може впливати на індексацію сайту в пошукових системах.

Для налаштування безпеки сайту буде використовуватись плагін Wordfence, оскільки він забезпечує комплексний захист від атак, підбору паролів, сканувань вразливостей та інших кіберзагроз. Крім того, Wordfence дозволяє легко керувати політиками безпеки через зрозумілий інтерфейс адміністратора, забезпечуючи ефективний захист сайту без необхідності в глибоких технічних знаннях. Це робить його надійним рішенням для захисту сайтів на WordPress.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Висновок до другого розділ

WordPress є надзвичайно популярною та ефективною платформою для створення веб-сайтів завдяки своїй гнучкості, зручності та великій кількості доступних розширень. Проте саме її поширеність робить цю систему привабливою цілью для зловмисників. Основні загрози безпеці пов'язані не з ядром WordPress, а зі сторонніми плагінами та темами, які часто стають джерелом критичних вразливостей.

Щоб забезпечити надійний захист веб-сайту, важливо поєднувати технічні засоби безпеки – як-от оновлення, фільтрація даних, використання захищених плагінів – із підвищенням власної обізнаності щодо кіберзагроз. Лише комплексний і свідомий підхід до безпеки дозволить повноцінно використовувати всі переваги WordPress і водночас уникати серйозних ризиків.

Особливо ефективним є впровадження спеціалізованих інструментів безпеки – таких як Wordfence, який забезпечує фаєрвол, сканер вразливостей, захист входу, моніторинг трафіку в режимі реального часу, блокування IP-адрес, що підозріло себе поведуть, а також автоматичне сповіщення про потенційні загрози. Це дає змогу своєчасно реагувати на будь-які спроби несанкціонованого доступу та зменшити ризики зламу.

Комплексний підхід до захисту – разом із підвищенням обізнаності користувачів, налаштуванням резервного копіювання, використанням складних паролів і двофакторної автентифікації – є запорукою стабільної та безпечної роботи сайту в умовах постійно зростаючих кіберзагроз. Лише системна й проактивна безпека дозволить власникам сайтів уникати серйозних проблем і забезпечити довготривалу довіру з боку відвідувачів і клієнтів.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ

3.1 Налаштування плагіну

Для налаштування безпеки сайту буде використовуватись плагін **Wordfence Security**, оскільки він забезпечує надійний захист від зловмисників, включає функції брандмауера, сканера на віруси та інструменти для моніторингу активності на сайті.

Потрібно зайти на сайт WordPress, вибрати потрібний плагін та встановити.

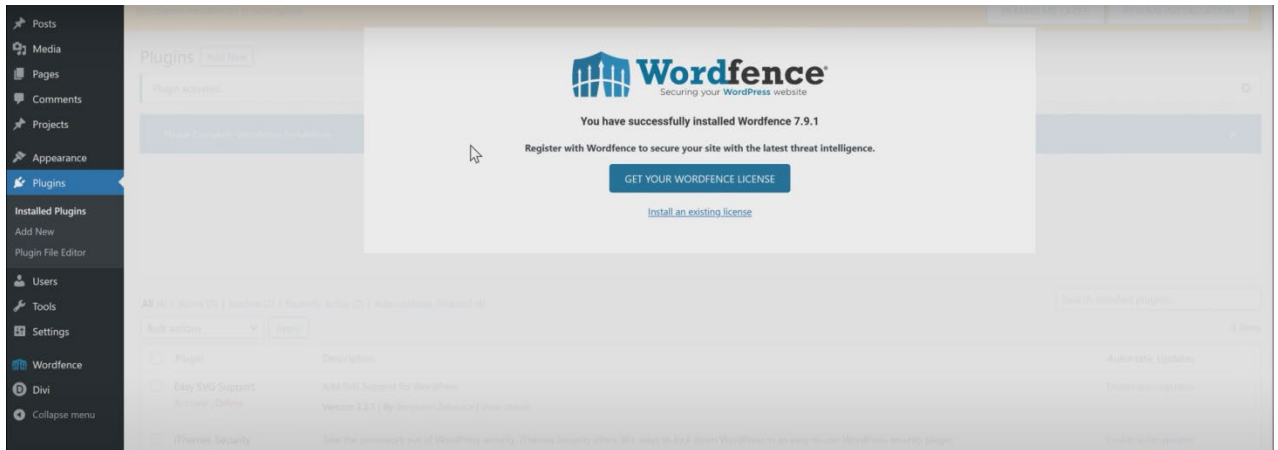


Рисунок 3.1 – Встановлення плагіну Wordfence

Налаштування брандмауера

Після успішного встановлення та активації плагіна Wordfence Security, відкривається його головне меню, де користувач може ознайомитися з основними функціональними можливостями. У цьому вікні відображаються такі ключові компоненти, як **брандмауер (Firewall)**, **сканер (Scan)**, а також налаштування повідомлень, інструменти діагностики та інтеграція з Wordfence Central.

Цей інтерфейс дозволяє розпочати базове налаштування захисту сайту, зокрема активувати режим навчання для брандмауера, запустити сканування системи, під'єднати сайт до централізованої панелі керування безпекою та переглядати сповіщення про потенційні загрози.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

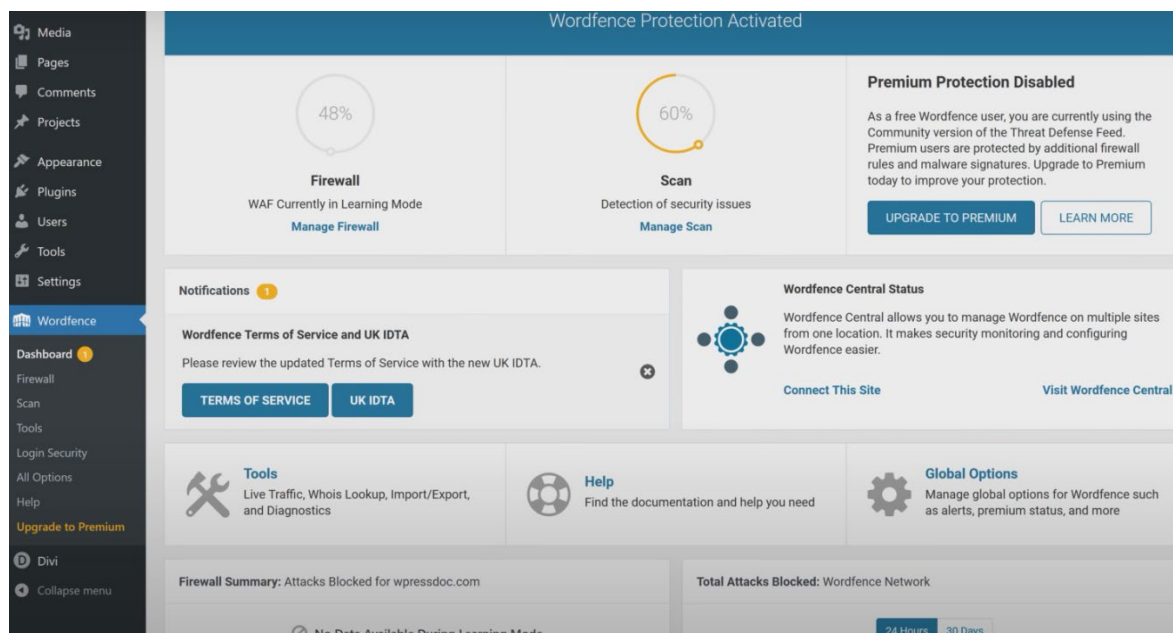


Рисунок 3.2 – Головна панель керування плагіном Wordfence після активації захисту.

Після встановлення плагіну Wordfence користувач переходить до розділу **Firewall**, де активується **вебфаєрвол** для захисту сайту. На скріншоті видно, що фаєрвол наразі працює в режимі **Learning Mode** – режим навчання, в якому плагін адаптується до поведінки сайту, вивчає нормальну активність користувачів і відвідувачів. Рекомендовано залишити цей режим активним протягом першого тижня, щоб уникнути хибних спрацювань.

- Web Application Firewall (35%) – фаєрвол вебзастосунків, активний у режимі навчання.
- Firewall Rules: Community (70%) – набір захисних правил із спільноти, оновлюється з затримкою (у преміум-версії оновлення відбуваються миттєво).
- Real-Time IP Blocklist: Disabled (0%) – функція блокування IP-адрес у реальному часі недоступна у безкоштовній версії.
- Brute Force Protection (100%) – захист від атак перебору паролів активовано.
- Rate Limiting – обмеження активності підозрілих ботів або сканерів, які перевищують ліміти запитів.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

- Blocking – можливість блокування трафіку за країною, IP, user-agent тощо.
- All Firewall Options – доступ до всіх налаштувань фаєрволу.

У нижній частині інтерфейсу розташовано блок із даними щодо заблокованих IP-адрес, однак під час режиму навчання статистика ще не доступна.

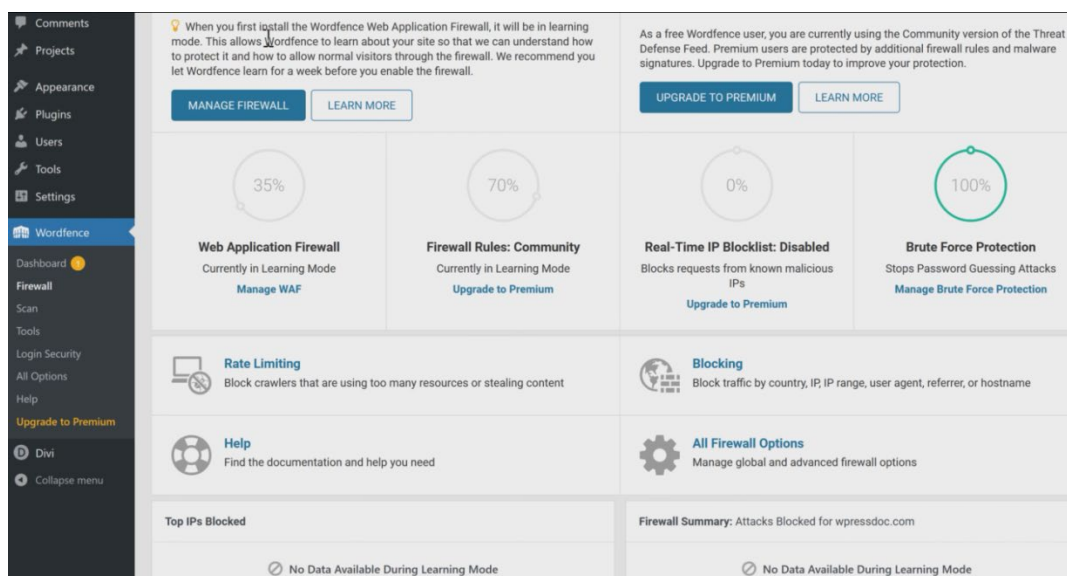


Рисунок 3.3 – Інтерфейс розділу Firewall після встановлення Wordfence

Далі слід перейти до розділу налаштування брандмауера. У відповідному пункті меню відкривається доступ до параметрів, де можна активувати Web Application Firewall, вибрати режим його роботи, задати правила фільтрації трафіку та увімкнути захист від атак типу Brute Force. У цьому ж розділі відображається статистика заблокованих загроз, а також надається доступ до розширених налаштувань для більш гнучкого керування системою безпеки.

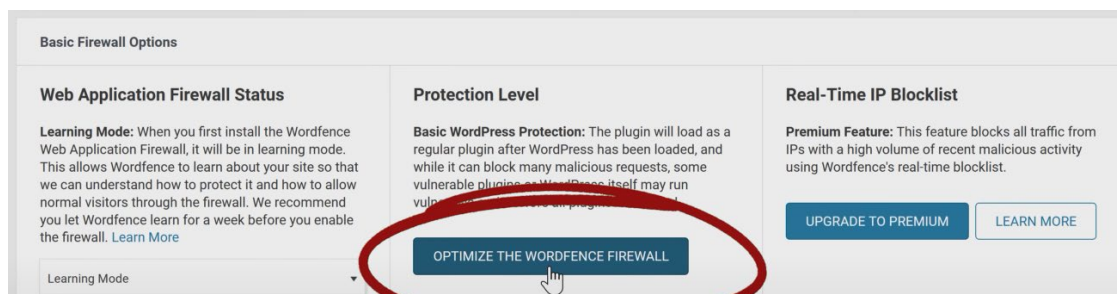


Рисунок 3.4 – Оптимізація брандмауера WordPress

Після натискання Wordfence запропонує оптимальний варіант файлу .htaccess для вебсайту. Вносити зміни до нього не потрібно – достатньо просто натиснути кнопку «Далі», щоб продовжити налаштування.

Optimize Wordfence Firewall If you cannot complete the setup process, [click here for help](#)

To make your site as secure as possible, the Wordfence Web Application Firewall is designed to run via a PHP setting called `auto_prepend_file`, which ensures it runs before any potentially vulnerable code runs.

NOTE: If you have separate WordPress installations with Wordfence installed within a subdirectory of this site, it is recommended that you perform the Firewall installation procedure on those sites before this one.

We've preselected your server configuration based on our tests, but if you know your web server's configuration, please select it now. You can also choose "Manual Configuration" for alternate installation details.

Apache + mod_php (recommended based on our tests)

Please download a backup of the following files before we make the necessary changes:

DOWNLOAD .HTACCESS

Once you have downloaded the files, click Continue to complete the setup. **CONTINUE**

Рисунок 3.5 – Завантаження .htaccess

На цьому етапі користувачеві пропонується завантажити резервну копію файлу .htaccess перед внесенням змін до конфігурації сервера. Для цього необхідно натиснути кнопку DOWNLOAD .HTACCESS, після чого файл автоматично збережеться на комп'ютері.

Цей крок використовується для створення резервної копії, яка дозволить відновити попередні налаштування у разі виникнення проблем.

Після завершення завантаження відбувається оптимізація брандмауера. У результаті Web Application Firewall починає завантажуватись раніше за ядро WordPress, що підвищує рівень безпеки сайту та дозволяє ефективніше блокувати загрози ще до їхнього впливу на систему.

Installation Successful

Nice work! The firewall is now optimized.

CLOSE

Рисунок 3.6 – Успішне завершення оптимізації

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Після завершення оптимізації з'явиться повідомлення Installation Successful. Це означає, що фаєрвол налаштовано та працює належним чином. Натисніть CLOSE, щоб завершити установку.

Після завершення оптимізації потрібно перейти до розділу налаштувань і встановити всі параметри безпеки Брандмауера.

Після завершення процесу оптимізації з'являється повідомлення "Installation Successful", що свідчить про успішне налаштування та активацію брандмауера. Для завершення встановлення користувач натискає кнопку CLOSE.

Після цього необхідно перейти до розділу налаштувань, де рекомендується встановити всі ключові параметри безпеки брандмауера, зокрема:

- Режим роботи фаєрвола
- Обмеження за кількістю запитів
- Блокування підозрілих IP-адрес
- Увімкнення розширеного логування

У розділі Advanced Firewall Options додається власна IP-адреса до списку "Allowedlisted IP addresses that bypass all rules". Це забезпечує безперешкодний доступ до сайту для адміністратора та запобігає випадковому блокуванню з боку системи безпеки.

Навіть у разі зміни IP-адреси це, як правило, не спричиняє серйозних проблем, оскільки зміни зазвичай незначні, і доступ зберігається.

Також у цьому розділі можна:

- дозволити обхід фаєрвола для сторонніх сервісів, таких як Uptime Robot чи ManageWP;
- визначити URL-адреси, спроби доступу до яких автоматично блокуватимуть IP-адресу;
- зазначити IP-адреси, для яких не відображатимуться сповіщення від Wordfence.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

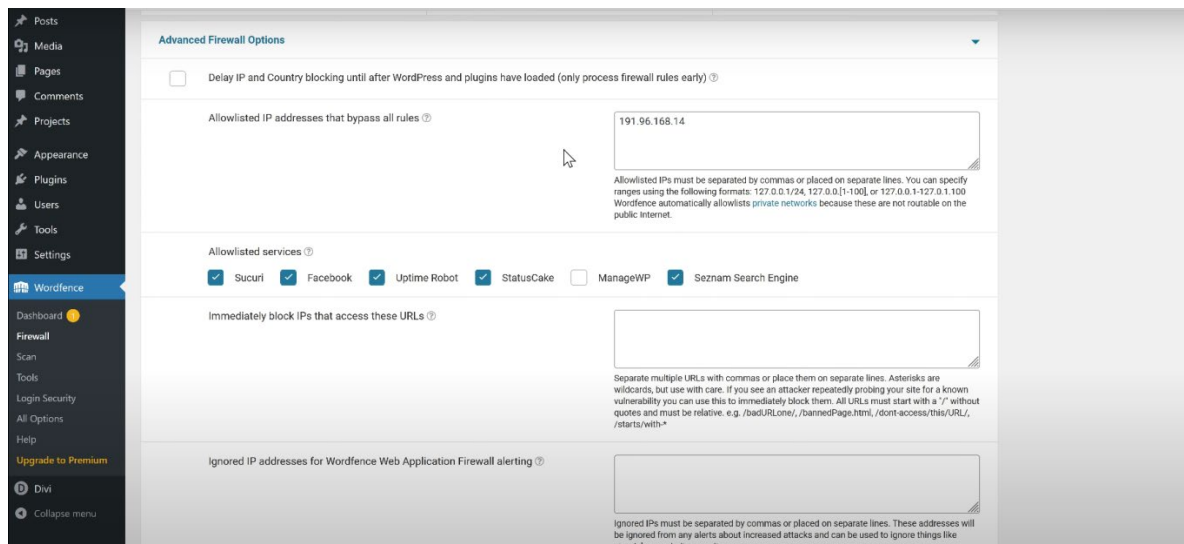


Рисунок 3.7 – Додавання власної IP-адреси до виключень

Секції Rules активуються правила захисту від найпоширеніших типів атак:

- SQL Injection (sqli) – захист від спроб втручання у базу даних.
- XSS: Cross Site Scripting (xss) – захист від впровадження шкідливого скрипту.
- Malicious File Upload – блокування спроб завантажити шкідливі файли.
- XXE: External Entity Expansion – захист від уразливості, пов'язаної з обробкою XML.
- Directory Traversal, LFI – захист від доступу до файлів за межами кореневого каталогу.

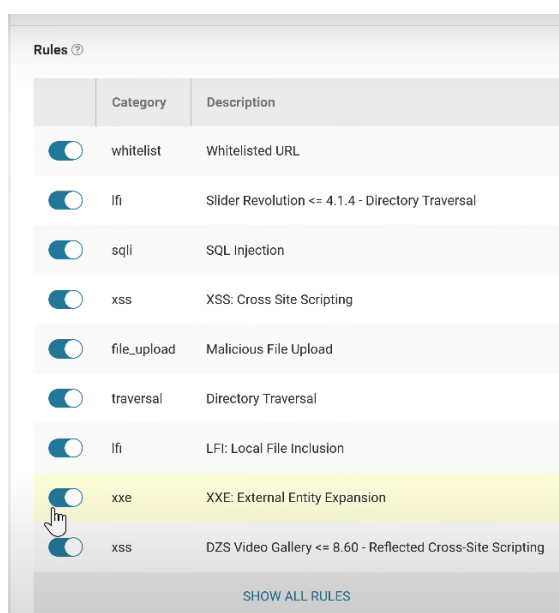


Рисунок 3.8 – Увімкнення захисту від загроз

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступним етапом є налаштування захисту від атак типу Brute Force – одного з ключових і найефективніших компонентів плагіна Wordfence. Ця функція активно протидіє автоматизованим спробам злому шляхом багаторазового підбору логіна і пароля. Вона дозволяє виявляти та блокувати підозрілу активність ще на ранньому етапі, запобігаючи доступу до адмін-панелі стороннім особам. Wordfence аналізує спроби входу, реагує на нетипову поведінку та автоматично застосовує захисні заходи, які суттєво знижують ризик успішного злому.

Налаштування Brute Force захисту є критично важливим, оскільки саме через слабо захищену авторизацію зловмисники найчастіше намагаються отримати контроль над сайтом. Завдяки цьому механізму Wordfence допомагає підтримувати високий рівень безпеки без необхідності постійного ручного втручання з боку адміністратора.

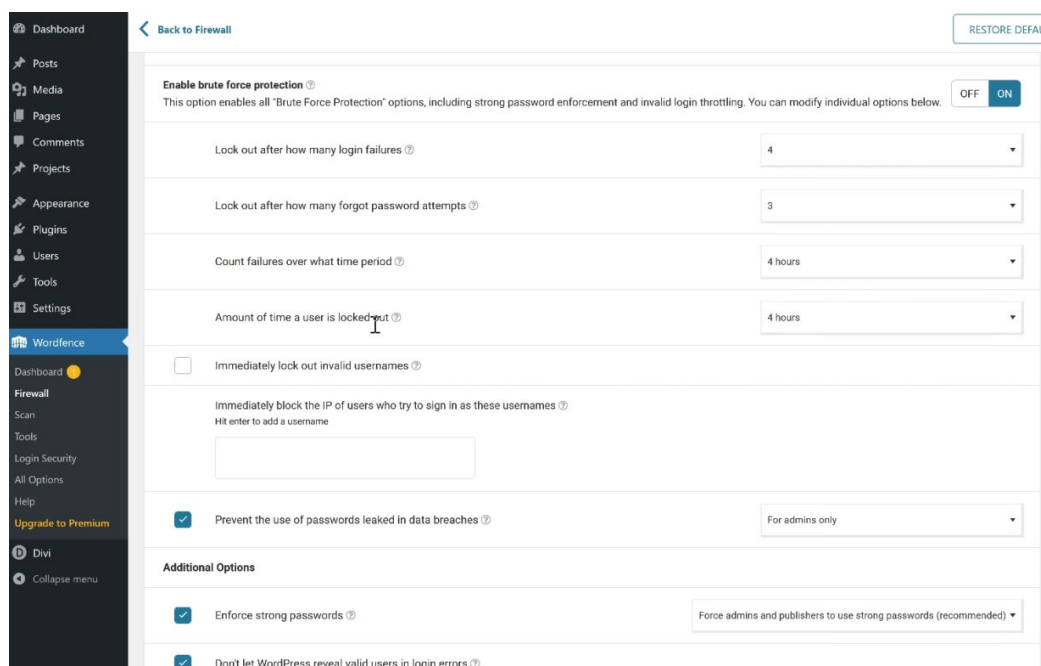


Рисунок 3.9 – Увімкнення захисту від загроз

У цьому розділі налаштовується захист від автоматичних спроб підбору паролів до сайту. Рекомендується активувати всі основні параметри безпеки, що забезпечують ефективне блокування підозрілої активності. Зокрема, вмикається функція захисту від Brute Force атак, після чого встановлюється обмеження – наприклад, блокування користувача після чотирьох невдалих спроб входу або

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

трьох невдалих спроб скидання паролю. Виявлені порушення обліковуються протягом чотирьох годин, а блокування триває такий самий період.

Також рекомендується активувати функцію, яка не дозволяє адміністраторам використовувати паролі, що раніше потрапляли в бази зламаних облікових даних. Обов'язкове використання складних паролів для адміністраторів і редакторів ще більше зміцнює захист системи.

Окремо активується параметр, який приховує точні причини помилок під час входу (наприклад, неправильне ім'я користувача чи пароль), що ускладнює зломисникам підбір справжніх облікових даних.

У разі необхідності також можна увімкнути додатковий захід – миттєве блокування IP-адрес, які намагаються авторизуватись із неіснуючими іменами користувачів. Ця функція особливо корисна, якщо ім'я адміністратора вже відоме і потребує підвищеного рівня захисту.

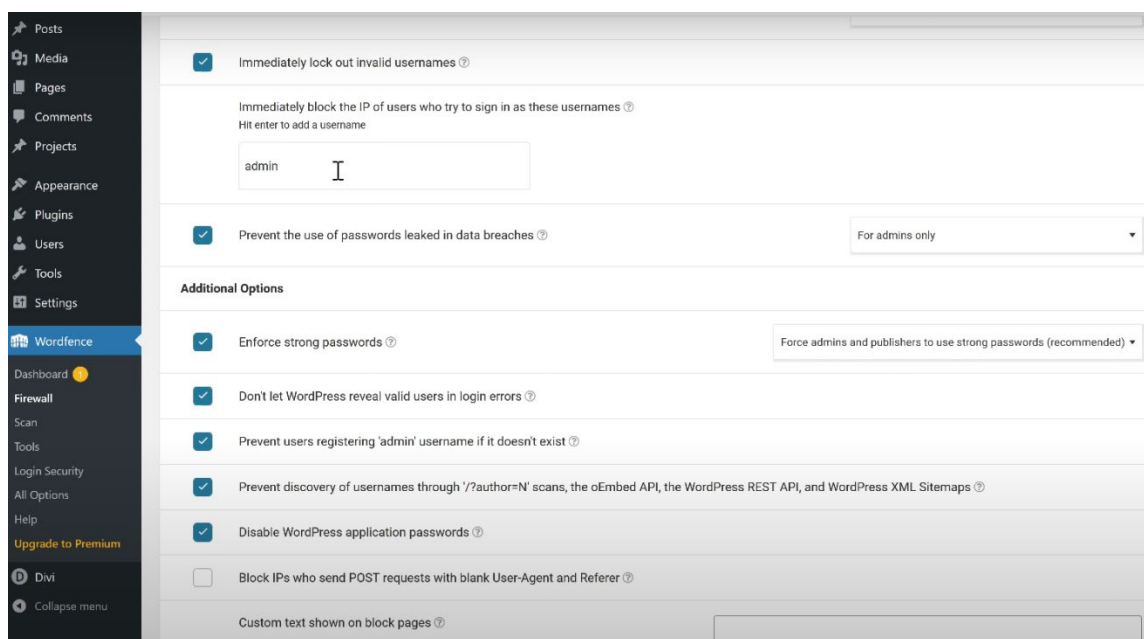


Рисунок 3.10 – Налаштування безпеки Wordfence у WordPress

На скріншоті вище показано процес створення нового користувача з правами адміністратора:

На наведеному нижче скріншоті продемонстровано процес створення нового облікового запису з правами адміністратора. Цей етап є важливим для надання доступу до панелі керування сайтом іншому користувачеві з повними

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

адміністративними повноваженнями. Під час створення облікового запису слід уважно заповнити всі обов'язкові поля: ім'я користувача, електронну пошту, пароль та вибрати роль "Administrator".

Рисунок 3.11 – Додавання нового адміністратора в WordPress

Рекомендується використовувати надійне ім'я користувача, яке складно вгадати, та унікальний складний пароль – це знижує ризик несанкціонованого доступу. Також варто переконатися, що новий адміністратор – довірена особа, оскільки такий обліковий запис має повний контроль над усім сайтом, включно з налаштуваннями безпеки, плагінами, темами та користувачами.

Рисунок 3.12 – Збереження налаштування.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

Після завершення налаштування брандмауера користувач переходить до конфігурації функції сканування на наявність шкідливого програмного забезпечення.

Цей етап є критично важливим для виявлення потенційних загроз, які могли проникнути на сайт – зокрема, вірусів, бекдорів, змінених файлів ядра WordPress, шкідливих скриптів або вразливостей у встановлених плагінах і темах.

Плагін Wordfence надає потужний інструмент сканування, який аналізує файли сайту, базу даних та плагіни на наявність підозрілих змін або шкідливого коду. Користувач має можливість налаштувати глибину перевірки, активувати регулярне автоматичне сканування, а також увімкнути надсилання звітів про результати перевірки на електронну пошту адміністратора.

Своєчасне налаштування цієї функції значно підвищує рівень безпеки ресурсу, дозволяючи виявити загрози до того, як вони завдадуть шкоди сайту або користувачам.

У розділі Scan користувач може запустити процес перевірки сайту на предмет потенційних загроз, змінених або підозрілих файлів, вбудованого шкідливого коду, фішингового вмісту та інших ознак компрометації.

Цей інструмент є одним із ключових компонентів плагіна Wordfence Security і виконує важливу роль у підтримці безпеки вебресурсу. Завдяки глибокому аналізу структури сайту, сканер дозволяє своєчасно виявити вразливості, відхилення від оригінальних файлів WordPress, небажані скрипти або ознаки зовнішнього втручання, що дає змогу оперативно вжити заходів для усунення загроз та захисту сайту від можливих атак.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

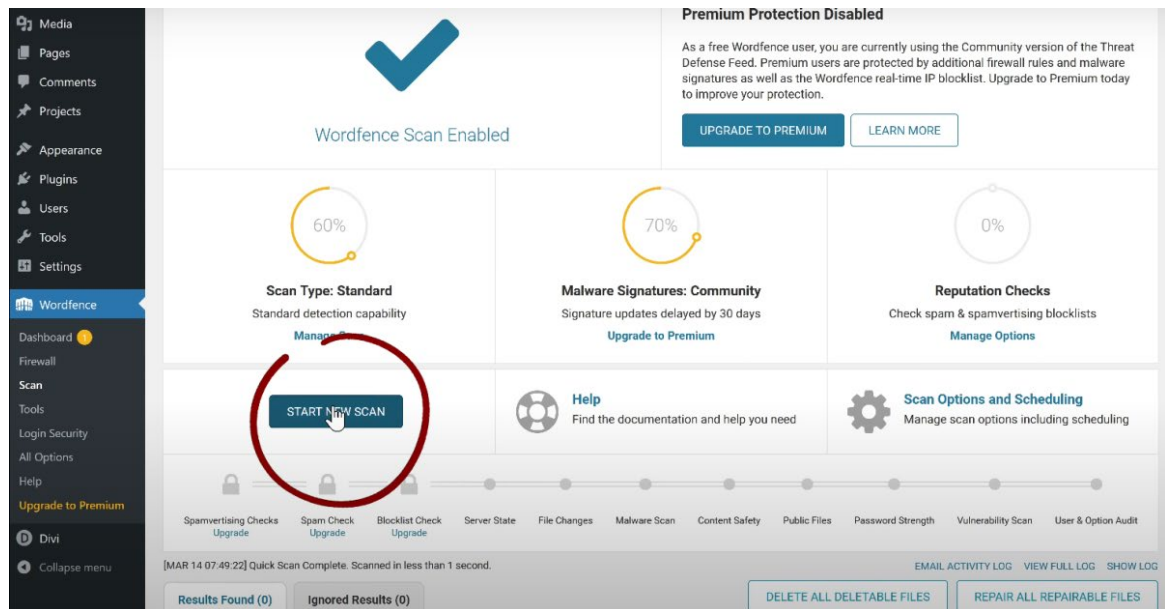


Рисунок 3.13 – Інтерфейс розділу **Scan** у Wordfence

Інтерфейс показує, що функція сканування вже активована (Wordfence Scan Enabled). Головним елементом є кнопка **START NEW SCAN**, за допомогою якої ініціюється процес повної перевірки сайту.

У нижній частині екрана відображається індикатор прогресу сканування, що охоплює різні етапи, зокрема перевірку на спам, фішингові загрози, зміни у файлах, безпеку контенту, аналіз публічних файлів, перевірку паролів та виявлення потенційних вразливостей.

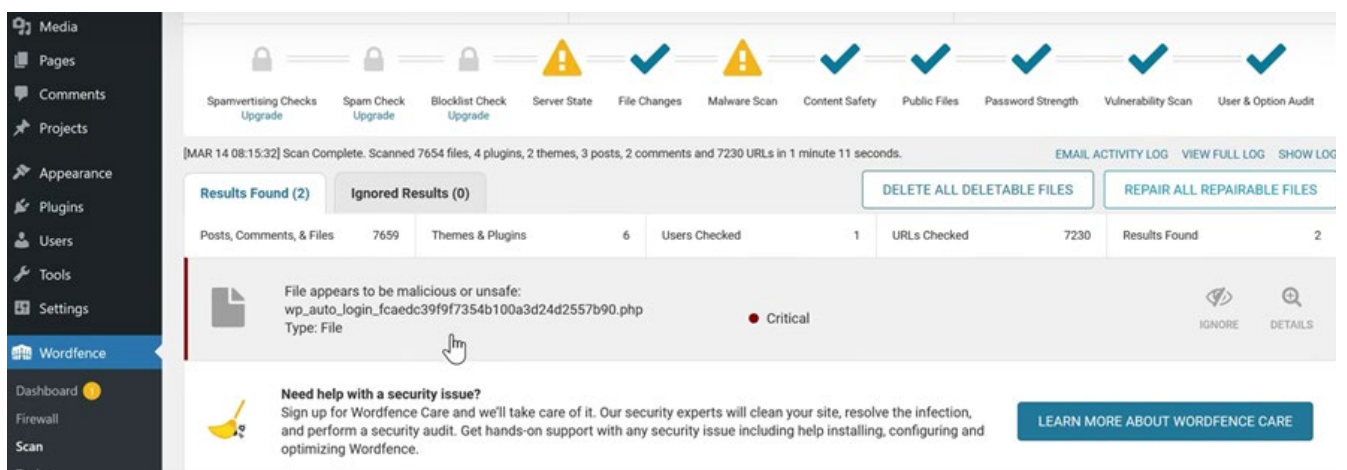


Рисунок 3.14 – Сканування сайту плагіном Wordfence Security у розділі Scan після натискання кнопки Start New Scan.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

У верхній частині інтерфейсу відображаються етапи сканування, серед яких перевірки на розсилку спаму (Spamvertising Checks, Spam Check, Blocklist Check), аналіз стану сервера, змін у файлах та виявлення шкідливого програмного забезпечення (Server State, File Changes, Malware Scan), а також оцінка безпеки контенту, публічних файлів і надійності паролів (Content Safety, Public Files, Password Strength) та інші важливі аспекти безпеки. Після завершення сканування користувач переходить до розділу Tools для перегляду активності сайту в реальному часі.

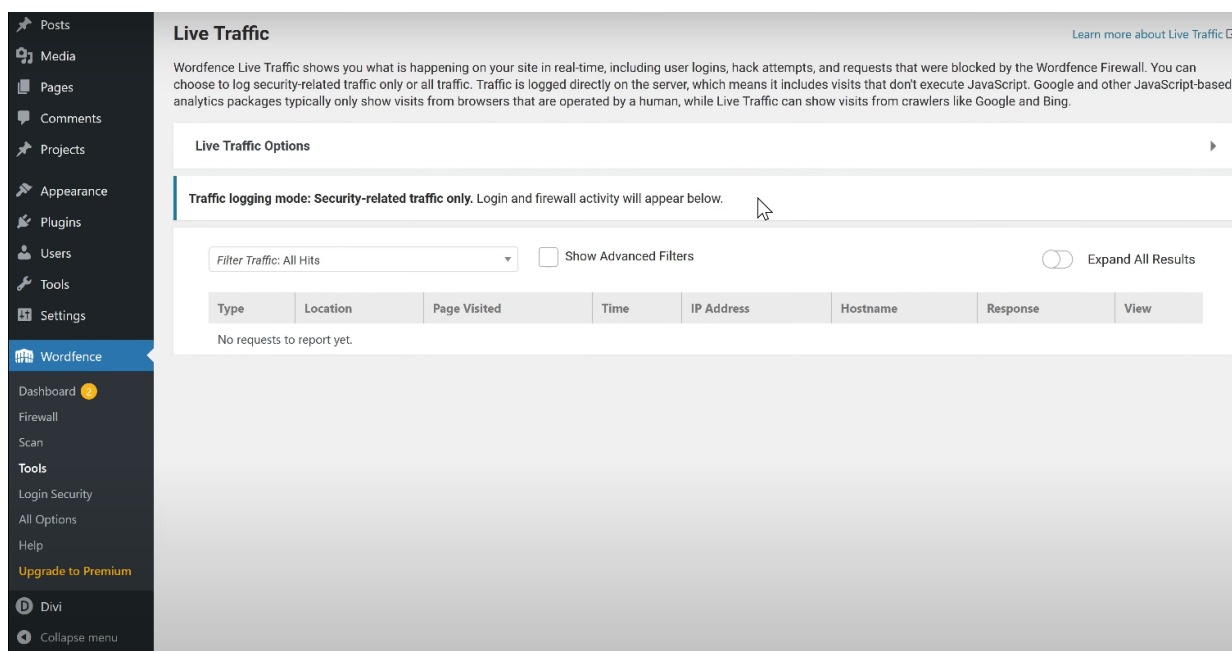


Рисунок 3.15 – Перегляд активності в реальному часі

У вкладці Live Traffic плагін Wordfence демонструє всі події, пов’язані із безпекою сайту, в режимі реального часу. Сюди входять інформація про входи користувачів, спроби злому або невдалі спроби авторизації, а також дії, які були заблоковані брандмауером. Крім того, відображаються дані про джерела трафіку, включно з IP-адресами, географічним розташуванням, часом подій та сторінками, які відвідували користувачі.

Наступним кроком користувач переходить до розділу Whois Lookup, що розташований у меню Wordfence > Tools.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

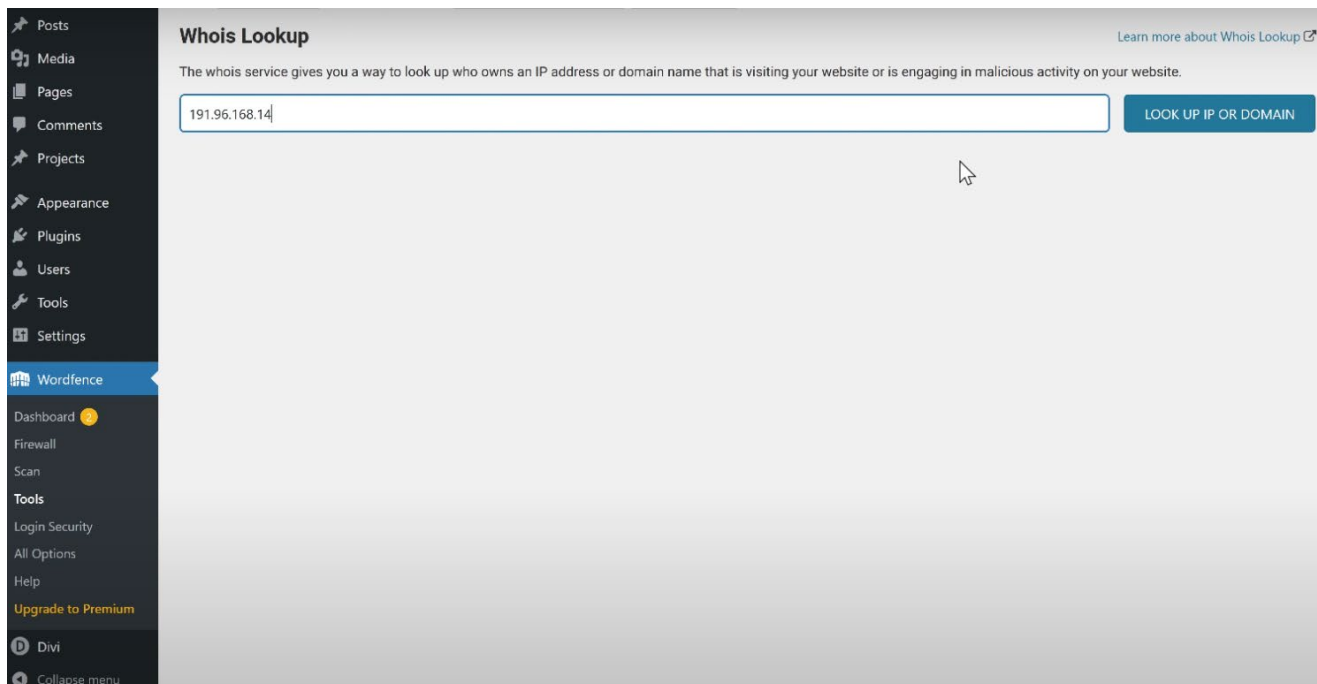


Рисунок 3.16 – Інтерфейс WordPress з відкритим розділом Wordfence > Tools > Whois Lookup.

Введення IP-адреси у форму WHOIS Lookup виконується для отримання інформації про власника цієї адреси. Це особливо корисно у випадках, коли на сайт заходять із підозрілих IP, виявлена спроба злому або зафіксована інша шкідлива активність у логах безпеки, зокрема в системі Wordfence.

Адміністратор може таким чином з'ясувати, хто стоїть за IP-адресою – це може бути хостингова компанія, VPN-сервіс, країна або конкретна організація. WHOIS Lookup надає такі дані, як назва організації, країна чи регіон, контактна інформація адміністратора IP-діапазону, провайдер або хостинг, а також інші технічні характеристики.

Отримана інформація допомагає приймати обґрунтовані рішення щодо подальших дій, зокрема блокування потенційно небезпечних IP-адрес.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

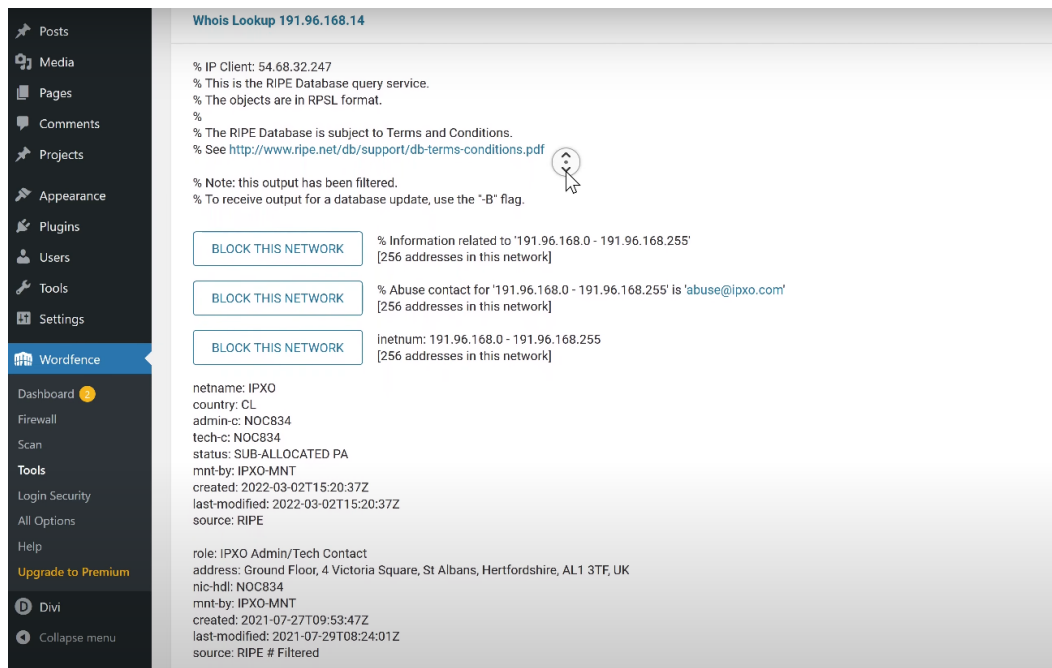


Рисунок 3.17 – Налаштування безпеки WordPress: WHOIS-запит для IP-адреси, що може бути пов'язана з VPN

Wordfence показує цю інформацію, щоб адміністратор сайту міг прийняти обґрунтоване рішення: чи блокувати трафік з цього діапазону IP-адрес, якщо він вважає його підозрілим (наприклад, через спроби злому, спам-коментарі тощо), чи дозволити його. Блокування IP-адрес, які належать VPN-сервісам, є поширеною практикою для сайтів, які намагаються запобігти обходу геообмежень, шкідливим діям або просто хочуть ідентифікувати реальне джерело трафіку.

Налаштування двофакторної автентифікації

Двофакторна автентифікація (2FA) є важливим компонентом безпеки, який значно підвищує рівень захисту облікових записів на сайті. У Wordfence дана функція доступна через розділ **Login Security** та дозволяє додати другий етап перевірки при вході – крім пароля, користувач має ввести одноразовий код із мобільного застосунку, такого як Google Authenticator або Authy.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

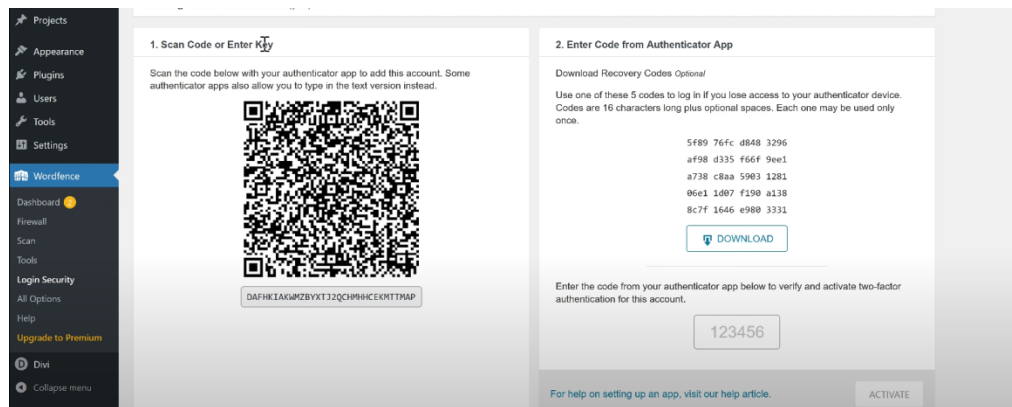


Рисунок 3.18 – Налаштування двофакторної автентифікації для плагіна Wordfence

На скріншоті відображається сторінка налаштувань двофакторної автентифікації в плагіні Wordfence для WordPress. Інтерфейс розділений на дві основні частини. У верхній секції користувачеві пропонується відсканувати QR-код або вручну ввести секретний ключ у додатку для автентифікації (наприклад, Google Authenticator чи Authy). Це дозволяє підключити захист 2FA до облікового запису.

У нижній частині сторінки передбачене поле для введення одноразового коду, згенерованого мобільним застосунком, що необхідно для підтвердження активації. Поряд із цим розташована опція генерації резервних кодів – на випадок втрати доступу до пристрою з автентифікатором.

Зліва видно стандартне меню адміністративної панелі WordPress, де виділений розділ Wordfence з активною вкладкою Login Security, що дозволяє орієнтуватися в налаштуваннях безпеки.

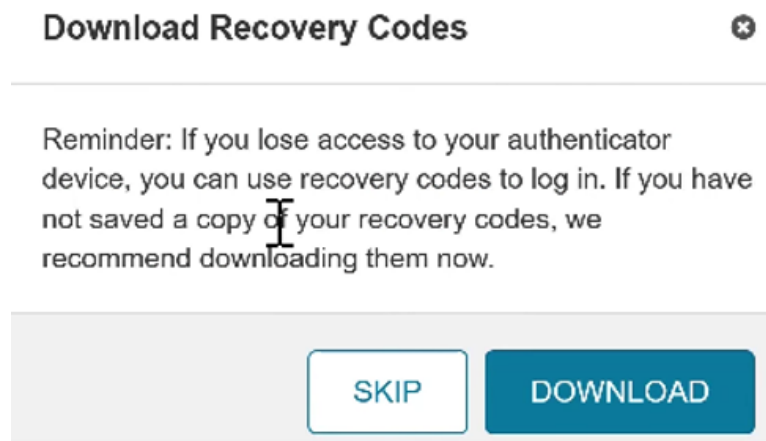


Рисунок 3.19 – Download Recovery Codes

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Користувач має можливість деактивувати захист або згенерувати нові резервні коди для відновлення доступу. Поверх основного вмісту відкрито модальне вікно, яке нагадує про необхідність завантажити резервні коди на випадок втрати доступу до пристрою з автентифікатором. У вікні пропонуються два варіанти: пропустити цей крок або завантажити коди. Ліворуч відображено стандартне навігаційне меню WordPress, де активним залишається розділ Wordfence.

Login Security Settings

Learn more about Login Security

CANCEL SAVE

User Summary Manage Users

Role	Total Users	2FA Active	2FA Inactive
Administrator	1	0	1
Total	1	0	1

2FA

2FA Roles

Administrator Editor Author Contributor Subscriber

Optional Disabled Disabled Disabled Disabled

Grace Period

10 days

For roles that require 2FA, users will have this many days to set up 2FA. Failure to set up 2FA during this period will result in the user losing account access. This grace period will apply to new users from the time of account creation. For existing users, this grace period will apply relative to the time at which the requirement is implemented. This grace period will not automatically apply to admins and must be manually enabled for each admin user.

☐ **Allow remembering device for 30 days**

If enabled, users with 2FA enabled may choose to be prompted for a code only once every 30 days per device.

Require 2FA for XML-RPC call authentication

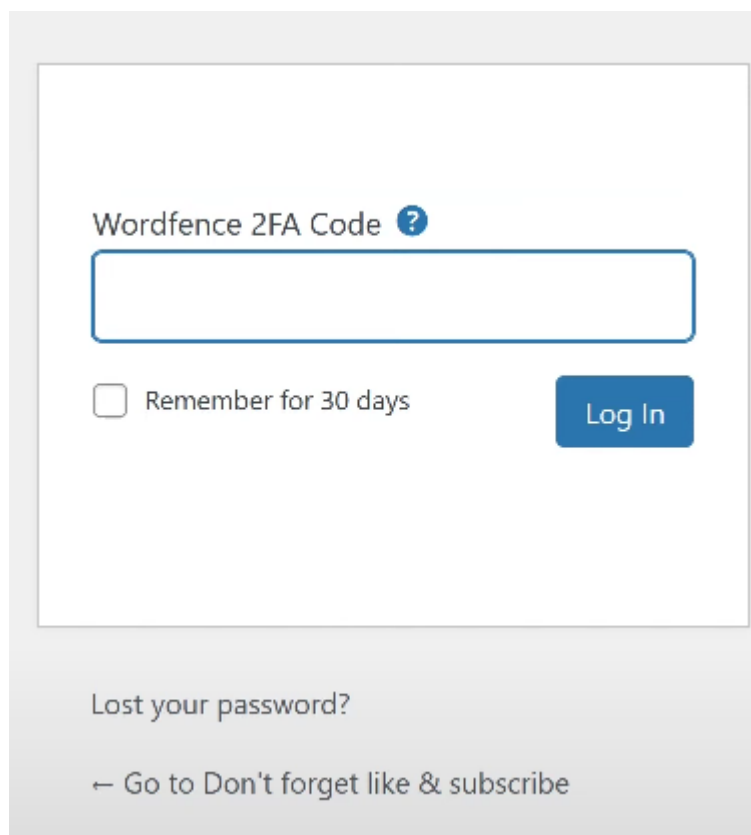
If enabled, XML-RPC calls that require authentication will also require a valid 2FA code to be appended to the password. You must choose the "Skipped" option if you use the WordPress app, the Jetpack plugin, or other services that require XML-RPC.

SKIPPED REQUIRED

Рисунок 3.20 – Сторінка "Login Security Settings"

Тут відображено статус 2FA для всіх ролей: для адміністратора вона необов'язкова, для інших – вимкнена. Налаштовується пільговий період у 10 днів для нових користувачів, опція запам'ятовування пристрою на 30 днів і захист XML-RPC запитів.

Другий рівень автентифікації для доступу до адміністративної частини сайту WordPress. Після введення логіну та пароля, система запитує одноразовий код підтвердження, згенерований у додатку двофакторної автентифікації (2FA). Це забезпечує підвищений рівень безпеки сайту, зменшуючи ризик несанкціонованого доступу навіть у разі компрометації основного пароля.



Wordfence 2FA Code ?

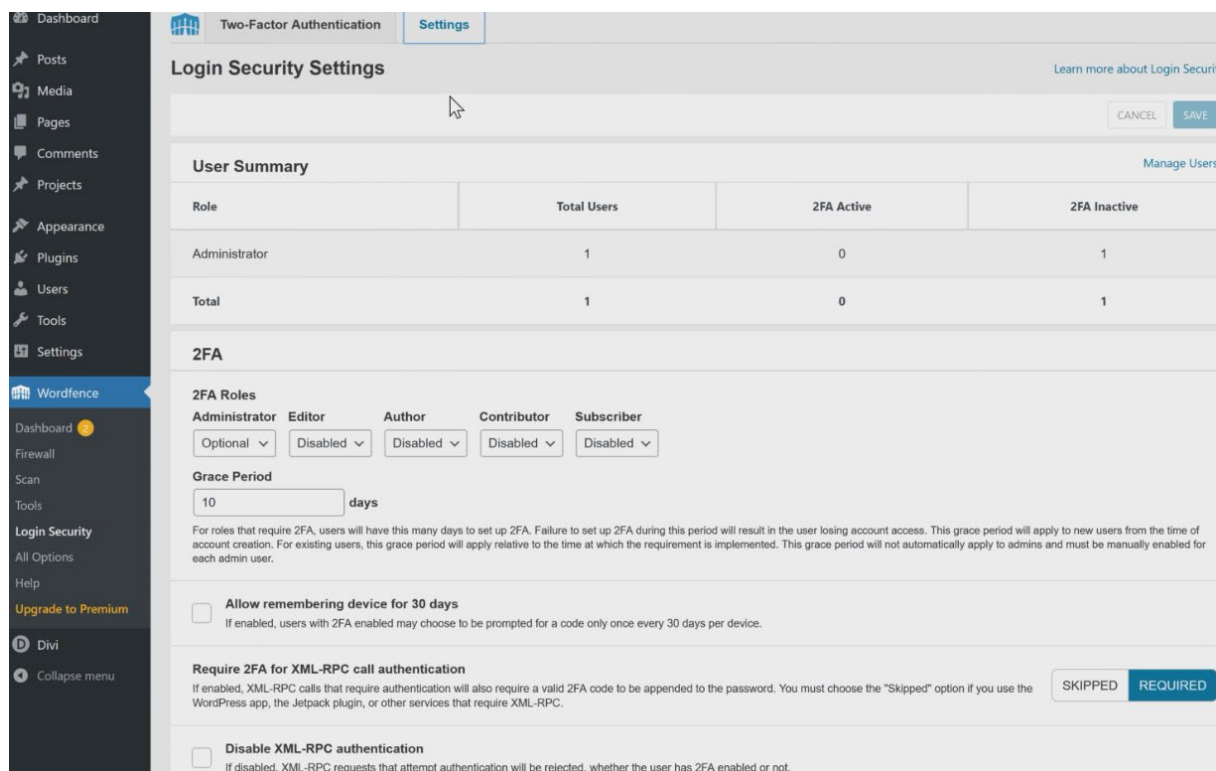
☐ Remember for 30 days Log In

Lost your password?

← Go to Don't forget like & subscribe

Рисунок 3.21 – Інтерфейс двофакторної автентифікації (2FA)

Також присутня опція «Remember for 30 days» (Запам'ятати на 30 днів), яка дозволяє уникати повторного введення коду з цього пристрою протягом місяця.



Two-Factor Authentication Settings

Learn more about Login Security

CANCEL SAVE

User Summary Manage Users

Role	Total Users	2FA Active	2FA Inactive
Administrator	1	0	1
Total	1	0	1

2FA

2FA Roles

Administrator Editor Author Contributor Subscriber

Optional Disabled Disabled Disabled Disabled

Grace Period

10 days

For roles that require 2FA, users will have this many days to set up 2FA. Failure to set up 2FA during this period will result in the user losing account access. This grace period will apply to new users from the time of account creation. For existing users, this grace period will apply relative to the time at which the requirement is implemented. This grace period will not automatically apply to admins and must be manually enabled for each admin user.

☐ Allow remembering device for 30 days

If enabled, users with 2FA enabled may choose to be prompted for a code only once every 30 days per device.

Require 2FA for XML-RPC call authentication

If enabled, XML-RPC calls that require authentication will also require a valid 2FA code to be appended to the password. You must choose the "Skipped" option if you use the WordPress app, the Jetpack plugin, or other services that require XML-RPC.

SKIPPED REQUIRED

☐ Disable XML-RPC authentication

If disabled, XML-RPC requests that attempt authentication will be rejected, whether the user has 2FA enabled or not.

Рисунок 3.22 – Налаштування двофакторної автентифікації (2FA)

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

На цьому етапі було виконано налаштування політик двофакторної автентифікації (2FA) для різних ролей користувачів у WordPress через плагін Wordfence. Для ролі адміністратора увімкнено опціональну 2FA, а для решти ролей вона вимкнена. Також встановлено пільговий період активації 2FA – 10 днів. Це дозволяє користувачам поступово перейти до безпечнішого входу без втрати доступу. Додатково ввімкнено можливість збереження пристрою на 30 днів та визначено політику автентифікації для XML-RPC-запитів.

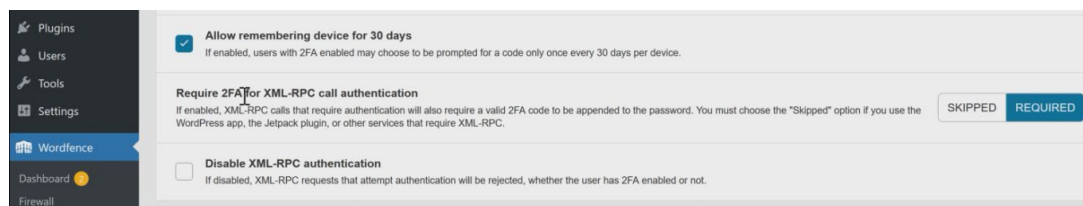


Рисунок 3.23 – Додаткові налаштування безпеки

Налаштування reCAPTCHA

Далі було здійснено перехід до розділу reCAPTCHA у плагіні Wordfence, що призначений для налаштування функцій захисту форм входу та реєстрації користувачів. У цьому розділі адміністратор має змогу активувати Google reCAPTCHA v3, яка дозволяє ідентифікувати автоматизовані запити (ботів) без необхідності виконання користувачем додаткових дій.

На відміну від попередніх версій, reCAPTCHA v3 не вимагає розв'язання головоломок або натискання чекбоксів. Замість цього вона аналізує поведінку користувача в реальному часі та автоматично присвоює йому оцінку (score) в діапазоні від 0.0 до 1.0.

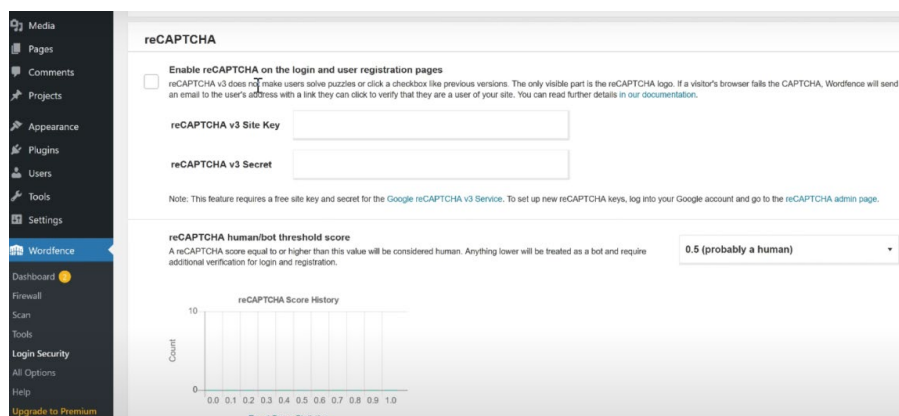


Рисунок 3.24 – Налаштувань reCAPTCHA v3 у плагіні Wordfence

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Було здійснено налаштування reCAPTCHA у межах плагіна Wordfence, що використовується у системі керування контентом WordPress. У процесі налаштування адміністратором активується функція захисту на сторінках входу та реєстрації, після чого у відповідні поля вводяться унікальні site key та secret key, отримані з облікового запису Google reCAPTCHA. Також задається порогове значення оцінки (threshold), яке визначає мінімальний допустимий рейтинг, при якому користувач вважається легітимним. У випадку, якщо рейтинг користувача є нижчим за встановлений поріг (наприклад, 0.5), такий запит класифікується як потенційно небезпечний, і вхід може бути заборонено або запитано додаткову перевірку. Крім цього, на сторінці налаштувань виводиться статистика розподілу оцінок reCAPTCHA, що дозволяє відстежувати частоту підозрілих дій.

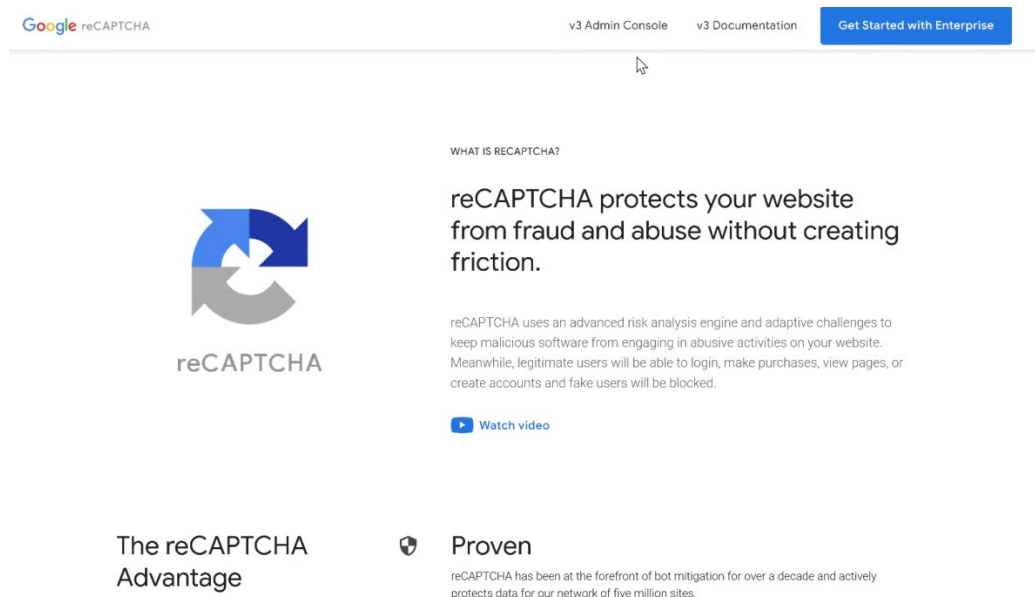


Рисунок 3.25 – Налаштування Google reCAPTCHA v3 у Wordfence (WordPress)

Було виконано реєстрацію сайту в адміністративній панелі Google reCAPTCHA. У відповідній формі зазначено назву ресурсу (Label), обрано версію захисту – reCAPTCHA v3, після чого додано доменне ім'я сайту та контактну електронну адресу власника. Також було прийнято умови надання послуг. Після завершення цього процесу система згенерувала унікальні ключі, необхідні для подальшої інтеграції сервісу із сайтом.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Рисунок 3.26 – Створення облікового запису сайту в Google reCAPTCHA admin panel

На цьому етапі вказується назва проєкту, обирається тип захисту (у прикладі – reCAPTCHA v3), додається домен сайту, а також електронна адреса власника. Після прийняття умов використання і підтвердження через кнопку **Submit** система генерує ключі (site key та secret key), які надалі інтегруються в сайт для забезпечення захисту від ботів та автоматизованих дій.

Після створення облікового запису сайту в Google reCAPTCHA адміністративна панель дозволяє вибрати тип reCAPTCHA (v2 або v3), додати домен, вказати власників, а також прийняти умови використання сервісу. У прикладі обрано reCAPTCHA v3, яка дозволяє перевіряти дії користувачів без введення коду вручну. Після заповнення всіх полів і натискання кнопки **Submit**, сайт успішно реєструється у Google reCAPTCHA

Рисунок 3.27 – Поле для ключа reCAPTCHA

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

Після успішної реєстрації сайту у Google reCAPTCHA система надає два ключі – **Site Key** та **Secret Key**, які необхідні для інтеграції reCAPTCHA з вебсайтом. Ці ключі копіюються у відповідні поля в плагіні Wordfence у WordPress. Увімкнення функції “Enable reCAPTCHA on the login and user registration pages” активує перевірку reCAPTCHA v3 на формах входу та реєстрації, що дозволяє ефективно захищати сайт від ботів та автоматизованих атак

☒ **Enable reCAPTCHA on the login and user registration pages**
 reCAPTCHA v3 does not make users solve puzzles or click a checkbox like previous versions. The only visible part is the reCAPTCHA logo. If a visitor's browser fails the CAPTCHA, Wordfence will send an email to the user's address with a link they can click to verify that they are a user of your site. You can read further details [in our documentation](#).

reCAPTCHA v3 Site Key: 6LeoG_0kAAAAAJOR8ojhDFHWbHkbwEU2fkH-YK29

reCAPTCHA v3 Secret: 6LeoG_0kAAAAAIDXWeyMnpxs3FSQGf6r1vnzfQtH

Note: This feature requires a free site key and secret for the [Google reCAPTCHA v3 Service](#). To set up new reCAPTCHA keys, log into your Google account and go to the [reCAPTCHA admin page](#).

Рисунок 3.28 – Ведення ключів

Перегляд та налаштування параметр

Глобальні налаштування, які дозволяють досвідченим користувачам швидко отримати доступ до основних параметрів безпеки. У секції **View Customization** користувач може активувати або вимкнути відображення окремих пунктів меню Wordfence, таких як “All Options”, “Blocking” та “Live Traffic”. Це дає змогу спростити інтерфейс адміністративної панелі, залишивши лише необхідні функції для щоденної роботи.

Рисунок 3.29 – All Options

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

Було увімкнено опцію **"Update Wordfence automatically when a new version is released"** – автоматичне оновлення плагіну при виході нової версії. Це важливо для забезпечення актуальності захисних механізмів, оскільки нові версії Wordfence містять оновлені сигнатури загроз та покращення захисту. Нижче вказується електронна адреса, на яку надходитимуть повідомлення про безпекові події. Також обирається метод визначення IP-адрес користувачів – **"Let Wordfence use the most secure method to get visitor IP addresses"**, що є рекомендованим і забезпечує точне виявлення джерел запитів, особливо у випадку використання проксі або хмарних сервісів.

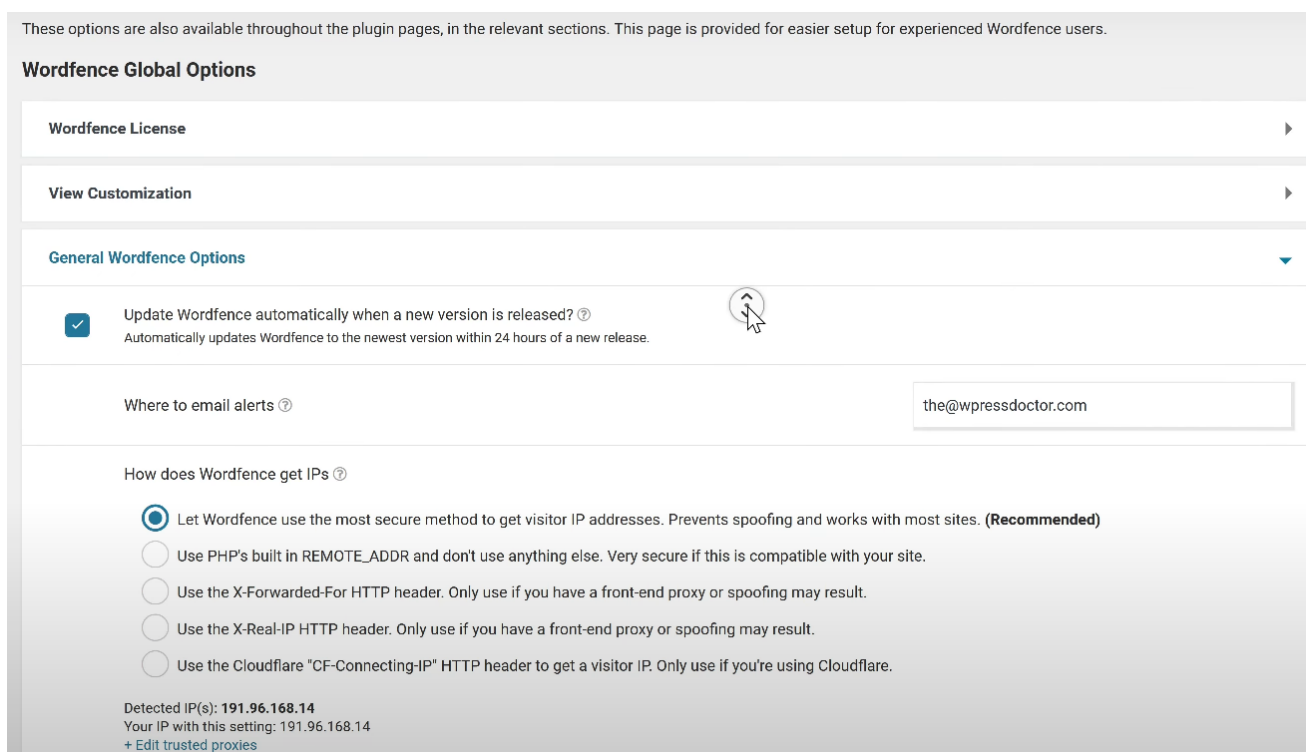


Рисунок 3.30 – All Options" (Всі опції) плагіна Wordfence

Додаткові налаштування безпеки. Перше з них – це опція **"Hide WordPress version"**, яка приховує версію CMS WordPress від сторонніх користувачів. Проте, згідно з рекомендаціями розробників Wordfence, ця опція **не увімкнена**, оскільки існують інші методи визначення версії (наприклад, через статичні файли CSS або JS), і вона не забезпечує ефективного захисту. Далі представлена важлива функція **"Disable Code Execution for Uploads directory"**, яка блокує виконання PHP-коду в папці `wp-content/uploads`. Це реалізується шляхом автоматичного створення

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

.htaccess-файлу з відповідними директивами. Такий підхід захищає від можливості запуску шкідливих скриптів, які можуть бути завантажені в цю директорію.

Hide WordPress version

WordPress, by default, discloses what its version is. This option will hide it from outsiders. [We generally recommend that you do not enable this anymore](#), since there are other methods of determining the WordPress version such as fingerprinting of static content such as CSS and javascript files. This option will be disabled on new installations.

Disable Code Execution for Uploads directory

Enabling this option will place a ".htaccess" file in your "wp-content/uploads/" directory which prevents any PHP code in your uploads directory from executing. This is an added level of protection against a hacker managing to upload PHP code into your "uploads" directory. Even if they manage to do that, the code won't execute if you have this option enabled. The contents of the .htaccess file are below:

```
# BEGIN Wordfence code execution protection
<IfModule mod_php5.c>
php_flag engine 0
</IfModule>
<IfModule mod_php7.c>
php_flag engine 0
</IfModule>
<IfModule mod_php.c>
php_flag engine 0
</IfModule>
AddHandler cgi-script .php .phtml .php3 .pl .py .jsp .asp .htm .shtml .sh .cgi
Options -ExecCGI
# END Wordfence code execution protection
```

Рисунок 3.31 – Налаштуваннями безпеки WordPress

Далі було обрано параметри відображення сповіщень у адмінпанелі. Увімкнено два типи сповіщень: **"Updates Needed"** (оновлення плагінів, тем або ядра) та **"Scan Results"** (результати перевірки безпеки). Ці повідомлення дозволяють адміністраторам швидко реагувати на вразливості або проблеми, виявлені на сайті. Додаткові типи сповіщень, як-от рекламні або комерційні, доступні лише у платній версії плагіну, але для базового захисту достатньо й безкоштовного функціоналу.

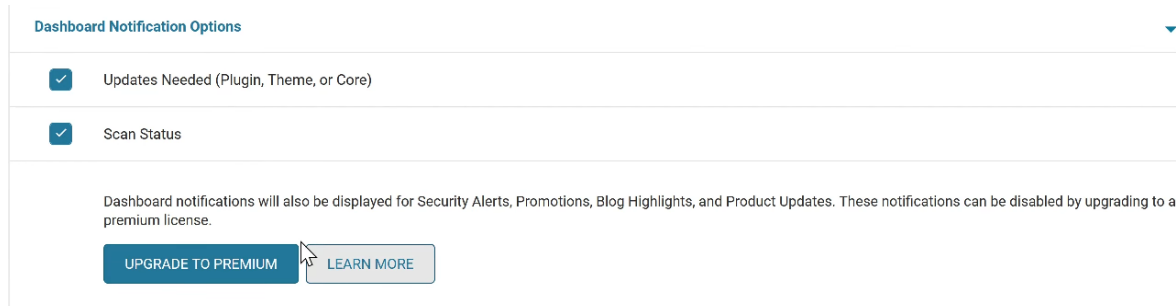


Рисунок 3.32 – Dashboard Notification Options

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

Активовано опції надсилання повідомлень на електронну пошту у випадку вимкнення плагіна або його фаєрволу. Також увімкнено сповіщення про результати сканування з будь-яким рівнем загрози, вхід адміністратора (лише з нового пристрою) та використання форми відновлення пароля. Це дозволяє адміністратору оперативно реагувати на підозрілі дії в системі безпеки сайту.

Рисунок 3.33 – Налаштування сповіщень системи безпеки Wordfence

Далі увімкнено перевірку на наявність публічно доступних конфігураційних, резервних і карантинних файлів, сканування ядра WordPress, тем і плагінів на відповідність офіційним версіям, а також пошук шкідливого коду, троянів, бекдорів, небезпечних URL-адрес та підозрілих коментарів. Ці налаштування забезпечують комплексну перевірку системи на вразливості та шкідливі елементи.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

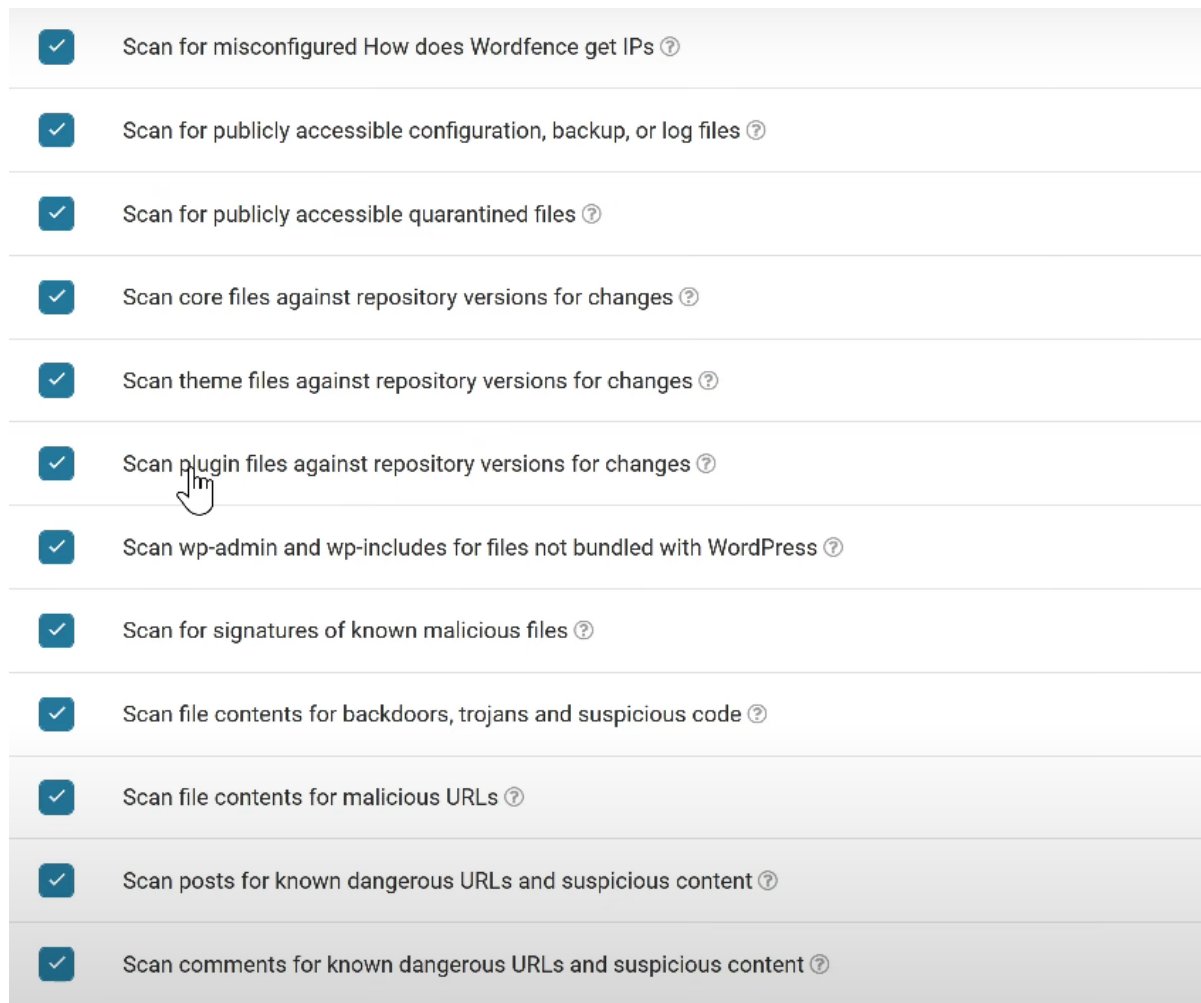


Рисунок 3.34 – Конфігурація параметрів сканування у Wordfence

На рисунку представлено налаштування продуктивності сканування у плагіні Wordfence (розділ *Performance Options*), яке дозволяє оптимізувати процес перевірки сайту на вразливості з урахуванням ресурсів сервера. У параметрах встановлено обмеження на кількість виявлених проблем, що надсилаються електронною поштою, до 1000, а також виділено 256 МБ оперативної пам'яті для виконання сканування. Час виконання одного етапу сканування залишено за замовчуванням (0 секунд), що дозволяє системі самостійно визначати оптимальний ліміт. Ліміт загального часу сканування не вказано, тому буде використане стандартне значення (до 3 годин). Опція економії ресурсів сервера (*Use low resource scanning*), яка знижує навантаження, але збільшує тривалість сканування, залишена неактивною, що свідчить про пріоритетність повної та швидкої перевірки безпеки сайту.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Performance Options

☒ Use low resource scanning (reduces server load by lengthening the scan duration) ⓘ

Limit the number of issues sent in the scan results email ⓘ
0 or empty means unlimited issues will be sent

Time limit that a scan can run in seconds ⓘ
0 or empty means the default of 3 hours will be used

How much memory should Wordfence request when scanning ⓘ
Memory size in megabytes

Maximum execution time for each scan stage ⓘ
0 for default. Must be 8 or greater and 10-20 or higher is recommended for most servers

Advanced Scan Options

Рисунок 3.35 – Налаштування параметрів продуктивності сканування у Wordfence

У процесі налаштування плагіна Wordfence Security було забезпечено комплексний підхід до захисту вебсайту на базі WordPress. Активовано ключові функції безпеки, зокрема: фаєрвол, сповіщення про підозрілі дії (вхід адміністратора, використання форми відновлення пароля), а також глибоке сканування файлів ядра, плагінів, тем, конфігураційних файлів та вмісту на наявність шкідливого коду, URL-адрес і коментарів.

Налаштовані параметри продуктивності дозволяють досягти балансу між швидкістю перевірки та стабільністю роботи сервера, що особливо важливо для сайтів із обмеженими ресурсами. Застосовані опції гарантують вчасне виявлення загроз і дозволяють адміністратору оперативно реагувати на спроби злому, що значно підвищує загальний рівень кібербезпеки сайту.

Отже, плагін Wordfence є ефективним інструментом для забезпечення надійного та гнучкого захисту вебресурсі.

3.2 Тестування WordFence

Процес тестування проводиться з метою перевірки ефективності основних функцій безпеки, таких як антивірусне сканування, міжмережевий екран (фаєрвол), аудит змін на сайті, двофакторна автентифікація та захист через Google reCAPTCHA.

На рисунку нижче показано робота механізму Google reCAPTCHA, який є частиною засобів безпеки, реалізованих за допомогою плагіна Wordfence. Після

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

введення облікових даних система вимагає підтвердження, що користувач не є автоматизованим ботом, шляхом виконання простого візуального завдання (наприклад, вибору всіх зображень із мостами). Цей захід спрямований на запобігання автоматизованим атакам перебору паролів (brute-force).

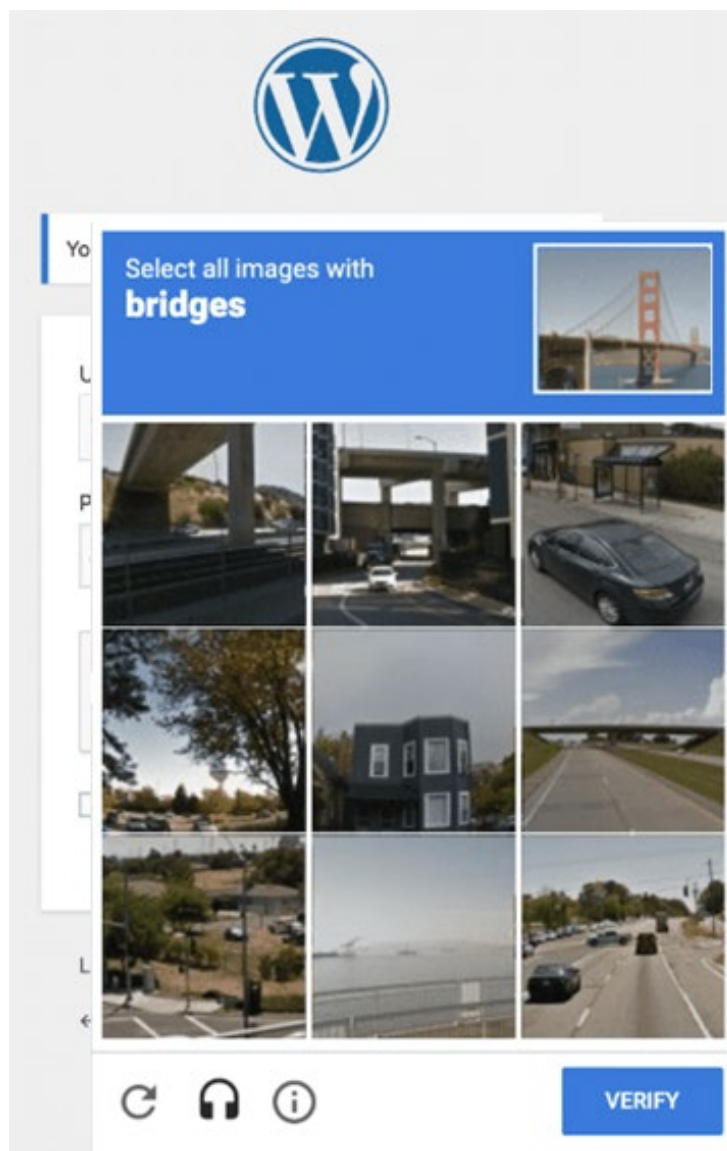


Рисунок 3.36 – reCAPTCHA

Після проходження reCAPTCHA система запитує одноразовий код, який генерується у мобільному додатку таких як Google Authenticator або Authy. Це створює додатковий рівень захисту, унеможливлюючи доступ до облікового запису навіть у разі компрометації основного пароля. Загалом, ці функції демонструють ефективність плагіна Wordfence у реалізації сучасних механізмів захисту авторизації на сайті WordPress.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

Рисунок 3.37 –Введення коду 2FA

Після невдалих спроб зайти, виникає повідомлення, яке при тимчасовому обмеженні доступу до вебсайту користувачеві. Це повідомлення генерується системою безпеки WordPress, найчастіше внаслідок підозрілої активності або надмірної кількості спроб авторизації. У повідомленні вказано, що доступ до сайту було тимчасово обмежено, а також наведено код відповіді сервера – 503 (Service Temporarily Unavailable). Користувач має можливість надіслати запит на розблокування, вказавши свою адміністративну електронну адресу. Подібний механізм забезпечує додатковий рівень захисту від несанкціонованого доступу та атак типу brute-force.

Your access to this site has been temporarily limited
by the site owner

Your access to this service has been temporarily limited. Please try again in a few minutes. (HTTP response code 503)

If you think you have been blocked in error, contact the owner of this site for assistance.

• [Return to the site home page](#)

If you are a WordPress user with administrative privileges on this site, please enter your email address in the box below and click "Send". You will then receive an email that helps you regain access.

email@example.com

SEND UNLOCK EMAIL

Block Technical Data

Block
Reason:

You have been temporarily locked out of this system. This means that you will not be able to log in for a while.

Рисунок 3.38 – Повідомлення про тимчасове блокування доступу до сайту через систему безпеки.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Також передбачена форма для відновлення доступу: адміністративний користувач може ввести свою електронну адресу, після чого система надсилає на пошту автоматичний лист із інструкціями щодо розблокування облікового запису. Цей механізм є частиною системи захисту і спрямований на запобігання несанкціонованому доступу до адміністративної панелі сайту.

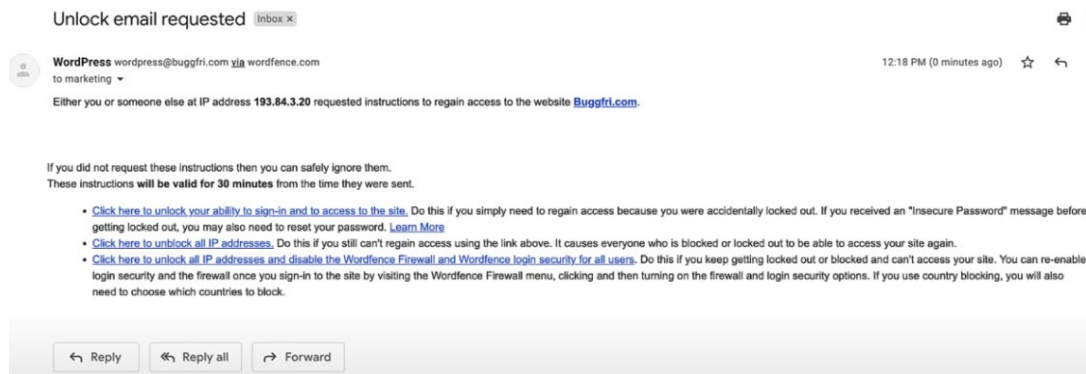


Рисунок 3.39 – Повідомлення з інструкціями щодо розблокування облікового запису

З адміністративної панелі сайту видно, що користувач із зазначеною IP-адресою був автоматично внесений до списку заблокованих. Система безпеки зафіксувала підозрілу активність або порушення встановлених правил доступу, внаслідок чого цей IP був тимчасово заблокований з метою запобігання потенційним загрозам. Адміністратор має можливість переглянути деталі блокування, змінити налаштування фільтрації або вручну розблокувати доступ у разі помилкового спрацювання захисту. На даному рисунку чітко вказана причина блокування – спроба входу з недійсним ім'ям користувача test, що є типовою ознакою підозрілої активності або брутфорс-атаки.

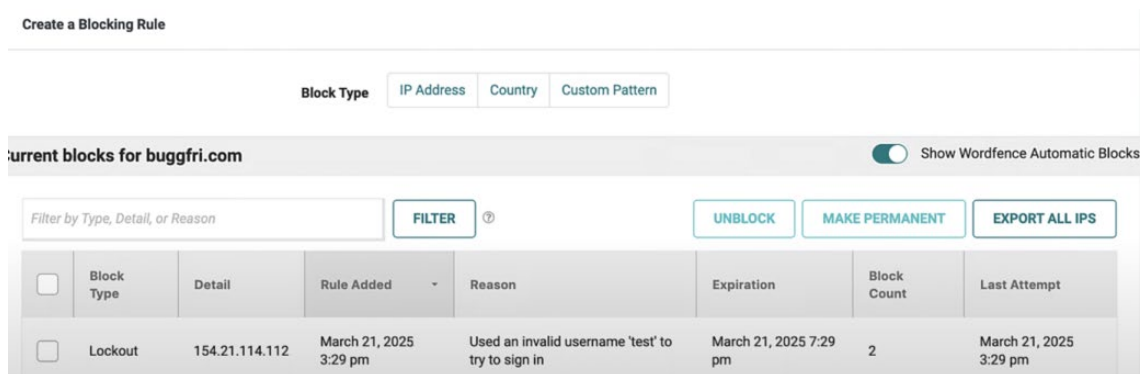


Рисунок 3.40 – Lockout

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

Адміністратор здійснив розблокування користувача, відновивши йому доступ до сайту. Це рішення було прийнято після перевірки інформації про блокування, яка засвідчила відсутність загрози з боку даного користувача. Відповідні дії були виконані через панель керування системою безпеки, де IP-адресу було видалено зі списку заблокованих. Таким чином, доступ до ресурсу для користувача було повністю відновлено.

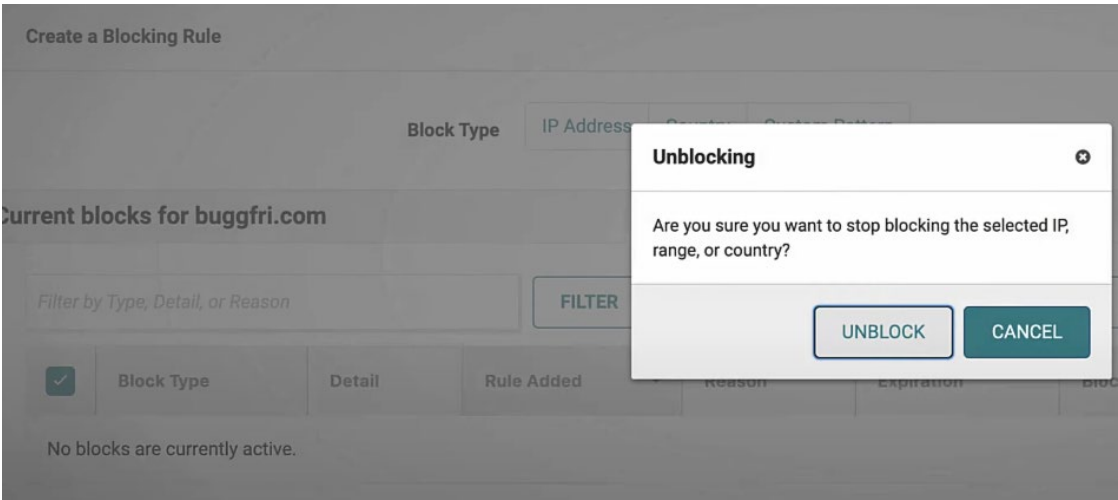


Рисунок 3.41 – Розблокування користувача

Для перевірки коректної роботи та актуального стану захисту, здійснюється вхід до розділу “All Options” у плагіні Wordfence. Тут можна переглянути основні параметри безпеки, активні функції, а також переконатись, що модулі захисту працюють відповідно до встановлених налаштувань.

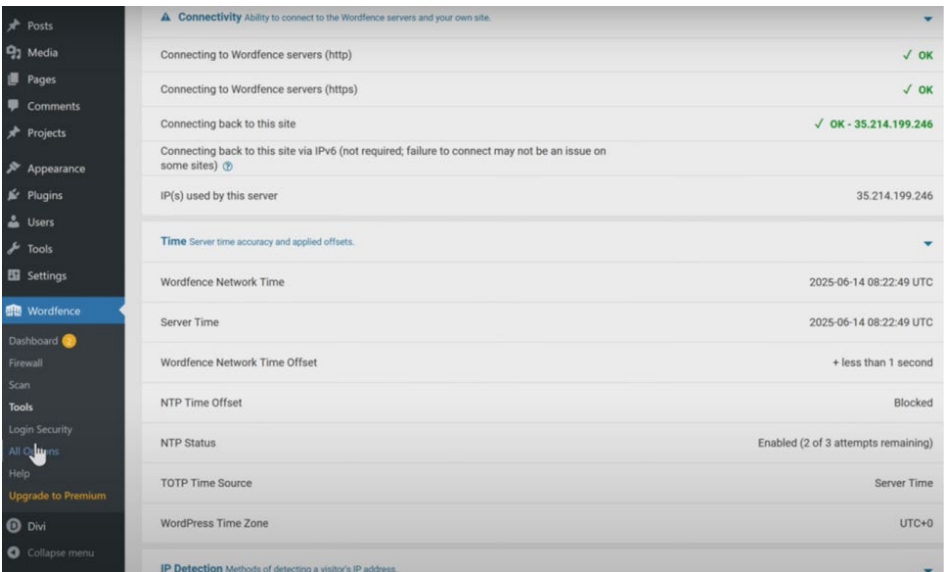


Рисунок 3.42 – All Options Wordfence

У Live Traffic плагіна Wordfence кожен запит позначений кольоровим індикатором, що дозволяє швидко визначити тип активності.

Наприклад:

- червоний – заблокована загроза,
- жовтий – підозріла дія,
- зелений – звичайний перегляд сайту,
- сірий – бот (наприклад, Googlebot). Це спрощує моніторинг і реагування

на потенційні атаки.

На скріншоті показано, що один із користувачів здійснив звичайний перегляд сайту (позначено зеленою точкою), тоді як інший – був заблокований через виявлення потенційної загрози (позначено червоною точкою). Це демонструє, як плагін Wordfence в реальному часі фіксує й розрізняє дії користувачів, своєчасно реагуючи на підозрілу активність та забезпечуючи безпеку ресурсу за допомогою фаєрволу й вбудованої системи моніторингу.

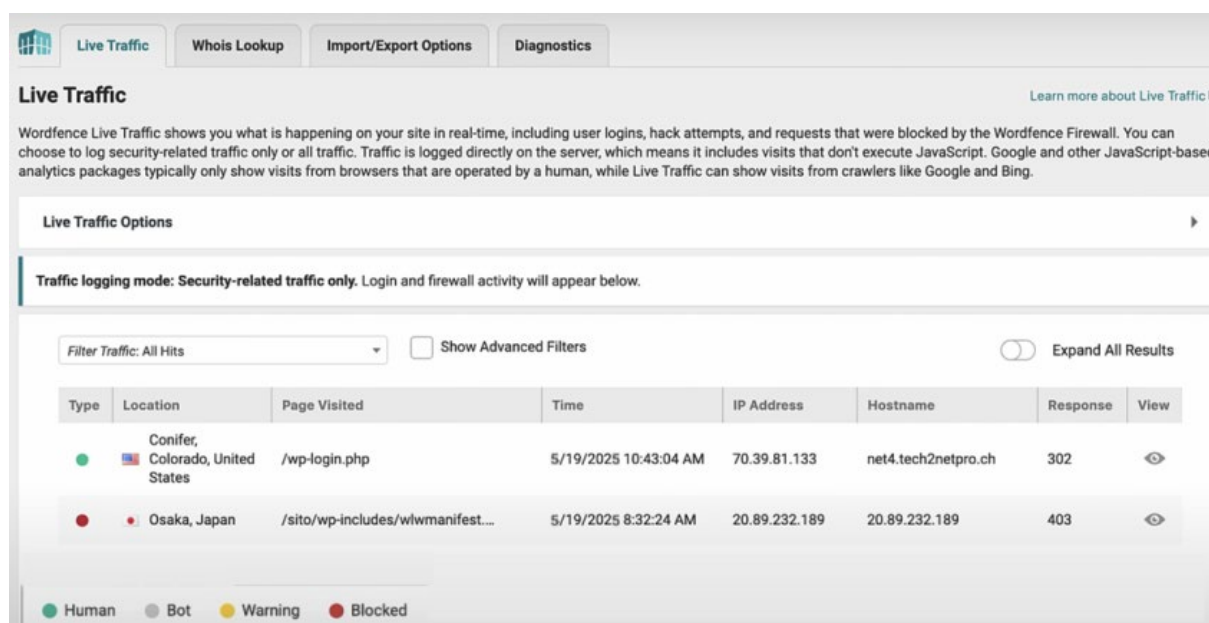


Рисунок 3.43 – Процес Live Traffic

Для виконання цих дій використовувався VPN, що дозволило імітувати доступ до сайту з різних IP-адрес та перевірити, як плагін Wordfence реагує на підозрілу активність, зміну локації та спроби несанкціонованого доступу.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

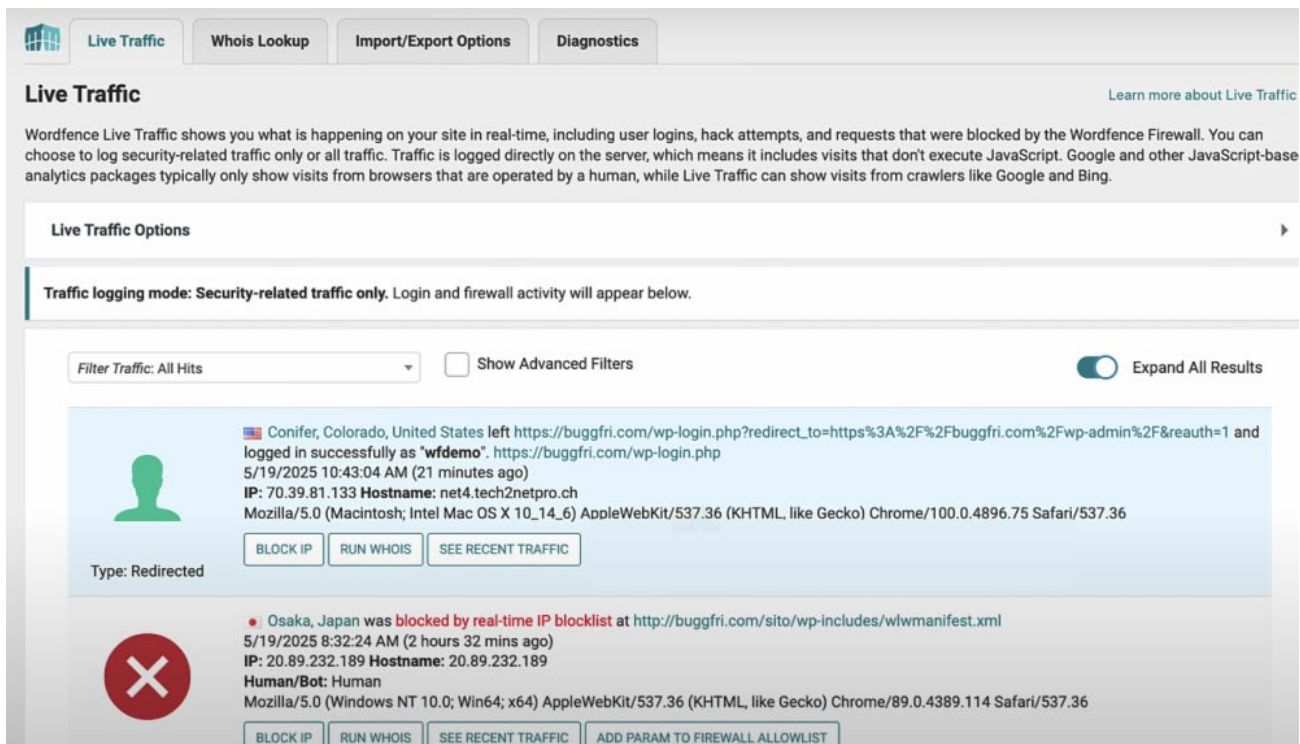


Рисунок 3.44 – Expand All Results

Під час тестування функції Live Traffic у плагіні Wordfence було активовано опцію "Expand All Results", яка дозволила переглядати розширену інформацію про всі дії користувачів на сайті. Це надало можливість оцінити IP-адресу, геолокацію, відвідану сторінку та статус взаємодії з фаєрволом (наприклад, чи було здійснено блокування). У випадках виявлення підозрілої активності з боку певного користувача, тестувальник мав змогу вручну заблокувати IP-адресу, виконати перевірку через сервіс Whois, переглянути недавні запити з того ж IP або, навпаки, додати його до білого списку. Дані можливості підтверджують ефективність інструментів моніторингу та реагування в реальному часі, що є важливим елементом у захисті ресурсу.

Після аналізу підозрілої активності в розділі Live Traffic було здійснено тестування функції блокування IP-адреси. Для цього було обрано IP, з якого зафіксовано потенційно небезпечну або підозрілу дію.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пирог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

Traffic logging mode: Security-related traffic only. Login and firewall activity will appear below.

Filter Traffic: All Hits

Show Advanced Filters

Expand All Results



🇨🇦 Montreal, Quebec, Canada left <https://buggfri.com/wp-login.php> and was **locked out from logging in** at <https://buggfri.com/wp-login.php>
5/19/2025 11:17:32 AM (3 minutes ago)
IP: 199.36.223.65 Hostname: envywomen.com
Human/Bot: Human
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.3 Safari/605.1.15

UNBLOCK IP

RUN WHOIS

SEE RECENT TRAFFIC

Type: Blocked

Рисунок 3.45 – Block IP

Під час перевірки роботи фаєрвола плагіна Wordfence було протестовано механізм автоматичного блокування IP-адрес користувачів, які порушують встановлені правила. У випадку виявлення підозрілої активності або повторних невдалих спроб входу, IP-адреса автоматично блокується на певний проміжок часу.

Тривалість блокування задається у відповідних параметрах Wordfence і може змінюватись відповідно до політики безпеки сайту. Для перевірки часу блокування було відкрито розділ, де відображаються всі заблоковані IP-адреси, включаючи дату та тривалість блокування. Це дає адміністратору змогу контролювати обмеження доступу та, за потреби, змінювати або скасовувати блокування вручну.

Search All Options

RESTORE DEFAULTS

Rate Limiting

Enable Rate Limiting and Advanced Blocking ⓘ
NOTE: This checkbox enables ALL blocking/throttling functions including IP, country and advanced blocking, and the "Rate Limiting Rules" below.

OFF ON

How should we treat Google's crawlers ⓘ
Verified Google crawlers will not be rate-limited

If anyone's requests exceed ⓘ
Unlimited then throttle it

If a crawler's page views exceed ⓘ
Unlimited then throttle it

If a crawler's pages not found (404s) exceed ⓘ
Unlimited then throttle it

If a human's page views exceed ⓘ
Unlimited then throttle it

If a human's pages not found (404s) exceed ⓘ
Unlimited then throttle it

How long is an IP address blocked when it breaks a rule ⓘ
5 minutes

Рисунок 3.46 – Тривалість блокування

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

Найшвидший спосіб переконатися, що сканування сайту відбувається максимально повно – це перейти до розділу **Scan Options and Scheduling** у плагіні Wordfence.

У цьому розділі користувач може вручну налаштувати параметри глибини та частоти сканування, увімкнути перевірку всіх основних файлів ядра WordPress, плагінів, тем, а також увімкнути виявлення шкідливого коду та потенційно небезпечних змін. Це дозволяє забезпечити повне охоплення під час аналізу сайту на загрози, що значно підвищує рівень безпеки ресурсу.

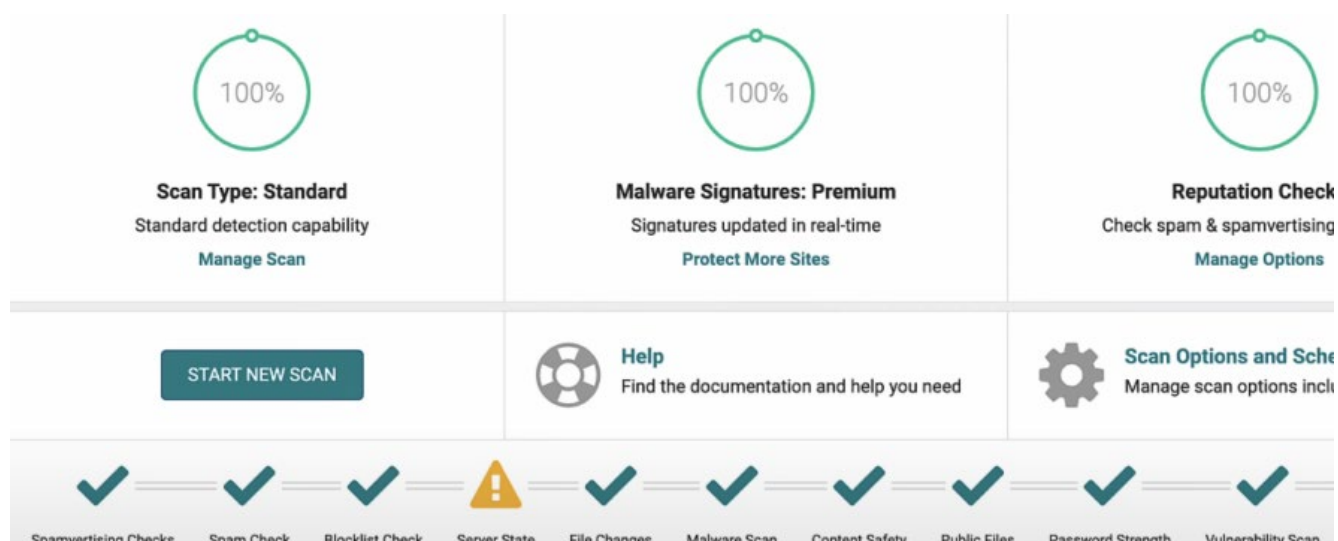


Рисунок 3.47 – Scan

Користувач обирає необхідні параметри сканування в розділі **Scan Options**, щоб забезпечити найбільш ефективну перевірку сайту. Це дозволяє точно налаштувати глибину аналізу, охопити всі критичні компоненти WordPress – включно з файлами ядра, темами, плагінами, базою даних – і виявити можливі загрози, підозрілі зміни або шкідливий код. Такий підхід дає змогу максимально точно оцінити стан безпеки ресурсу.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

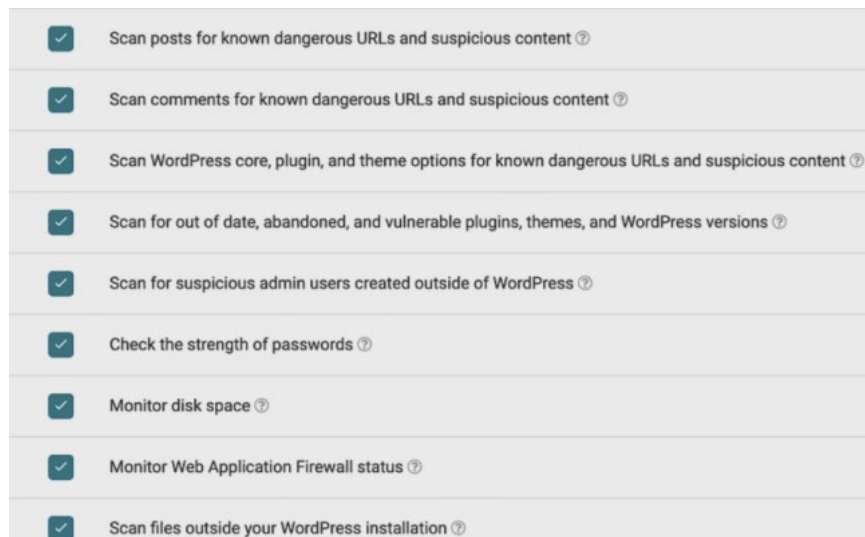


Рисунок 3.48 – Опції або список

Після внесення змін користувач зберігає налаштування та запускає процес перевірки, натиснувши кнопку Start Scan. Це ініціює повне сканування сайту згідно з обраними параметрами безпеки.

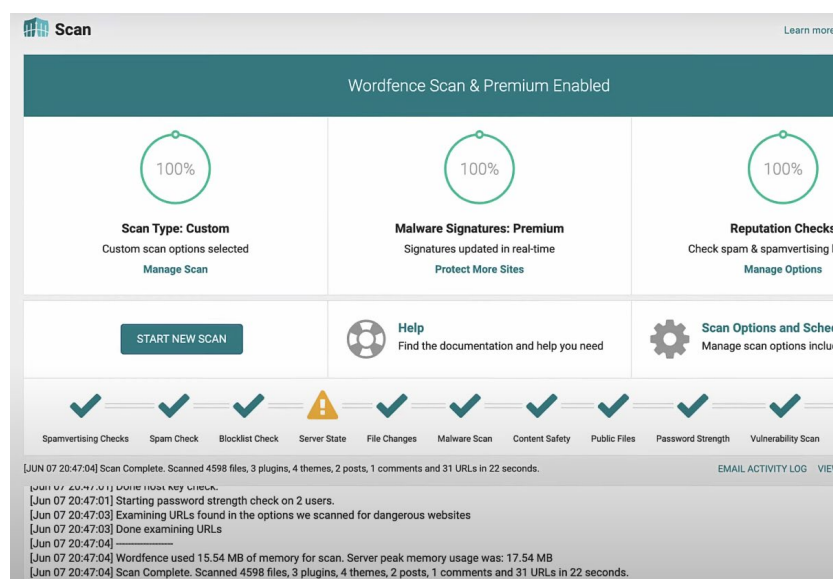


Рисунок 3.49 – Процес сканування

Функції сканування дозволяють переконатися, що сайт не розсилає спам і не перебуває в жодних чорних списках. Крім того, вони допомагають виявити потенційно шкідливі елементи, які можуть загрожувати репутації ресурсу або безпеці користувачів. Регулярне сканування – важлива складова загального захисту вебсайту від кіберзагроз.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

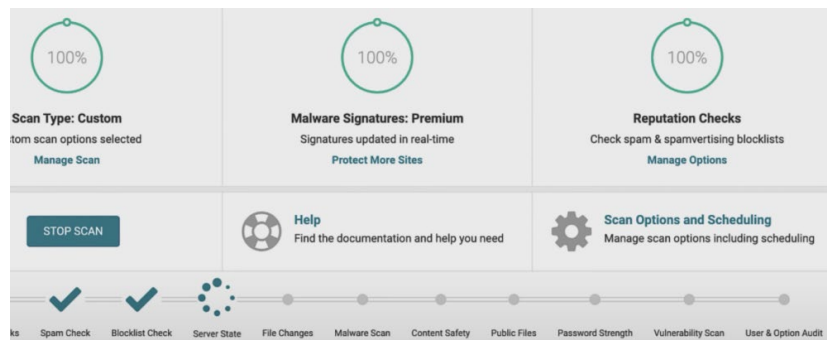


Рисунок 3.50 – Процес сканування

Як видно, сканування було виконано та завершено без виявлення підозрілих результатів. Варто пам'ятати, що з міркувань безпеки перед відновленням або видаленням файлів за допомогою сканера доцільно створити резервну копію сайту або його даних. Це дозволить уникнути втрати важливої інформації у разі непередбачених ситуацій. Крім того, регулярне створення резервних копій сприяє швидкому відновленню роботи сайту у випадку зламу чи технічного збою.

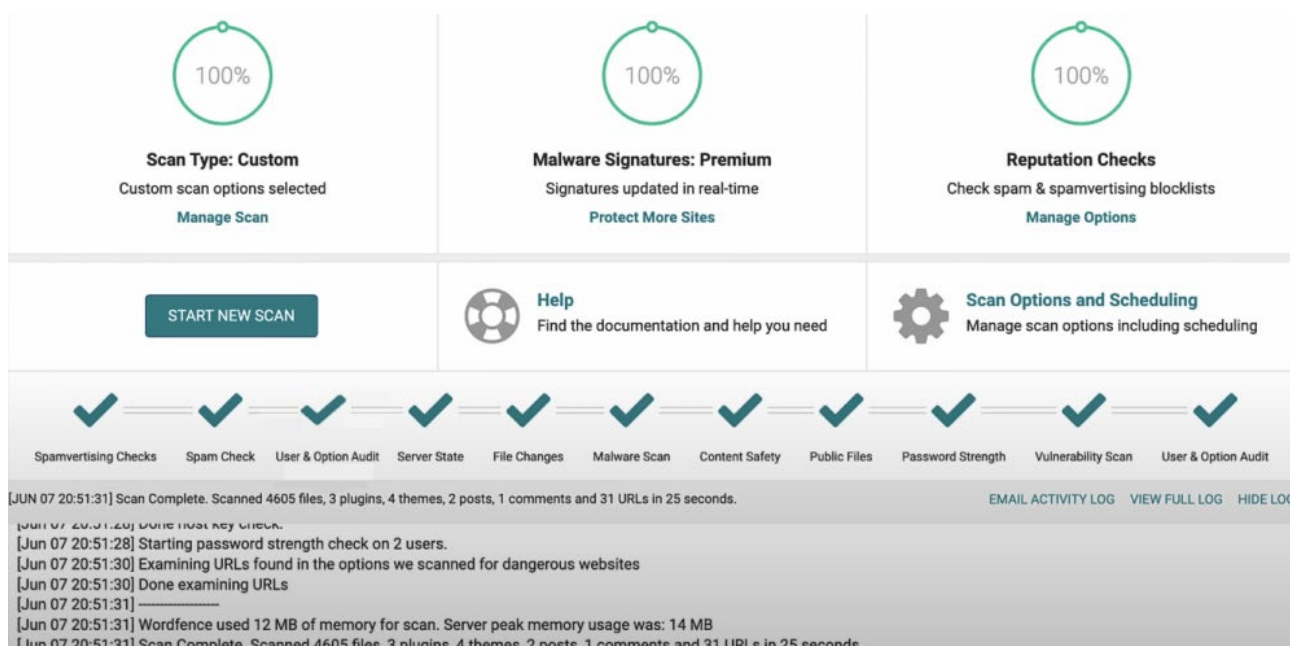


Рисунок 3.51 – Сканування завершено

Після цього адміністратор переходить до тестування Audit Log з метою перевірки коректності фіксації подій у системі. В рамках цього процесу здійснюється ряд дій, таких як спроби входу до панелі керування, активація або деактивація плагінів, зміна файлів, а також імітація підозрілої активності для перевірки реакції системи. Усі події мають бути відображені в журналі з

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

зазначенням часу, IP-адреси, імені користувача та описом дії. Це дозволяє переконатися, що Audit Log працює стабільно та забезпечує надійний контроль за всіма важливими змінами на сайті.

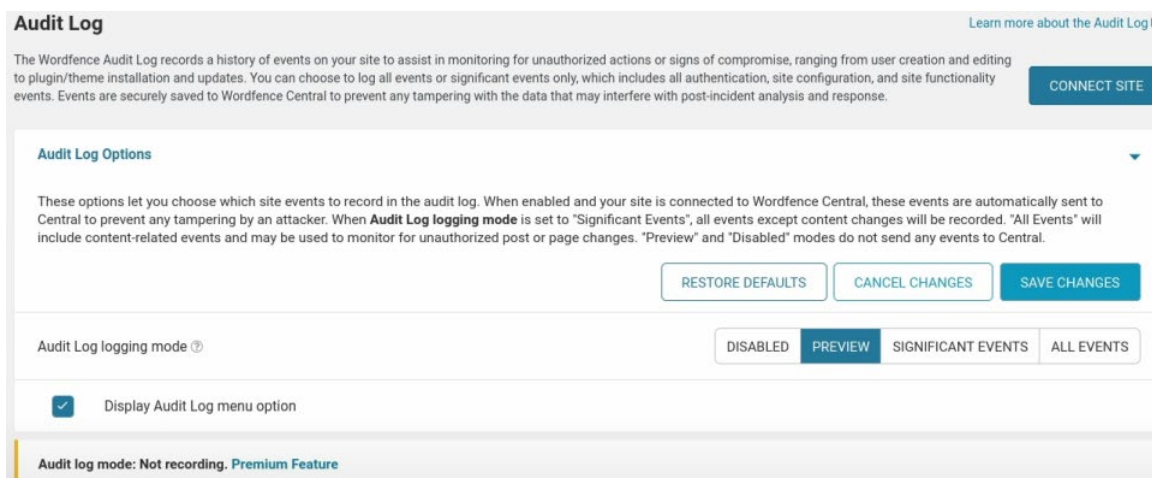


Рисунок 3.52 – Audit Log

Після натискання кнопки **CONNECT SITE** розпочинається процес підключення вебсайту до централізованої системи управління **Wordfence Central**. Сайт автоматично проходить автентифікацію, після чого встановлюється захищене з'єднання між сервером Wordfence та обраним ресурсом. У результаті підключення адміністратор отримує можливість у зручному форматі моніторити стан безпеки сайту, переглядати звіти сканувань, активність користувачів, журнали подій (Audit Log), а також дистанційно керувати налаштуваннями фаєрволу, сканера та іншими функціями без необхідності заходити безпосередньо в панель керування кожного сайту окремо. Це значно спрощує управління безпекою у випадку наявності кількох ресурсів.

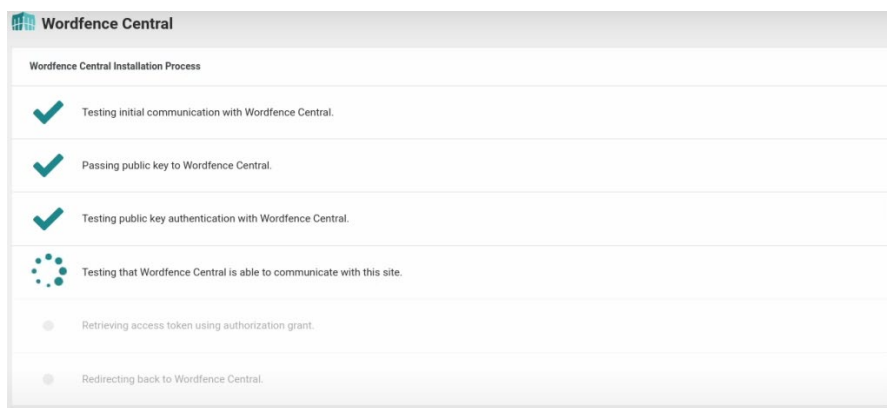


Рисунок 3.53 – Підключення сайтів до Audit Log

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

LAUNCH SCAN			HIGHEST SEVERITY ▾			LICENSE TYPE ▾		LICENSE S	
	Audit Log ▴	Last Scan Date ▴	Highest Severity ▾	Findings ▴	Firewall % ▴	Scan % ▴	License Type ▴	Help	Ac
	Audit Log	June 12; 2025	Critical Malware Scan	11 Res	100%	100%	Premium Upgrade		
n	Audit Log	June 12; 2025	Critical Malware Scan	14 Res	100%	100%	Premium Upgrade		
it	Audit Log	June 12; 2025	Medium File Changes	2 Results	78%	10%	Response		
e	Audit Log	June 12; 2025	Low File Changes	2 Results	78%	98%	Response		
e	Audit Log	June 12; 2025	Medium File Changes	1 Results	78%	48%	Care Upgrade		
!	Audit Log	June 12; 2025	Done found	0 Results	48%	60%	Free Upgrade		
	Audit Log	June 12; 2025	Critical Malware Scan	1 Results	100%	100%	Care Upgrade		
	Audit Log	June 12; 2025	None found	0 Results	10%	100%	Expiring		
...	Audit Log	June 12; 2025	Critical Malware Scan	19 Result	100%	100%	Care Upgrade		

Рисунок 3.54 – Інтерфейс централізованої системи управління безпекою сайтів – Wordfence Central

У таблиці відображено список підключених сайтів, дату останнього сканування (наприклад, *June 12, 2025*), статус фаєрволу, а також найвищий рівень виявлених загроз (наприклад, *Critical | Malware Scan*). Система дозволяє адміністратору здійснювати моніторинг безпеки, переглядати журнали подій, запускати сканування та керувати налаштуваннями без необхідності входу до кожного сайту окремо. Такий підхід значно підвищує ефективність управління інформаційною безпекою у разі роботи з кількома ресурсами.

Також у плагіні Wordfence Security реалізована можливість обмежити доступ до сайту користувачам із конкретних країн. На зображенні видно, як заборонено вхід із певних географічних регіонів. Така функція використовується для запобігання атакам із країн, де найчастіше реєструються спроби злому.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

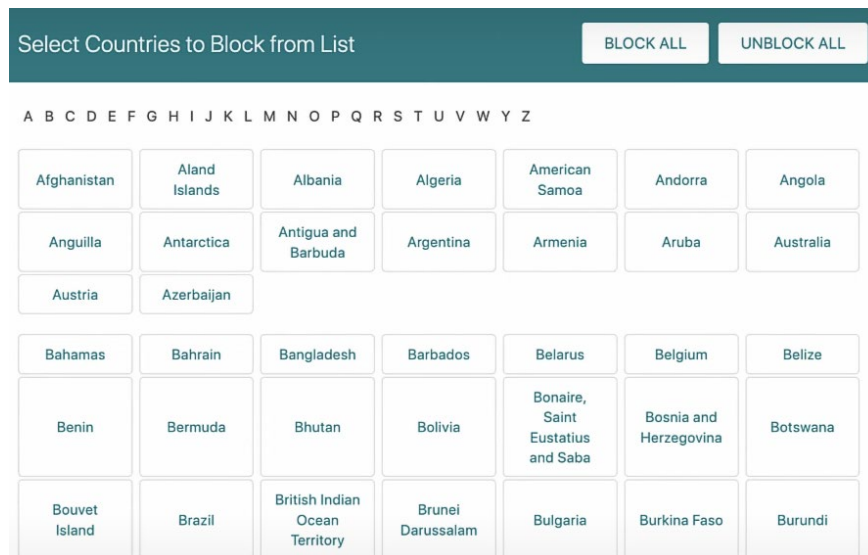


Рисунок 3.55 – Функціонал географічного блокування (Country Blocking) у WordFence

Даний інструмент може блокувати як повний доступ до сайту, так і лише до форми входу. Проте важливо зазначити, що ця функція доступна лише у платній (Premium) версії плагіна Wordfence, тому не кожен адміністратор має змогу її застосовувати. У безкоштовній версії ця можливість відсутня, що обмежує потенціал захисту від загроз, пов'язаних із географічно визначеними джерелами. Використання Country Blocking особливо доцільне для сайтів, орієнтованих на локальну аудиторію, де міжнародний трафік є непотрібним або потенційно небезпечним.

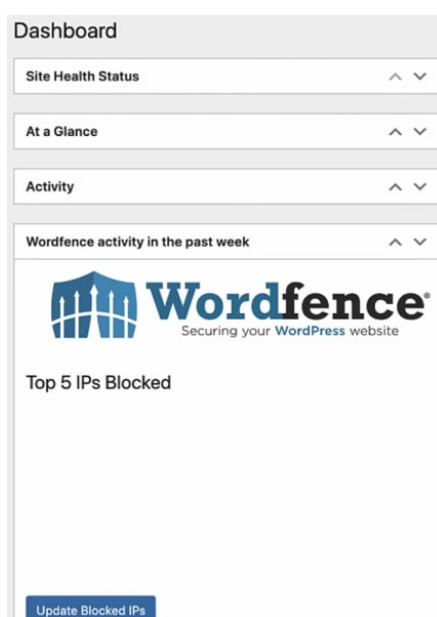


Рисунок 3.56 – Частина панелі керування (Dashboard) WordPress

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

У процесі практичного тестування було перевірено ключові можливості плагіна Wordfence Security, а саме: функцію сканування сайту (Scan), журнал подій (Audit Log), двохфакторну автентифікацію (2FA), аналіз вхідного трафіку, блокування IP-адрес, а також географічне блокування (Country Blocking).

Сканування сайту виявило потенційні загрози, включаючи змінені файли та підозрілі плагіни, що дозволяє оперативно реагувати на ризики. Audit Log надійно зафіксував усі дії користувачів і системи, що є важливим для контролю безпеки. Впровадження 2FA значно підвищило рівень захисту облікових записів адміністраторів. Аналіз трафіку надав можливість виявити джерела підозрілої активності, а блокування IP-адрес дозволило швидко реагувати на несанкціоновані спроби доступу. Окремо було протестовано функцію Country Blocking, яка доступна лише у преміум-версії плагіна. Вона дає змогу обмежити доступ до сайту або до форми входу для користувачів з певних країн, що є корисним інструментом для захисту від атак з конкретних географічних регіонів.

Висновок до третього розділу

У процесі налаштування та тестування плагіна Wordfence Security було реалізовано комплексний підхід до забезпечення інформаційної безпеки вебсайту на базі WordPress. Активовано ключові модулі захисту, зокрема: фаєрвол, система сповіщень про підозрілу активність (вхід адміністратора, використання форми відновлення пароля), а також глибоке сканування ядра CMS, плагінів, тем, конфігураційних файлів, коментарів і вмісту на наявність шкідливого коду, шкідливих URL-адрес і змінених компонентів.

Налаштування параметрів продуктивності плагіна дозволило досягти оптимального балансу між глибиною перевірки та стабільністю роботи сервера, що особливо важливо для сайтів з обмеженими технічними ресурсами. Це забезпечило безперервний захист без негативного впливу на швидкодію системи.

У рамках практичного тестування були перевірені такі функції плагіна, як:

- **Scan** – інструмент сканування сайту, який дозволив виявити змінені файли, потенційно небезпечні плагіни та шкідливі фрагменти коду;

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

- **Audit Log** – журнал подій, що надійно фіксував усі дії користувачів і системи, дозволяючи здійснювати контроль над активністю на сайті;
- **Двофакторна автентифікація (2FA)** – додатковий рівень захисту облікових записів адміністраторів, що знижує ймовірність несанкціонованого доступу;
- **Аналіз трафіку** – моніторинг підозрілих запитів і визначення джерел потенційних атак;
- **Блокування IP-адрес** – можливість оперативно заблокувати доступ з небажаних або зловмисних IP;
- **Country Blocking** – функція географічного блокування, яка протестована окремо й доступна лише у преміум-версії. Вона дозволяє обмежити доступ до сайту або до його адміністративної частини для користувачів з певних країн, що особливо актуально для локальних ресурсів.

Загалом, проведене налаштування й тестування плагіна Wordfence підтвердило його високу ефективність як інструменту для багаторівневого, надійного та гнучкого захисту вебресурсів. Інтеграція функцій активного моніторингу, реагування на загрози та автоматичного блокування суттєво підвищує загальний рівень кіберзахисту сайту, зменшує ризик зовнішнього втручання та дозволяє адміністраторам вчасно реагувати на потенційні атаки.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

ВИСНОВКИ

У результаті проведеної кваліфікаційної роботи було реалізовано комплексний підхід до підвищення рівня безпеки вебсайту на базі системи управління вмістом WordPress. На основі детального аналізу архітектури WordPress, типових вразливостей вебзастосунків і сучасних загроз інформаційній безпеці, було сформовано перелік вимог до безпечної конфігурації сайту, а також підібрано ефективні інструменти для його захисту.

Найважливішим компонентом практичної частини роботи стало впровадження і налаштування плагіна **Wordfence Security**, що дозволило досягти високого рівня захищеності вебресурсу від найпоширеніших типів атак. У рамках дослідження було досягнуто всіх поставлених завдань:

1. Проаналізовано структуру WordPress та типові уразливості, серед яких – наявність плагінів з ненадійним кодом, використання слабких паролів, відсутність шифрування передавання даних, відкритий доступ до важливих системних файлів тощо. Це дозволило більш точно визначити зони ризику та шляхи їх усунення.

2. Обґрунтовано необхідність впровадження плагінів безпеки, зокрема таких, що здійснюють моніторинг, блокування, сканування та контроль доступу. На підставі порівняння кількох доступних рішень було обрано Wordfence як один із найпотужніших і найбільш функціональних плагінів.

3. Реалізовано тестування функціоналу Wordfence, що охоплювало:

- запуск системи сканування на наявність змінених файлів, потенційно шкідливих кодів і загроз;
- використання журналу подій (Audit Log), який дозволив простежити всі дії на сайті та виявити підозрілу активність;
- налаштування **фаєрволу**, який ефективно фільтрує небезпечні запити ще до того, як вони потраплять у WordPress;
- увімкнення **двохфакторної автентифікації (2FA)** для облікових записів адміністраторів, що знижує ризик несанкціонованого доступу;

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

- **блокування IP-адрес** – протестовано функцію автоматичного обмеження доступу для користувачів, які намагаються підібрати паролі або надсилають підозрілі запити;
- використання **системи сповіщень**, яка в режимі реального часу повідомляє адміністратора про критичні події: спроби входу, зміну файлів, підозрілу активність;
- протестовано елементи преміум-версії, зокрема **геоблокування (Country Blocking)** – ефективний інструмент для локальних проєктів, що дозволяє закривати доступ до адміністративної частини сайту з певних країн.

4. Проведено симуляцію типових загроз, зокрема: спроби підбору паролів, надсилання шкідливих SQL-запитів, використання небезпечних плагінів, тестування вразливостей XSS. У кожному випадку плагін Wordfence надавав адекватну відповідь: блокував дії, сповіщав про інцидент або дозволяв адміністратору втрутитися вручну.

Ключовим результатом дослідження стало усвідомлення того, що захист WordPress неможливо забезпечити лише одним плагіном чи окремим заходом. Лише системний, багаторівневий і постійно оновлюваний підхід дає змогу ефективно протистояти сучасним кібератакам. Серед таких заходів – оновлення ядра, плагінів і тем, обмеження прав користувачів, регулярне резервне копіювання, контроль активності, використання HTTPS, приховування панелі входу, впровадження CAPTCHA і 2FA.

Wordfence є ефективним і гнучким засобом для підвищення рівня кіберзахисту вебресурсів, побудованих на WordPress. Його впровадження у поєднанні з іншими методами захисту дозволяє значно знизити ризик проникнення, втрати даних і компрометації системи.

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The Role of Themes in WordPress Website Security. [Електронний ресурс] – Режим доступу: <https://debutify.com/blog/role-of-themes-in-wordpress-website-security/>
2. How and why you should use WordPress to develop a Web Application. [Електронний ресурс] – Режим доступу: <https://illustrate.digital/wordpress/how-and-why-you-should-use-wordpress-to-develop-a-web-application/>
3. Ways of protecting the CMS WordPress-based sites . [Електронний ресурс] – Режим доступу: [file:///C:/Users/hh824/Downloads/232204-Article%20Text-530695-1-10-20210521%20\(1\).pdf](file:///C:/Users/hh824/Downloads/232204-Article%20Text-530695-1-10-20210521%20(1).pdf)
4. What Is Web Application Security and How Does It Work? . [Електронний ресурс] – Режим доступу: [.blackduck.com/glossary/what-is-web-application-security.html#:~:text=Web%20application%20security%20\(also%20known,assets%20from%20potentially%20malicious%20agents](https://blackduck.com/glossary/what-is-web-application-security.html#:~:text=Web%20application%20security%20(also%20known,assets%20from%20potentially%20malicious%20agents)
5. What are Confidentiality, Integrity and Availability in Information Security? . [Електронний ресурс] – Режим доступу: <https://vinciworks.com/blog/what-are-confidentiality-integrity-and-availability-in-information-security/>
6. Confidentiality, Integrity, and Availability: The CIA Triad. [Електронний ресурс] – Режим доступу: <https://informationsecurity.wustl.edu/guidance/confidentiality-integrity-and-availability-the-cia-triad/>
7. Розуміння основних принципів інформаційної безпеки . [Електронний ресурс] – Режим доступу: <https://www.centraleyes.com/core-principles-of-information-security/>
8. DataSunrise Achieves AWS DevOps Competency Status in AWS DevSecOps and Monitoring, Logging, Performance . [Електронний ресурс] – Режим доступу: <https://www.datasunrise.com/knowledge-center/confidentiality-integrity-availability-examples/>

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

9. Common Web Application Vulnerabilities Explained - Rapid7 . [Електронний ресурс] – Режим доступу:<https://www.rapid7.com/fundamentals/web-application-vulnerabilities/>

10. Measures to secure content management systems (CMS) . [Електронний ресурс] – Режим доступу: <https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-cms.html>

11. What is WordPress: Benefits, Uses and Website Creation. [Електронний ресурс] – Режим доступу: <https://jam.in.ua/en/blog-en/what-is-cms-wordpress-and-how-to-use-it-a-complete-guide/>

12. WordPress CMS: Key Concepts and Features Explained[Електронний ресурс] – Режим доступу: <https://blog.shiftingcube.com.au/wordpress-cms-key-concepts-and-features-explained/>

13. What Is an Injection Attack?. [Електронний ресурс] – Режим доступу: <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/injection-attack/>

14. What is cross-site scripting (XSS) and how to prevent it?.[Електронний ресурс] – Режим доступу: <https://portswigger.net/web-security/cross-site-scripting>

15. Cross Site Request Forgery (CSRF) [Електронний ресурс] – Режим доступу: <https://owasp.org/www-community/attacks/csrf>

16. What is Social Engineering? [Електронний ресурс] – Режим доступу: <https://www.kaspersky.com/resource-center/definitions/what-is-social-engin>

17. Top 10 Most Common WordPress Vulnerabilities to Look Out For in 2024[Електронний ресурс] – Режим доступу: <https://thecyberexpress.com/top-10-wordpress-vulnerabilities/>

18. Most Common WordPress Vulnerabilities & How to Fix Them[Електронний ресурс] – Режим доступу: <https://patchstack.com/articles/common-plugin-vulnerabilities-how-to-fix-them/>

19. Запобігання міжсайтовому скриптингу (XSS) в JavaScript[Електронний ресурс] – Режим доступу: <https://webcraftingcode.com/uk/krashchi-praktyky-veb-rozrobky/zapobihannia-mizhsaytovomu-skryptynhu-xss-v-javascript/>

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

20. WordPress CSRF Attack: What It Is and How to Prevent It? [Електронний ресурс] – Режим доступу: <https://passwordprotectedwp.com/wordpress-csrf-attack/>
21. Best Practices and Plugins For a Secure WordPress Site [Електронний ресурс] – Режим доступу: <https://medium.com/@anuj.tomar11/best-practices-and-plugins-for-a-secure-wordpress-site-1f4112cda194>
22. The Ultimate WordPress Security Guide – Step by Step (2025) [Електронний ресурс] – Режим доступу: <https://www.wpbeginner.com/wordpress-security/>
23. How to set up WordPress role based access control to secure site folders? [Електронний ресурс] – Режим доступу: <https://www.miniorange.com/blog/access-control-on-website-folders-with-reverse-proxy/>
24. How to Secure Your WordPress Login Page (Complete Guide) [Електронний ресурс] – Режим доступу: <https://jetpack.com/resources/wordpress-login-security/>
25. Protecting the WordPress admin panel [Електронний ресурс] – Режим доступу: <https://fornex.com/help/security-wp-admin/>
26. How to Secure Your WordPress Pages With SSL (Step by Step) [Електронний ресурс] – Режим доступу: <https://www.wpbeginner.com/wp-tutorials/how-to-secure-your-wordpress-pages-with-ssl/>
27. How To Fix Common SSL Issues In WordPress) [Електронний ресурс] – Режим доступу: <https://www.dreamhost.com/blog/how-to-fix-common-ssl-issues-wordpress/>
28. Understanding TLS for WordPress Users [Електронний ресурс] – Режим доступу: <https://www.elegantthemes.com/blog/wordpress/understanding-tls-for-wordpress-users>
29. iThemes Security vs Wordfence: Which Security Plugin Should You Choose? [Електронний ресурс] – Режим доступу: <https://www.malcare.com/blog/ithemes-security-vs-wordfence/>
30. Wordfence Security – Firewall, Malware Scan, and Login Security [Електронний ресурс] – Режим доступу: <https://ru.wordpress.org/plugins/wordfence/>

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

31. Wordfence Security – Firewall, Malware Scan, and Login Security
[Електронний ресурс] – Режим доступу: <https://uk.wordpress.org/plugins/wordfence/>

32. iThemes Security [Електронний ресурс] – Режим доступу:
[Електронний ресурс] – Режим доступу: <https://infinitewp.com/addons/ithemes-security/>

33. iThemes Security Review: Is It Worth Installing on Your WordPress Site?
[Електронний ресурс] – Режим доступу: <https://www.malcare.com/blog/ithemes-security-review/>

		Томасов Р.О.			ККІКБ.КР.Б – 125 – 49 – ПЗ	Арк.
		Пірог О.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		92