Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Порівняльний аналіз сканерів вразливостей і брандмауера веб-додатків для бізнесу

Виконав(ла): студент(ка) 4 курсу, групи СБ-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Тригубець М. І. (прізвище та ініціали)

Керівник (підпис) Загородна Н. В. (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т. Б. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) Луцків А. М. (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н. В.
(підпис) (прізвище та ініціали)
«19» червня 2023 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Тригубцю Мирославу Івановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Порівняльний аналіз сканерів вразливостей і брандмауера веб-додатків для бізнесу

Керівник роботи Загородна Наталія Володимирівна, кандидат технічних наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*03*» *квітня* 2023 року № *4\7-349*

2. Термін подання студентом завершеної роботи 19.06.2023

3. Вихідні дані до роботи включають деталі про структуру використовуваної інформаційної системи та вимоги до її системи захисту, які обхоплюють апаратне та програмне забезпечення, типи даних, які обробляються, і специфічні критерії безпеки.

4. Зміст роботи (перелік питань, які потрібно розробити)
Робота охоплює аналіз технічного завдання та вимог до системи захисту інформації, розробку загальної структури захисту інформації та моделей загроз, обґрунтування вибору політики та засобів безпеки, проектування системи захисту, її реалізацію та тестування, а також розгляд питань безпеки життєдіяльності та впливу електромагнітних полів на людей.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Аналіз вимог до системи захисту інформації, OWASP і сканери вразливостей, Вибір тестового середовища: OWASP Juice Shop, Огляд та порівняльний аналіз сканерів вразливостей, Порівняльний аналіз результатів: Acunetix, Burp Suite Enterprise Edition, Nessus Professional, OpenVAS, Огляд та порівняльний WAF, Порівняльний аналіз сканерів вразливостей брандмауерів: CloudFlare WAF, AWS Shield/WAF, AstraSecurity Firewall, Результати дослідження - ефективність WAF та рекомендації, Висновки, Практична значимість

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 18.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Початок роботи, визначення теми та мети дослідження	31.01.2023 – 14.02.2023	*Виконано*
2	Аналіз технічного завдання та вимог до системи захисту	15.02.2023 – 28.02.2023	*Виконано*
3	Розробка узагальненої структури системи захисту інформації	1.03.2023 – 14.03.2023	*Виконано*
4	Розробка моделі загроз та моделі порушника	15.03.2023 – 31.03.2023	*Виконано*
5	Обґрунтування вибору політики та засобів безпеки	1.04.2023 – 14.04.2023	*Виконано*
6	Проектування системи захисту інформації	15.04.2023 – 30.04.2023	*Виконано*
7	Реалізація або моделювання проектних рішень	1.05.2023 – 15.05.2023	*Виконано*
8	Тестування системи захисту інформації	16.05.2023 – 31.05.2023	*Виконано*
9	Розгляд питань безпеки життєдіяльності, основ охорони праці	1.06.2023 – 10.06.2023	*Виконано*
10	Підготовка висновків, формування списку використаних джерел та підготовка до захисту	11.06.2023 – 19.06.2023	*Виконано*
11	Захист кваліфікаційної роботи	21.06.2023	

Студент _____ Тригубець М. І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Загородна Н.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Порівняльний аналіз сканерів вразливостей і брандмауера веб-додатків для бізнесу // Кваліфікаційна робота ОР «Бакалавр» // Тригубець Мирослав Іванович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // С. 70, рис. 13, табл. 8, кресл. – , додат. 2

Ключові слова: СКАНЕРИ ВРАЗЛИВОСТЕЙ, БРАНДМАУЕР, ВЕБ-ДОДАТОК, БІЗНЕС, ПОРІВНЯЛЬНИЙ АНАЛІЗ

Об'єктом дослідження – сканери вразливостей та брандмауери веб-додатків, які використовуються в бізнес-середовищі.

У першому розділі роботи проведений аналіз вимог до систем захисту інформації У другому розділі здійснений порівняльний аналіз сканерів вразливостей, таких як Acunetix, Burp Suite Enterprise Edition, Nessus Professional та OpenVAS, з урахуванням їх функціональності, можливостей і обмежень та здійснений порівняльний аналіз різних брандмауерів, зокрема CloudFlare WAF, AWS Shield/WAF та AstraSecurity Firewall. У третьому розділі проведено тестування сканерів вразливостей та брандмауерів. У четвертому розділі проведено аналіз актуальності безпеки життєдіяльності людини та вплив електромагнітних полів (ЕМП) на людину та заходи щодо зменшення їх впливу на обслуговуючий персонал.

В результаті аналізу було визначено, що WAF є ефективними інструментами для захисту веб-додатків у бізнес-середовищі. Кожен з них має свої переваги та особливості, які потрібно враховувати при виборі найбільш підходящого рішення для конкретного бізнесу.

Отже, дана кваліфікаційна робота надає корисні рекомендації щодо вибору і використання сканерів вразливостей та брандмауерів для ефективного захисту веб-додатків у бізнес-середовищі.

ABSTRACT

Comparative analysis of vulnerability scanners and web application firewall for business // Thesis of educational level "Bachelor" // Tryhubets Myroslav Ivanovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, СБ-41 group // Ternopil, 2023 // P. 70 , fig. - 13, table. - 8 , chair. -, added. - 2.

Keywords: VULNERABILITY SCANNERS, WEB APPLICATION FIREWALLS, WEB APPLICATION, BUSINESS, COMPARATIVE ANALYSIS

The object of the research is vulnerability scanners and web application firewalls used in a business environment.

In the first section of the work, an analysis of information security system requirements is conducted. The second section presents a comparative analysis of vulnerability scanners, such as Acunetix, Burp Suite Enterprise Edition, Nessus Professional, and OpenVAS, taking into account their functionality, capabilities, and limitations. A comparative analysis of various web application firewalls, including CloudFlare WAF, AWS Shield/WAF, and AstraSecurity Firewall, is also performed.

The third section focuses on the testing of vulnerability scanners and web application firewalls. The fourth section analyzes the relevance of human life security and the impact of electromagnetic fields (EMF) on humans, as well as measures to mitigate their effects on support personnel.

Based on the analysis, it was determined that web application firewalls (WAFs) are effective tools for protecting web applications in a business environment. Each of them has its advantages and features that need to be considered when selecting the most suitable solution for a specific business.

Therefore, this qualification work provides valuable recommendations for the selection and use of vulnerability scanners and web application firewalls for effective web application protection in a business environment.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

WAF — веб-додатковий брандмауер;

MFA — багатофакторна аутентифікація;

AWS — Amazon Web Services;

ІБ — інформаційна безпека;

SSL — протокол безпеки передачі даних;

VPN — віртуальна приватна мережа;

ЕМП — Електромагнітні поля ЕМП;

ВСТУП

У сучасному цифровому світі, де комп'ютерні системи та веб-додатки стали неодмінною частиною бізнес-середовища, забезпечення безпеки цих систем стає надзвичайно важливим завданням для будь-якої організації. Розмір та складність загроз веб-середовищу зростають, що ставить компанії перед необхідністю в захисті своїх додатків та даних від вразливостей та атак.

Однією з найпоширеніших практик щодо забезпечення безпеки веб-додатків є використання сканерів вразливостей та брандмауерів. Сканери вразливостей - це інструменти, призначені для виявлення потенційних вразливостей у веб-додатках, тоді як брандмауери веб-додатків забезпечують захист від різних типів атак та зловживань.

У рамках кваліфікаційної роботи метою є проведення порівняльного аналізу сканерів вразливостей та брандмауерів веб-додатків для бізнес-середовища. Основна увага буде приділена розгляду та оцінці різних сканерів вразливостей, які використовуються для виявлення потенційних вразливостей веб-додатків, а також брандмауерів, які забезпечують захист від різних типів атак та зловмисниць.

Основна мета дослідження полягає в обґрунтуванні та наданні рекомендацій щодо вибору оптимальних рішень для забезпечення безпеки веб-додатків у бізнес-середовищі. Для досягнення цієї мети виконуються наступні завдання:

1. Проведення огляду та аналізу різних сканерів вразливостей веб-додатків, включаючи їх функціональні можливості, методи виявлення вразливостей, швидкість та точність роботи, а також зручність використання та налаштування.

2. Вивчення основних характеристик та функцій брандмауерів веб-додатків, які забезпечують захист від різних типів атак та зловмисниць.

Особлива увага приділяється можливостям фільтрації вхідного та вихідного трафіку, контролю доступу та автоматичному виявленню та блокуванню атак.

3. Порівняння та аналіз різних сканерів вразливостей та брандмауерів веб-додатків з точки зору їх ефективності, надійності, легкості використання та налаштування, інтеграції з іншими системами, вартості та підтримки.

4. Визначення переваг та недоліків кожного з розглянутих рішень і надання рекомендацій щодо вибору оптимальних засобів захисту веб-додатків для бізнес-середовища.

В результаті проведеного порівняльного аналізу очікується, що кваліфікаційна робота надасть корисну інформацію та рекомендації бізнес-спільноті щодо вибору найкращих сканерів вразливостей та брандмауерів веб-додатків для забезпечення безпеки їх інформаційних активів. Таке дослідження допоможе підвищити рівень безпеки веб-додатків у бізнес-середовищі та запобігти можливим загрозам та атакам.

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

Разом з тим, як кіберпростір стає все більше заплутаним та небезпечним, впровадження ефективних систем кібербезпеки стає все більш актуальним для більшості організацій. Саме тому початковий етап аналізу технічного завдання в контексті цього проекту є критично важливим. Наша ціль - забезпечити зрозуміння всіх вимог, особливостей та викликів, з якими ми можемо зіткнутися під час розробки системи кібербезпеки.

Технічне завдання - це документ, що детально описує всі вимоги до майбутнього продукту або системи, включаючи технічні та функціональні характеристики, специфікації, стандарти якості та інші важливі аспекти. Цей документ стане нашим головним керівництвом протягом усього процесу розробки.

При аналізі технічного завдання нашою основною метою є визначення вимог до системи кібербезпеки. Це може включати, наприклад, вимоги до безпеки даних, до доступності системи, до її масштабованості та інтеграції з іншими системами, до часу відновлення після аварії та багато іншого. Такий аналіз дає нам змогу більше дізнатися про очікування клієнта та визначити, які ресурси та технології будуть необхідні для досягнення цих цілей.

Крім того, на цьому етапі ми збираємося проаналізувати різні можливі рішення для реалізації поставленого завдання. Це може означати дослідження різних технологій та підходів, оцінювання їхньої відповідності нашим вимогам, вартості та потенційного впливу на загальну продуктивність системи.

На заключному етапі аналізу ми складаємо план реалізації проекту, визначаємо основні етапи роботи, відповідні відповідальності та терміни виконання.

1.1 Аналіз вимог до системи захисту інформації

При розробці системи захисту інформації критично важливо правильно зрозуміти і визначити вимоги до системи. Вимоги відіграють ключову роль у формуванні стратегії кібербезпеки, виборі технологій, проектуванні архітектури системи та плануванні ресурсів.

Перш за все, потрібно визначити, які дані будуть оброблятися та зберігатися в системі. Це можуть бути персональні дані, фінансова інформація, комерційні таємниці, технічні деталі продуктів або інша важлива інформація. Виходячи з типу даних, можна визначити рівень захисту, який потрібно забезпечити, та відповідні нормативні вимоги.

Крім того, важливо враховувати функціональні вимоги до системи. Це може включати в себе питання доступності та продуктивності системи, її масштабованості, можливості інтеграції з іншими системами, способу обробки даних та взаємодії з користувачами.

Також важливо визначити вимоги до відновлення системи після потенційних інцидентів кібербезпеки. Це включає в себе планування резервного копіювання, відновлення даних, реагування на інциденти та здійснення заходів з попередження подальших порушень.

При аналізі вимог до системи захисту інформації важливо враховувати технічні та організаційні обмеження. Це можуть бути бюджет, доступні технології, кваліфікація персоналу, час на реалізацію проекту та інші фактори, які можуть впливати на проектування та впровадження системи захисту інформації.

Вимоги до системи захисту інформації можуть бути різноманітними, залежно від конкретних потреб та контексту організації. Вимоги до системи захисту відповідно до українського законодавства описано в [1]. Приклади вимог, які можуть бути поставлені:

1. Конфіденційність. Вимога забезпечення конфіденційності означає, що система повинна захищати інформацію від несанкціонованого

доступу. Наприклад, може вимагатися, щоб система забезпечувала шифрування даних під час їх передачі, а також контроль доступу до конфіденційних даних на рівні користувачів.

2. Цілісність. Вимога цілісності передбачає, що система має захищати дані від несанкціонованої модифікації або втрати. Це може включати застосування механізмів контролю цілісності, таких як хеш-суми, цифрові підписи або контрольні суми, для перевірки цілісності даних під час передачі або зберігання.

3. Доступність. Вимога до доступності ставить завдання забезпечити, щоб система завжди була доступною для користувачів, яким вона призначена. Це означає використання механізмів резервування, розподіленого оброблення завдань та контролю навантаження, щоб запобігти перебоям у роботі системи.

4. Аутентифікація і авторизація. Вимога до аутентифікації та авторизації передбачає, щоб система перевіряла ідентичність користувачів та надавала їм доступ тільки до необхідної інформації і функцій. Це може включати використання паролів, біометричних методів або двофакторної аутентифікації для перевірки ідентичності користувачів.

5. Моніторинг та аудит. Вимога до моніторингу та аудиту означає, що система має збирати, аналізувати та зберігати дані про події та дії, що відбуваються в системі. Це дозволяє виявляти потенційні загрози, проводити аналіз вразливостей і забезпечувати звітність щодо безпеки системи.

6. Захист від вторгнень. Вимога до захисту від вторгнень передбачає, щоб система виявляла та захищала себе від несанкціонованого доступу, вторгнень або зловживань. Це може включати встановлення системи виявлення вторгнень (Intrusion Detection System) та системи попередження про вторгнення (Intrusion Prevention System) для моніторингу та блокування підозрілих активностей.

7. Захист від витоку даних. Вимога до захисту від витоку даних ставить завдання забезпечити, щоб конфіденційна інформація не потрапляла

в руки несанкціонованих осіб. Це може включати використання механізмів шифрування для захисту даних під час зберігання та передачі, контроль доступу до конфіденційної інформації та встановлення політик та процедур безпеки для управління даними.

8. Управління ризиками. Вимога до управління ризиками включає визначення та оцінку потенційних загроз, вразливостей та можливих наслідків для системи. Це передбачає розробку стратегій та процедур управління ризиками, проведення оцінки ризиків, виконання аудиту безпеки та впровадження заходів з мінімізації ризиків.

9. Спротив стихійним лихам. Вимога до спротиву стихійним лихам передбачає, щоб система була захищена від можливих впливів негативних природних явищ, таких як пожежі, повені, землетруси або інші природні катастрофи. Це включає розробку планів надійності, резервне копіювання даних, розташування серверів у безпечних місцях та забезпечення ефективного резервного живлення.

10. Відповідність до регуляторних вимог. Вимога до відповідності до регуляторних вимог передбачає, щоб система відповідала вимогам законодавства та стандартів щодо захисту інформації. Це може включати виконання вимог GDPR (Загального регламенту про захист персональних даних), встановлення політик та процедур з охорони персональних даних, аудит безпеки та забезпечення вимогів щодо зберігання і обробки даних.

11. Антивірусний захист. Вимога до антивірусного захисту передбачає, щоб система була захищена від шкідливих програм, таких як віруси, троянські коні, черв'яки та інші види шкідливого програмного забезпечення. Це може включати встановлення антивірусного програмного забезпечення, регулярне оновлення баз даних вірусних сигнатур та контроль запуску виконуваних файлів.

12. Фізична безпека. Вимога до фізичної безпеки передбачає захист інформаційних ресурсів від несанкціонованого фізичного доступу. Це може включати застосування систем контролю доступу, використання

відеоспостереження, захищену фізичну інфраструктуру та інші заходи, що забезпечують фізичну безпеку обладнання та приміщень.

13. Захист мережі. Вимога до захисту мережі передбачає, щоб система була захищена від несанкціонованого доступу до мережевих ресурсів та зловживання. Це може включати використання брандмауерів, інтрудер-детекторів, віртуальних приватних мереж (VPN), захищених протоколів зв'язку та інших технологій, що забезпечують безпеку мережі.

14. Управління доступом. Вимога до управління доступом ставить завдання забезпечити, щоб користувачі мали лише той рівень доступу до інформації і функцій системи, який необхідний для виконання їхніх обов'язків. Це може включати встановлення різних рівнів доступу, автоматизовану систему керування правами доступу, двофакторну аутентифікацію та аудит доступу.

15. Безпека мобільних пристроїв. Вимога до безпеки мобільних пристроїв передбачає захист інформації, яка зберігається на мобільних телефонах, планшетах та інших пристроях. Це може включати встановлення паролів, використання шифрування даних, віддалене видалення даних у випадку втрати або крадіжки пристрою, контроль доступу до мобільних додатків та інші заходи, що забезпечують безпеку мобільних пристроїв.

16. Захист від соціальної інженерії. Вимога до захисту від соціальної інженерії передбачає забезпечення, щоб користувачі були усвідомлені щодо можливих загроз та не надавали недозволений доступ до системи через маніпуляції або обман. Це може включати проведення навчання та освіти щодо кібербезпеки, встановлення політик безпеки, обмежень на розголошення конфіденційної інформації та інші заходи, спрямовані на підвищення обізнаності користувачів.

17. Захист від витоку інформації через периферійні пристрої. Вимога до захисту від витоку інформації через периферійні пристрої передбачає захист системи від можливого витоку конфіденційної інформації через зовнішні пристрої, такі як USB-накопичувачі, зовнішні жорсткі диски або принтери.

Це може включати встановлення політик та технологій контролю використання периферійних пристроїв, шифрування даних на таких пристроях або фізичне обмеження доступу до них.

18. Захист від атак з використанням вразливостей програмного забезпечення. Вимога до захисту від атак з використанням вразливостей програмного забезпечення передбачає, щоб система була захищена від можливих атак, що використовують підозрілі коди або вразливості в програмному забезпеченні. Це може включати встановлення систем оновлення та патчів, перевірку безпеки коду, використання механізмів виявлення та захисту від шкідливих кодів.

19. Забезпечення безпеки в хмарних сервісах. Вимога до безпеки в хмарних сервісах передбачає, щоб система мала відповідні заходи безпеки при використанні хмарних сервісів для зберігання, обробки та обміну даними. Це може включати шифрування даних перед їх передачею в хмару, перевірку безпеки постачальників хмарних сервісів, контроль доступу до хмарних ресурсів та резервне копіювання даних.

20. Захист від фізичного знищення інформації. Вимога до захисту від фізичного знищення інформації передбачає забезпечення, щоб система була захищена від можливого фізичного пошкодження або знищення даних. Це може включати використання резервного копіювання та архівування даних, розташування серверних приміщень у безпечних місцях, встановлення протиускладнених систем охорони та захисту від пожеж та витоку води.

21. Захист від внутрішніх загроз. Вимога до захисту від внутрішніх загроз передбачає, щоб система була захищена від можливих загроз, які виникають зсередини самої організації. Це може включати контроль доступу до системи, моніторинг активності користувачів, використання систем детекції некоректної поведінки та викривлення загроз.

22. Захист від фізичних атак. Вимога до захисту від фізичних атак передбачає, щоб система була захищена від можливих фізичних спроб незаконного доступу до обладнання або інфраструктури. Це може включати

встановлення фізичних бар'єрів, систем виявлення вторгнень, відеоспостереження та охоронних послуг.

23. Захист інформації під час передачі. Вимога до захисту інформації під час передачі передбачає забезпечення безпеки даних під час їх передачі по мережі. Це може включати використання протоколів шифрування, віртуальних приватних мереж (VPN), захищених каналів зв'язку та інших технологій, що забезпечують конфіденційність та цілісність даних під час передачі.

24. Захист від атак на інфраструктуру. Вимога до захисту від атак на інфраструктуру передбачає забезпечення безпеки самих компонентів та систем, що використовуються для зберігання та обробки інформації. Це може включати встановлення захисних механізмів на рівні мережі, серверів, баз даних та інших компонентів, що забезпечують надійність та безпеку інфраструктури.

25. Резервне копіювання та відновлення даних. Вимога до резервного копіювання та відновлення даних передбачає забезпечення наявності резервних копій інформації та можливості їх відновлення в разі втрати або пошкодження даних. Це може включати регулярне створення резервних копій, тестування процедур відновлення та забезпечення безпеки резервних копій.

Це лише кілька додаткових прикладів вимог до системи захисту інформації. Конкретні вимоги будуть залежати від потреб та особливостей конкретної організації та її інформаційних активів.

Всі ці вимоги та фактори разом формують зрозумілу і чітку картину того, що очікується від системи захисту інформації, які проблеми вона повинна вирішити, і яким чином це повинно бути зроблено. За допомогою цього аналізу ми можемо розробити ефективну стратегію кібербезпеки, яка відповідає потребам організації і допомагає забезпечити захист її найцінніших активів - інформації.

1.2 Аналіз можливих рішень поставленого завдання

У сучасному цифровому світі безпека інформації є важливим аспектом для бізнесу. Особливо увагу приділяється захисту веб-додатків, оскільки вони є основою для багатьох бізнес-процесів. Зловмисники намагаються використовувати вразливості веб-додатків, щоб отримати несанкціонований доступ до цінної інформації або завдати шкоди компанії.

У нашій кваліфікаційній роботі ми зосередимося на аналізі можливих рішень для забезпечення безпеки веб-додатків. Ми детально розглянемо різні технології та інструменти, які можуть бути використані для виявлення та запобігання вразливостям веб-додатків.

Проблема безпеки є комплексною, існує багато потенційних загроз та ризиків, які потрібно враховувати. Але в цій роботі ми сконцентруємося саме на вразливостях веб-додатків, які можна виявити та оцінити за допомогою сканерів вразливостей.

Для цього ми проведемо докладний аналіз різних сканерів, зокрема Acunetix, Burp Suite Enterprise Edition, Nessus Professional та OpenVAS. Ми вивчимо їх функціональність, можливості та обмеження, щоб зрозуміти, наскільки ефективними вони можуть бути для виявлення та розв'язання проблем безпеки веб-додатків у бізнес-середовищі.

Крім того, аналізу підлягають і різноманітні рішення фаерволів, таких як Cloudflare, AWS Shield, AstraSecurity Firewall. Це дозволяє визначити найбільш відповідний WAF, який забезпечить ефективний контроль і фільтрацію мережевого трафіку для захисту веб-додатків та інформаційних ресурсів бізнесу. Принцип роботи WAF описано в [2]. Вибір оптимального WAF залежить від потреб компанії, типу додатків та інфраструктури, а також вимог до безпеки та доступності.

Один з можливих підходів - використання комерційних сканерів безпеки. Комерційні сканери безпеки є платними продуктами, які надають широкий набір функціональності для виявлення вразливостей і аналізу

безпеки системи. Вони можуть автоматизувати процес сканування, перевірку відповідності до стандартів безпеки та генерацію детальних звітів. Приклади комерційних сканерів безпеки включають Acunetix, Qualys, Nessus.

За бюджетними обмеженнями або для менш складних систем можна розглянути використання безкоштовних сканерів безпеки. Безкоштовні сканери безпеки, такі як OpenVAS, Nikto, Vega та інші, можуть надати базовий функціонал для виявлення загроз та перевірки безпеки системи.

Для забезпечення повноцінного аналізу можливих рішень, варто врахувати інші аспекти, такі як ідентифікація та автентифікація користувачів, шифрування даних, постійний моніторинг та оновлення, аудит безпеки, навчання користувачів та інші. Відповідний вибір рішень залежить від особливостей системи, вимог безпеки та бюджету проекту.

1.3 Аналіз узагальненої структури системи захисту інформації

Аналіз узагальненої структури системи захисту інформації є важливим етапом в процесі забезпечення безпеки інформаційних систем. У цьому розділі роботи буде проведено детальний аналіз та розгляд основних аспектів розробки структури системи захисту інформації з метою забезпечення надійного та ефективного захисту інформаційних активів організації.

Один із найважливіших аспектів узагальненої структури системи захисту інформації - це аналіз потреб безпеки, специфічних для бізнесу. Кожна організація має свої унікальні вимоги та потреби, пов'язані з безпекою її інформаційних активів. Детальний аналіз цих потреб дозволяє встановити пріоритети та розробити стратегію розвитку системи захисту інформації, яка оптимально задовольнятиме потреби організації.

Розпізнавання потенційних загроз та вразливостей - ще один важливий аспект аналізу потреб безпеки бізнесу який описаний в [3]. Це передбачає ідентифікацію можливих загроз, які можуть вплинути на систему, таких як хакерські атаки, внутрішнє шпигунство або природні катастрофи, а також

визначення вразливостей, які можуть бути використані загрозами для незаконного доступу до інформації або недоступності системи. Наприклад, підприємство, що займається електронною комерцією, може бути під загрозою кібератак, спрямованих на крадіжку конфіденційної інформації про клієнтів або зламу системи оплати.

Оцінка ризиків пов'язаних з інформаційними активами організації - це ключовий етап аналізу потреб безпеки бізнесу. Вона полягає в оцінці ймовірності та наслідків виникнення загроз, що допомагає визначити рівень ризику та встановити пріоритети в заходах безпеки. Організація може використовувати методи оцінки ризиків, такі як аналіз ймовірності та впливу, для визначення наслідків можливих загроз та їх потенційного впливу на бізнес.

Загалом, аналіз потреб безпеки бізнесу визначає основні цілі, вимоги, загрози та ризики, що впливають на безпеку інформаційних активів. Цей аналіз надає організації необхідні інформаційні засоби для прийняття обґрунтованих рішень щодо розробки системи захисту інформації, яка відповідає її потребам та забезпечує надійний рівень безпеки. Наприклад, на підставі аналізу потреб безпеки, банк може визначити вимоги до захисту клієнтських фінансових даних та встановити механізми контролю доступу, шифрування та моніторингу для їх захисту. [3]

Таким чином, аналіз потреб безпеки бізнесу визначає фундаментальні основи розробки системи захисту інформації. Він дозволяє встановити пріоритети, розробити стратегію і визначити необхідні заходи безпеки, що забезпечать ефективний та надійний захист інформаційних активів організації.

Для середньо статистичного бізнесу аналіз потреб безпеки може включати такі аспекти:

1. Визначення цілей безпеки: Наприклад, цілі можуть включати забезпечення конфіденційності клієнтських даних, запобігання втраті даних, забезпечення цілісності операцій та захист від кібератак.

2. Вимоги до безпеки: Вивчення законодавчих вимог, стандартів і регуляторних вимог, які стосуються безпеки даних та конфіденційності. Наприклад, вимоги щодо захисту персональних даних відповідно до Загального регламенту про захист персональних даних (GDPR).

3. Розпізнавання загроз та вразливостей: Аналіз ідентифікації потенційних загроз, які можуть впливати на бізнес, таких як фішинг-атаки, віруси, зловживання привілегіями співробітників або фізичні ризики, пов'язані зі зламом приміщень.

4. Оцінка ризиків: Визначення ймовірності виникнення загроз та наслідків, які вони можуть мати на бізнес. Наприклад, оцінка вірогідності імовірних кібератак та потенційних фінансових втрат, які можуть виникнути в результаті таких атак.

5. Визначення заходів безпеки: Розроблення плану заходів безпеки, які допоможуть зменшити виявлені ризики та захистити інформаційні активи. Наприклад, встановлення ефективних систем моніторингу та виявлення загроз, використання шифрування для захисту даних, навчання співробітників правилам кібербезпеки.

6. Бюджетні обмеження: Врахування бюджетних обмежень та ресурсів компанії при визначенні заходів безпеки. Це допомагає забезпечити реалістичну реалізацію запланованих заходів безпеки.

Наприклад, середньо статистична компанія може визначити свої цілі безпеки, такі як захист клієнтських даних та забезпечення цілісності фінансових операцій. Вимоги до безпеки можуть включати виконання вимог GDPR щодо захисту персональних даних. Аналіз загроз та вразливостей може виявити потенційні загрози, наприклад, кібератаки або недбале ставлення співробітників до захисту даних. Оцінка ризиків допоможе визначити, наскільки серйозними є ці загрози та які можуть бути фінансові втрати. На основі цього аналізу будуть прийняті конкретні заходи безпеки, такі як установка ефективного фірмового м'якого WAF для захисту

веб-додатків або організація тренінгів з кібербезпеки для співробітників. Усі ці дії будуть проводитись в рамках бюджетних обмежень і ресурсів компанії.

Далі в розділі будуть розглянуті компоненти системи захисту інформації. Для кожного компонента буде проведено детальний аналіз його функцій, можливостей та взаємодії з іншими компонентами системи. Визначення компонентів допомагає встановити необхідні технології, інструменти та методи захисту для реалізації цих компонентів.

У розділі будуть розглянуті компоненти системи захисту інформації, які є важливими складовими частинами забезпечення безпеки інформаційних активів організації. Кожен компонент буде піддано детальному аналізу його функцій, можливостей та взаємодії з іншими компонентами системи.

Перший компонент, який буде розглянутий, - це система ідентифікації та аутентифікації. Цей компонент відповідає за перевірку ідентичності користувачів і надання їм доступу до системи. В рамках аналізу будуть визначені потрібні функції, такі як багаторівнева аутентифікація, керування користувачами та доступом, а також взаємодія з іншими компонентами, наприклад, з системою керування доступом.

У рамках системи ідентифікації та аутентифікації можуть бути використані різні методи та технології забезпечення безпеки доступу до системи. Ось декілька прикладів, що можуть бути використані:

1. Багаторівнева аутентифікація: Цей метод передбачає використання декількох шарів аутентифікації для перевірки ідентичності користувача. Наприклад, це може включати використання паролів, одноразових кодів, біометричних даних або фізичних токенів. Така комбінація різних методів забезпечує вищий рівень безпеки.

2. Керування користувачами та доступом: Цей компонент системи відповідає за управління користувачами та контроль доступу до різних ресурсів системи. Наприклад, це може включати створення та управління користувачними обліковими записами, надання ролей та прав доступу, налаштування політик паролів та аудиту активності користувачів.

3. Двофакторна аутентифікація: Цей метод вимагає введення двох незалежних факторів аутентифікації для підтвердження ідентичності користувача. Наприклад, це може бути поєднання паролю та одноразового коду, який надсилається на мобільний пристрій користувача.

4. Система одноразових паролів: Цей метод використовується для забезпечення безпеки під час входу в систему. Кожен пароль може бути використаний лише один раз, і після використання він стає недійсним. Це дозволяє запобігти підбору або викраденню паролів.

5. Шифрування трафіку: Для забезпечення безпеки під час передачі даних між користувачем і системою можна використовувати шифрування трафіку. Наприклад, застосування протоколу HTTPS дозволяє шифрувати комунікацію між веб-браузером та сервером, що забезпечує конфіденційність даних під час їх передачі.

Наступним компонентом для аналізу буде система моніторингу та виявлення загроз. Цей компонент відповідає за постійне спостереження за системою та виявлення потенційних загроз та атак. В рамках аналізу будуть розглянуті функції, такі як моніторинг мережі, виявлення незвичайних активностей, аналіз журналів подій та сповіщення про можливі загрози. Також буде встановлена взаємодія з іншими компонентами, наприклад, з системою виявлення вторгнень.

У рамках системи моніторингу та виявлення загроз можуть бути використані різні інструменти та методи для постійного спостереження за системою та виявлення потенційних загроз та атак. Ось декілька прикладів таких інструментів:

1. Системи моніторингу мережі: Ці системи дозволяють контролювати мережевий трафік та виявляти незвичайні або підозрілі активності. Вони можуть аналізувати пакети даних, відстежувати мережеві з'єднання та реєструвати виявлені аномалії, що можуть вказувати на потенційні загрози.

2. Системи аналізу журналів подій: Ці системи збирають та аналізують журнали подій з різних компонентів системи, таких як сервери, мережеві

пристрої, додатки тощо. Вони виявляють незвичайні або підозрілі активності, які можуть свідчити про можливі загрози або атаки.

3. Системи виявлення аномалій: Ці системи використовують алгоритми та моделі для виявлення незвичайних патернів або аномалій в системі. Вони аналізують поведінку системи та користувачів, і якщо виявляють незвичайні або підозрілі активності, генерують сповіщення про можливі загрози.

4. Системи сповіщення про вторгнення: Ці системи спостерігають за спробами вторгнення в систему та виявляють підозрілі або небезпечні дії. Вони можуть використовувати сигнатури атак, евристичні правила або машинне навчання для виявлення вторгнень та сповіщення про них.

5. Системи реагування на інциденти: Ці системи включають процеси та процедури для реагування на виявлені загрози та атаки. Вони можуть включати автоматизовану реакцію, таку як блокування підозрілих IP-адрес або відключення доступу, або вимагати ручного втручання операторів безпеки.

Третій компонент, який буде розглянутий, - це система шифрування даних. Цей компонент забезпечує захист конфіденційності інформації шляхом застосування різних шифрувальних методів. Аналіз цього компонента включатиме вивчення різних методів шифрування, таких як симетричне шифрування та асиметричне шифрування, а також можливостей для захисту передачі даних і збереження шифрованих даних. Взаємодія з іншими компонентами, наприклад, з системою керування ключами, також буде детально розглянута.

У системі шифрування даних можуть бути використані різні методи та алгоритми шифрування для захисту конфіденційності інформації. Ось декілька прикладів таких методів:

1. Симетричне шифрування: Цей метод передбачає використання одного ключа для шифрування та розшифрування даних. Прикладом може бути алгоритм AES (Advanced Encryption Standard), який є одним з найпоширеніших методів симетричного шифрування.

2. Асиметричне шифрування: Цей метод використовує два ключі - публічний та приватний - для шифрування та розшифрування даних. Прикладом може бути алгоритм RSA (Rivest-Shamir-Adleman), який є одним з найпоширеніших методів асиметричного шифрування.

3. Шифрування каналу зв'язку: Цей метод використовується для захисту передачі даних між комунікуючими сторонами. Прикладом може бути протокол SSL/TLS, який забезпечує шифрування трафіку між веб-браузером і веб-сервером під час передачі конфіденційних даних.

4. Шифрування файлів та дисків: Цей метод застосовується для захисту збережених даних на файлових системах або на цілих дисках. Прикладами можуть бути шифрування файлової системи BitLocker для Windows або шифрування диску FileVault для macOS.

5. Шифрування електронної пошти: Цей метод використовується для захисту конфіденційної інформації, яка передається по електронній пошті.

Крім того, розглянуті будуть інші компоненти, такі як система резервного копіювання та відновлення, система контролю доступу, система контролю цілісності даних та система автоматизованого виявлення вразливостей. Аналіз кожного з цих компонентів допоможе визначити їхню роль, функції, можливості та взаємодію з іншими компонентами системи захисту інформації.

Компонент системи резервного копіювання та відновлення відповідає за забезпечення захисту даних шляхом регулярного створення резервних копій і можливості відновлення інформації в разі виникнення непередбачуваних ситуацій. Для цього можуть бути використані такі методи та технології:

1. Резервне копіювання на зовнішні носії: Цей метод включає створення резервних копій даних на зовнішніх носіях, таких як жорсткі диски, магнітні стрічки або USB-накопичувачі. Резервні копії можуть бути зберігані на віддалених місцях для захисту від фізичних пошкоджень або крадіжок.

2. Система контролю доступу відповідає за обмеження доступу до системи інформації лише для авторизованих користувачів.

3. Система контролю цілісності даних відповідає за перевірку цілісності даних та виявлення будь-яких змін або незаконних втручань.

4. Система автоматизованого виявлення вразливостей відповідає за сканування системи та виявлення потенційних вразливостей, що можуть бути використані зловмисниками.

Такий детальний аналіз компонентів системи захисту інформації дозволить встановити необхідні технології, інструменти та методи захисту для реалізації кожного компонента та забезпечити надійний рівень безпеки для інформаційних активів організації.

РОЗДІЛ 2 ТЕОРЕТИЧНА ЧАСТИНА

2.1 Розробка моделі загроз та моделі порушника

У даному розділі буде проведена розробка моделі загроз та моделі порушника для системи захисту інформації. Ці моделі допоможуть визначити потенційні загрози, які можуть вплинути на безпеку системи, а також профіль та характеристики можливих порушників. Розробка цих моделей є важливим етапом проектування безпеки, оскільки дозволяє зрозуміти сценарії атак і використовувати цю інформацію для розробки відповідних заходів захисту описано в [4-5].

Розробка моделі загроз передбачає ідентифікацію та аналіз різних загроз, які можуть вплинути на систему захисту інформації. Це можуть бути зовнішні атаки, такі як хакерські напади або фішинг, або внутрішні загрози, пов'язані з несанкціонованим доступом або недбалістю співробітників. При розробці моделі загроз важливо врахувати специфіку системи та її особливості.

Наприклад, для середнього статистичного бізнесу, загрози можуть включати:

1. Фішинг: Це атака, коли зловмисник намагається отримати конфіденційну інформацію, таку як паролі або банківські реквізити, шляхом вигадливих методів, таких як підробка електронних листів або створення фальшивих веб-сторінок. Прикладом може бути спроба використати фішинговий електронний лист, який видаватиметься за повідомлення від банку, щоб отримати конфіденційну інформацію від співробітників бізнесу.

2. Внутрішній доступ: Це загроза, коли несанкціонована особа або співробітник здійснює неправомірний доступ до конфіденційної інформації. Наприклад, співробітник, який має доступ до бази даних клієнтів, може незаконно отримати доступ до конфіденційної інформації та використовувати її в своїх особистих цілях.

3. Malware (Шкідливий програмний засіб): Це загроза, коли зловмисник використовує шкідливе програмне забезпечення для злому системи або отримання конфіденційної інформації. Прикладом може бути використання вірусу або шкідливого коду, який прихований у прикладних програмах або електронних листах, для отримання доступу до системи та викрадення даних.

Розробка моделі порушника передбачає визначення характеристик і профілю потенційного порушника. Це допомагає зрозуміти мотивацію, наміри та методи, які можуть використовувати порушники для атак на систему. Наприклад, можливі профілі порушників можуть включати:

1. Хакери. Це зловмисники, які мають технічні навички і намагаються проникнути в комп'ютерну систему з метою отримання конфіденційної інформації або здійснення інших шкідливих дій. Вони володіють глибоким розумінням комп'ютерних мереж, операційних систем, програмного забезпечення та криптографії, що дозволяє їм ефективно використовувати різноманітні методи та техніки для злому системи.

Хакери можуть використовувати різні методи для проникнення в систему. Наприклад, вони можуть використовувати вразливості в програмному забезпеченні або операційній системі, атакувати слабкі паролі, використовувати соціальну інженерію, фішингові атаки або зламувати мережеві протоколи. Метою хакерів може бути отримання конфіденційних даних, таких як фінансова інформація, особисті дані, комерційна інформація або доступ до системи для завдання подальших шкідливих дій, таких як поширення шкідливих програм, розкрадання ресурсів або завдання фінансових збитків.

Хакери можуть діяти самостійно або організовуватися в групи, відомі як хакерські колективи або кіберпреступні угруповання. Вони часто використовують складні технології та програмні інструменти, щоб захистити свою ідентичність та залишити мінімальні сліди своїх дій, що ускладнює виявлення та притягнення їх до відповідальності.

Протидія хакерам вимагає комплексного підходу до кібербезпеки, включаючи використання сильних паролів, регулярне оновлення програмного забезпечення, використання захисних механізмів, таких як файрволи та антивірусне програмне забезпечення, та навчання персоналу з питань кібербезпеки. Крім того, важливо проводити регулярний аналіз і аудит безпеки, щоб виявити можливі вразливості та прийняти відповідні заходи для їх усунення.

Незважаючи на зусилля в попередженні та протидії хакерам, кібербезпека залишається постійним викликом, оскільки хакери постійно еволюціонують та вдосконалюють свої методи атак. Тому важливо підтримувати свої системи захищеними, оновлювати навички та знання в галузі кібербезпеки та бути завжди на крок попереду потенційних загроз.

2. Конкуренти. Це організації або особи, які мають подібні бізнес-інтереси або діють в тій самій галузі, і можуть мати мотиви для отримання конфіденційної інформації бізнесу з метою витоку даних або завдання шкоди. Їхні цілі можуть включати отримання переваги на ринку, крадіжку ідей, планів або розробок, а також здійснення конкурентних атак з метою послаблення позицій компанії або завдання фінансових збитків.

Серед способів, якими конкуренти можуть намагатися отримати доступ до конфіденційної інформації, можна відзначити підкуп або найм внутрішніх співробітників, які мають прямий доступ до важливих даних, а також використання шпигунських методів або злому комп'ютерних систем компанії. Конкуренти можуть залучати спеціалістів з кібербезпеки для використання різних методів атак, таких як фішинг, соціальна інженерія, викрадення паролів або використання вразливостей програмного забезпечення.

Для захисту від таких загроз важливо вживати заходи безпеки, як обмеження доступу до конфіденційної інформації лише для необхідних співробітників, використання шифрування даних, контроль за виходом конфіденційної інформації з компанії, а також встановлення систем моніторингу та виявлення незвичайних активностей. Крім того, проведення

навчання та підвищення свідомості серед співробітників щодо кібербезпеки може допомогти виявити можливі загрози та зменшити ризик витоку конфіденційної інформації компанії.

3. Внутрішні порушники. Це співробітники, які мають легальний доступ до системи і ресурсів компанії, але можуть використовувати свої привілеї для незаконних дій або зловживання конфіденційною інформацією. Вони мають внутрішні знання про систему, процедури та потенційні слабкі місця, що може зробити їх особливо небезпечними.

Причини внутрішніх порушень можуть бути різноманітними. Деякі співробітники можуть мати недостатню мотивацію або задоволення від роботи і намагатися скористатися цим для особистої вигоди. Інші можуть мати фінансові проблеми або внутрішні конфлікти, що спонукають їх до незаконних дій. Також можуть виникати ситуації, коли співробітники стають недовірливими до компанії або мають негативне ставлення до управління, що спонукає їх до вчинення порушень.

Внутрішні порушники можуть використовувати свій доступ для викрадення конфіденційної інформації, такої як бізнес-плани, клієнтські дані, технічні розробки або інтелектуальна власність. Вони також можуть зловживати своїми привілеями для внесення змін в систему, розкрадання ресурсів, підробки даних або виконання шкідливих дій, що може призвести до серйозних наслідків для компанії.

Для запобігання внутрішнім порушенням необхідно вживати заходів контролю доступу, таких як розподілення ролей та привілеїв, встановлення політик доступу та моніторинг діяльності співробітників. Важливо проводити навчання з питань етики та свідомості про кібербезпеку, щоб збільшити усвідомлення серед персоналу про ризики порушень та їхні наслідки. Крім того, важливо мати ефективні процедури виявлення та реагування на внутрішні порушення, щоб вчасно виявити та припинити незаконну діяльність співробітників.

Це лише деякі приклади потенційних загроз та типів порушників, які можуть бути враховані при розробці моделі загроз та моделі порушника. При розробці цих моделей важливо враховувати унікальні потреби та характеристики організації, а також актуальні тренди в кібербезпеці.

2.2 Обґрунтування вибору політики та засобів безпеки

Обґрунтування вибору політики та засобів безпеки є важливим етапом розробки системи захисту інформації. На цьому етапі проводиться аналіз потреб організації, враховуючи специфіку її діяльності, цілей та вимог до безпеки. Вибір політики та засобів безпеки повинен бути обґрунтованим, забезпечуючи високий рівень захисту інформації організації від потенційних загроз.

Політика безпеки визначає набір правил, процедур та підходів, які регулюють захист інформації. При обґрунтуванні вибору політики безпеки необхідно враховувати особливості організації, її потреби, цілі та обмеження. Наприклад, для фінансової установи може бути важливим забезпечення конфіденційності фінансової інформації клієнтів, тоді як для науково-дослідної компанії пріоритетом може бути забезпечення цілісності та доступності дослідницьких даних.

При обґрунтуванні вибору політики безпеки також необхідно враховувати вимоги законодавства та регулятивних організацій у сфері кібербезпеки. Наприклад, у деяких галузях, таких як фінанси або охорона здоров'я, існують обов'язкові стандарти безпеки, які необхідно виконувати. Обґрунтування вибору політики безпеки повинно враховувати ці вимоги та встановлювати відповідні заходи для виконання нормативних вимог.

Одним із факторів, які впливають на вибір політики безпеки, є оцінка ризиків. На основі аналізу загроз, вразливостей та потенційних наслідків, проводиться оцінка ризиків, що дозволяє визначити, які загрози є найбільш ймовірними та найшкідливішими для організації. Обґрунтування вибору

політики безпеки повинно враховувати ці ризики і пропонувати відповідні заходи для зменшення ризиків до прийнятного рівня.

Засоби безпеки включають різноманітні технології, програмне забезпечення та методи захисту інформації. При обґрунтуванні вибору засобів безпеки слід враховувати потреби організації та вимоги до безпеки. Наприклад, можуть використовуватися такі засоби, як файрволи, системи виявлення вторгнень, антивірусне програмне забезпечення, системи шифрування, системи резервного копіювання та відновлення, системи керування доступом та багато інших.

Обґрунтування вибору засобів безпеки включає аналіз їхніх функцій, можливостей, ефективності та взаємодії з іншими компонентами системи захисту інформації. Наприклад, при виборі файрвола можуть бути враховані його можливості фільтрації трафіку, налаштування політик доступу та моніторингу мережі. При виборі системи виявлення вторгнень можуть бути враховані її можливості аналізу журналів подій, виявлення незвичайних активностей та сповіщення про можливі загрози.

Таким чином, обґрунтування вибору політики та засобів безпеки включає ретельний аналіз потреб організації, оцінку ризиків, врахування вимог законодавства та регулятивних вимог, а також вибір відповідних засобів безпеки для забезпечення ефективного захисту інформації.

2.3 Огляд та порівняльний аналіз сканерів безпеки

Acunetix є потужним автоматичним сканером веб-застосунків, призначеним для виявлення та оцінки загроз безпеки. Він має широкий спектр функціональності, що дозволяє знайти різноманітні типи вразливостей, такі як SQL-ін'єкції, міжсайтовий скриптінг (XSS), міжсайтовий запрос (CSRF) та багато інших описано в [6].

Однією з переваг Acunetix є його висока швидкість сканування, що дозволяє швидко провести аналіз веб-додатків на вразливості. Крім того, він

інтегрується з системами керування інцидентами, що спрощує процес виявлення та реагування на загрози безпеки. Також варто відзначити зручний інтерфейс та візуалізацію результатів, що полегшує розуміння виявлених проблем.

Проте, варто враховувати деякі недоліки Acunetix. Вартість цього сканера може бути високою для деяких користувачів, особливо для менших бізнесів з обмеженим бюджетом. Крім того, варто зазначити, що Acunetix не виявляє деякі типи уразливостей на рівні мережі, що може бути важливим для комплексного аналізу безпеки.

У підсумку, Acunetix є потужним і корисним інструментом для виявлення вразливостей веб-застосунків. Його швидкість сканування, інтеграція з системами керування інцидентами та зручний інтерфейс роблять його популярним серед професіоналів з інформаційної безпеки. Однак, необхідно враховувати вартість та обмеження виявлення уразливостей на рівні мережі при виборі та використанні цього сканера.

Burp Suite Enterprise Edition - це розширене рішення для тестування безпеки веб-застосунків, яке поєднує автоматичне та ручне тестування. Він надає повний контроль над процесом сканування, дозволяючи виконувати детальні перевірки та налаштування. Крім того, Burp Suite Enterprise Edition інтегрується з іншими інструментами безпеки, що сприяє комплексному підходу до аналізу вразливостей веб-застосунків описано в [7].

Серед переваг Burp Suite Enterprise Edition варто виділити високий рівень деталізації результатів. Він надає змогу отримувати докладну інформацію про виявлені проблеми та допомагає зрозуміти їх важливість та потенційні наслідки для безпеки системи. Крім того, завдяки широкому спектру функцій, Burp Suite Enterprise Edition може задовольнити потреби професіоналів з інформаційної безпеки.

Проте, варто зазначити, що Burp Suite Enterprise Edition має вищий рівень складності налаштування та використання порівняно з іншими сканерами. Це може вимагати додаткових знань та навичок для ефективного

використання всіх можливостей цього інструменту. Крім того, вартість Burp Suite Enterprise Edition може бути високою для деяких користувачів, особливо для менших бізнесів з обмеженим бюджетом.

У підсумку, Burp Suite Enterprise Edition є потужним та розширеним рішенням для тестування безпеки веб-застосунків. Високий рівень контролю над процесом сканування, інтеграція з іншими інструментами безпеки та деталізація результатів роблять його популярним серед професіоналів з інформаційної безпеки. Проте, варто враховувати складність налаштування та високу вартість при розгляді вибору цього інструменту для конкретного бізнесу.

Nessus Professional - це один з найбільш відомих сканерів безпеки, який надає широкий спектр функцій для оцінки уразливостей в мережі та веб-застосунках. Він є потужним інструментом для виявлення різних типів уразливостей, включаючи мережеві проблеми, уразливості операційних систем та уразливості веб-додатків. Nessus Professional працює на різних платформах та операційних системах, що робить його доступним для широкого кола користувачів [8].

Окрім того, для малого та середнього бізнесу, які не мають великої кількості інфраструктури, існує варіант Nessus Essentials. Nessus Essentials дозволяє безкоштовно сканувати до 16 IP-адрес, що робить його корисним і доступним рішенням для бізнесів з обмеженими ресурсами. Це дозволяє компаніям з меншими мережами та складністю інфраструктури отримати доступ до потужних функцій сканування безпеки без великих витрат.

Переваги Nessus Professional включають широкий спектр виявлення вразливостей, високий рівень гнучкості та налаштування, а також інтеграцію з різними системами керування інцидентами. Це дозволяє користувачам налаштовувати сканування з урахуванням їхніх конкретних потреб та вимог безпеки. Проте, використання Nessus Professional вимагає певного рівня знань та досвіду для оптимального використання, і вартість може бути високою для деяких користувачів, особливо для малих бізнесів з обмеженим бюджетом.

Загалом, Nessus Professional та Nessus Essentials є ефективними рішеннями для сканування та виявлення уразливостей в мережі та веб-застосунках. Вони надають користувачам засоби для забезпечення безпеки своєї інфраструктури та захисту від потенційних загроз. Залежно від розміру бізнесу та його потреб в безпеці, компанії можуть вибрати підходящий варіант - від платної версії Nessus Professional до безкоштовної Nessus Essentials для малого бізнесу з обмеженими ресурсами.

OpenVAS є популярним відкритим сканером безпеки, спрямованим на виявлення мережевих уразливостей. Його основна перевага полягає в тому, що він є безкоштовним та має відкритий вихідний код, що дозволяє користувачам перевірити та налаштувати його функціонал за своїми потребами описано в [9].

OpenVAS постійно оновлює свою базу даних уразливостей, що забезпечує користувачам актуальну інформацію про потенційні загрози. Також варто відзначити його гнучкість налаштування, що дозволяє враховувати специфічні особливості мережі та веб-додатків. Більшість налаштувань та опцій доступні користувачам для відрегулювання сканування під їхні потреби.

Однак, важливо враховувати, що OpenVAS може мати менш точне та повне виявлення уразливостей порівняно з комерційними аналогами. Це пов'язано з обмеженістю ресурсів та потужностей, які доступні для розробки та підтримки безкоштовного програмного забезпечення. Також відсутня технічна підтримка та гарантії від розробників OpenVAS, що може бути недоліком для користувачів, які шукають професійну підтримку та відповідальність.

В цілому, OpenVAS є цінним інструментом для виявлення мережевих уразливостей, особливо для користувачів, які шукають безкоштовне та гнучке рішення. Враховуючи його переваги та недоліки, важливо ретельно оцінювати його придатність для конкретних потреб безпеки та враховувати рівень підтримки та відповідальності, який ви очікуєте від розробників.

Ціни на продукти для тестування безпеки, такі як Acunetix, Burp Suite Enterprise Edition, Nessus Professional та OpenVAS, можуть суттєво варіюватися. Acunetix пропонує щорічну підписку вартістю приблизно $3,500 за користувача, що може бути вищим за інші сканери. Burp Suite Enterprise Edition пропонує підписку від €1,999 в рік та додатково €9 за годину сканування. Nessus Professional пропонує підписку вартістю приблизно $2,790 за рік за користувача. OpenVAS - безкоштовна альтернатива, яка доступна для загального використання.

Вибір між цими продуктами залежить від потреб і можливостей організації. Вартість Acunetix, Burp Suite Enterprise Edition і Nessus Professional можуть бути бар'єром для більш обмежених бюджетів, особливо для малих підприємств. OpenVAS, з своєю безкоштовною моделлю, може бути привабливим варіантом для тих, хто не має великого бюджету або хоче спробувати безкоштовну альтернативу.

При виборі продукту для тестування безпеки, важливо враховувати не тільки ціну, але й функціональні можливості, надійність, якість підтримки, інтеграцію з іншими інструментами та вимоги організації. Ретельне порівняння і аналіз цих факторів допоможе визначити оптимальний вибір для конкретних потреб.

Після порівняльного аналізу сканерів безпеки можна зробити наступні висновки:

- Acunetix та Burp Suite Enterprise Edition: Ці сканери веб-застосунків є найкращими виборами для тестування безпеки. Acunetix спеціалізується на виявленні уразливостей, таких як SQL-ін'єкції та XSS, і має інтеграційні можливості з системами керування інцидентами. Burp Suite Enterprise Edition поєднує автоматичне та ручне тестування, надаючи повний контроль над процесом сканування та інтеграцію з іншими інструментами безпеки описано в [14].

- Nessus Professional та OpenVAS: Ці сканери спеціалізуються на виявленні мережевих уразливостей. Nessus Professional працює на різних

операційних системах та виявляє широкий спектр уразливостей, включаючи мережеві, ОС та веб-застосунки. OpenVAS, який є відкритим джерелом, регулярно оновлює свою базу даних уразливостей та надає гнучкість налаштування.

Ці різноманітні сканери забезпечують високий рівень захисту для веб-додатків та мережевих систем. Вибір конкретного сканера залежить від потреб бізнесу, типу застосунків та бюджету. Рекомендується ретельно оцінити характеристики кожного сканера та вибрати той, який найкраще відповідає потребам безпеки вашої компанії. Детальну порівняльну таблицю надано у додатку А.

2.4 Огляд та порівняльний аналіз брандмауерів

Браундмауер або WAF - це засіб захисту, що використовується для захисту веб-додатків від різних видів атак. працює на рівні додатку і аналізує вхідний трафік до веб-додатку. Він застосовує набір правил і фільтрів для виявлення та блокування потенційно шкідливого трафіку. Це дозволяє запобігти атакам, таким як SQL-ін'єкції, міжсайтовий скриптінг (XSS), кросс-сайтовий запрос (CSRF) та іншим що описано в [10].

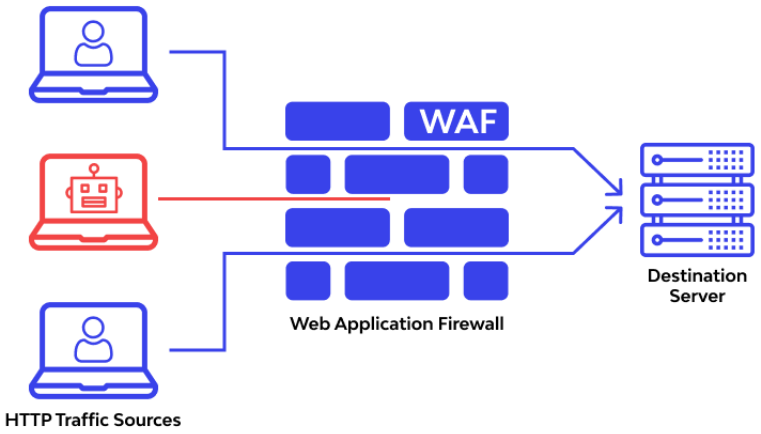

Рисунок 2.1 – Схему роботи WAF

Вхідний трафік до веб-додатку спочатку проходить через WAF. WAF аналізує цей трафік, використовуючи правила та алгоритми, що визначені налаштуваннями. Якщо WAF виявляє потенційно шкідливий трафік, він може блокувати або фільтрувати його, щоб запобігти атакам до веб-додатку.

У розділі буде проведено огляд та порівняльний аналіз різних WAF, їх функціональності, можливостей та обмежень. Це допоможе визначити найбільш підходящий WAF для захисту веб-додатків у бізнес-середовищі.

CloudFlare WAF є потужним рішенням для захисту веб-додатків, яке надає різноманітні функції та можливості для забезпечення безпеки. CloudFlare пропонує два основних тарифні плани для своєї WAF - безкоштовний (Free) та розширений (Pro) плани, які надають різні рівні захисту та функціональності.

CloudFlare WAF (Free) дозволяє отримати базовий рівень захисту для вашого веб-додатку безкоштовно. Він надає наступні функції:

- Захист від DDoS-атак: CloudFlare WAF має вбудований захист від різних типів DDoS-атак, що допомагає утримувати ваш веб-сайт доступним навіть під великим навантаженням.

- Базовий рівень фільтрації трафіку: WAF виявляє та блокує деякі типи вразливостей, такі як SQL-ін'єкції та XSS, забезпечуючи базовий рівень захисту для вашого веб-додатку.

З іншого боку, CloudFlare WAF (Pro) є розширеним тарифним планом, який надає більші можливості та функціональність за певну плату. Професійний план має наступні функції:

- Розширені правила захисту: CloudFlare WAF (Pro) надає розширені можливості налаштування фільтрації трафіку, дозволяючи вам заблокувати специфічні типи атак або вразливостей, які відповідають вашим потребам.

- Захист від роботів і зловмисних ботів: Професійний план WAF має функцію розпізнавання та блокування зловмисних ботів, що допомагає захистити ваш веб-додаток від автоматизованих атак.

- Висока пропускна здатність та швидкість: CloudFlare WAF (Pro) надає високу швидкість та пропускну здатність, що забезпечує ефективний захист вашого веб-додатку навіть при великому навантаженні.

Обираючи між безкоштовним та професійним планом CloudFlare WAF, вам слід враховувати потреби та рівень захисту, необхідний для веб-додатку. Безкоштовний план може бути досить ефективним для малих бізнесів, які шукають базовий рівень захисту, тоді як професійний план може бути більш підходящим для середніх і великих підприємств, які мають вищі вимоги до безпеки та функціональності.

AWS Shield та AWS WAF є двома ключовими компонентами безпеки, які надаються в рамках інфраструктури облікового запису AWS. AWS Shield спеціалізується на захисті від DDoS-атак, тоді як AWS WAF забезпечує захист від веб-атак та небажаного трафіку що описано в [11].

AWS Shield надає захист від DDoS-атак: AWS Shield допомагає захистити вашу інфраструктуру від різних типів DDoS-атак, таких як атаки на рівні мережі або на рівні прикладного програмного забезпечення. Він виявляє та мінімізує вплив цих атак, забезпечуючи неперервну доступність ваших додатків.

AWS WAF надає наступні функції:

- Фільтрація трафіку: AWS WAF дозволяє налаштовувати правила для фільтрації трафіку, що надходить до ваших веб-додатків. Це дозволяє виявляти та блокувати різні типи веб-атак, такі як SQL-ін'єкції, міжсайтовий скриптінг (XSS) та інші, забезпечуючи безпеку вашого додатку.

- Централізоване керування: AWS WAF забезпечує централізоване керування правилами та політиками безпеки для всіх ваших веб-додатків. Ви можете легко налаштовувати, керувати та оновлювати правила захисту для всіх ваших додатків з одного місця.

Інтеграція з AWS-екосистемою: AWS WAF добре інтегрується з іншими послугами та рішеннями AWS, такими як Amazon CloudFront, Amazon API Gateway та Amazon Elastic Load Balancer. Це дозволяє використовувати WAF

разом з іншими службами AWS для створення комплексних стратегій безпеки.

Слід зазначити, що інтеграція AWS Shield та AWS WAF може бути вимогливою через залежність від інфраструктури AWS. Для повноцінного використання цих сервісів потрібно мати наявну інфраструктуру в AWS та налаштувати їх відповідно до потреб вашої системи. Це може вимагати певного рівня експертизи та знань AWS-екосистеми для належної настройки та управління цими сервісами.

Крім того, слід мати на увазі, що ефективність AWS Shield та AWS WAF може залежати від правильного конфігурування та налаштування. Неправильна конфігурація або недостатній рівень захисту можуть знизити ефективність цих сервісів. Тому рекомендується залучати кваліфікованих спеціалістів або консультантів, які мають досвід у налаштуванні та оптимізації AWS Shield та AWS WAF для вашої конкретної інфраструктури та потреб безпеки.

Загалом, AWS Shield та AWS WAF є потужними інструментами безпеки, які забезпечують захист вашої інфраструктури та веб-додатків в середовищі AWS. Проте, перед їх використанням слід ретельно оцінити складність інтеграції, залежність від AWS та належність до ваших потреб безпеки.

AstraSecurity Firewall є потужним інструментом для захисту веб-додатків від різних загроз безпеки. Цей фаєрвол пропонує широкий набір функціональності та захисту, допомагаючи забезпечити безпеку вашого веб-сайту або додатку.

Однією з головних переваг AstraSecurity Firewall є його здатність виявляти та блокувати різноманітні атаки, такі як SQL-ін'єкції, міжсайтовий скриптінг (XSS), крадіжка ідентифікаторів сесій та інші загрози безпеки. Він також надає можливість контролювати доступ до веб-додатків, налаштовувати правила фільтрації трафіку та керувати правами користувачів.

Важливо відзначити, що AstraSecurity Firewall не проксірує весь трафік, але забезпечує захист на рівні веб-додатку. Це означає, що він застосовується безпосередньо до веб-додатку і перехоплює та аналізує трафік, який йде до нього. Це дозволяє фаєрволу виявляти та блокувати шкідливі запити або дії перед тим, як вони досягнуть веб-додатку.

Проте, слід зазначити, що AstraSecurity Firewall не забезпечує захист від DDoS-атак. Його функціональність спрямована на виявлення та блокування загроз безпеки на рівні веб-додатку, а не на мережевому рівні. Якщо вам потрібен захист від DDoS-атак, може бути необхідно розглянути додаткові рішення, такі як мережеві фаєрволи або спеціалізовані сервіси для захисту від DDoS.

В цілому, AstraSecurity Firewall є корисним інструментом для захисту веб-додатків від різних загроз безпеки на рівні веб-додатку. Він надає широкий спектр функціональності та можливостей налаштування, але слід мати на увазі, що його застосування залежить від інфраструктури AWS та може потребувати певного рівня експертизи для належної інтеграції та налаштування.

Нижче наведено порівняння цін на CloudFlare WAF, AWS Shield/WAF та AstraSecurity Firewall:

CloudFlare WAF пропонує кілька планів підписки, включаючи безкоштовний план, Pro план, Business план та Enterprise план. Безкоштовний план доступний для всіх користувачів та надає базовий рівень захисту. Pro план починається зі ставки в $20 на місяць і має розширені функції та додатковий рівень захисту. Business план має розширені можливості та надає придатність для великих підприємств з високими вимогами до безпеки. Enterprise план надає індивідуальні умови та ціни для великих організацій з особливими потребами в захисті.

AWS Shield/WAF також пропонує два рівні підписки: AWS Shield Standard та AWS Shield Advanced. AWS Shield Standard є безкоштовним для всіх користувачів AWS та надає базовий захист від DDoS-атак на рівні

мережі. AWS Shield Advanced є платним планом, який надає розширений рівень захисту та додаткові функції, такі як виявлення та митигація атак на рівні мережі та додатку. Ціни для AWS Shield Advanced починаються від базової ставки в $3,000 на місяць, додаткові витрати можуть бути залежними від обсягу трафіку та потреб користувача.

AstraSecurity Firewall має кілька планів підписки, включаючи Starter план, Pro план, Business план та Custom план. Starter план доступний зі стартовою ціною в $19 на місяць і надає базовий рівень захисту для невеликих бізнесів. Pro план починається з $149 на місяць і надає розширені функції та додаткові рівні захисту. Business план призначений для великих організацій та має початкову ціну в $499 на місяць. Крім того, AstraSecurity Firewall також пропонує Custom план з індивідуальними умовами та цінами для специфічних потреб користувача.

Варто зазначити, що ці ціни є орієнтовними і можуть змінюватися в залежності від обраного плану, обсягу трафіку, додаткових функцій та особливостей користувача. Перед прийняттям рішення про підписку варто ретельно ознайомитися з офіційними веб-сайтами кожного провайдера та отримати актуальну інформацію про ціни та деталі планів підписки.

CloudFlare WAF, AWS Shield/WAF та AstraSecurity Firewall є потужними інструментами для захисту веб-додатків та мережевої інфраструктури. Кожне рішення має свої переваги та особливості, і вибір залежить від конкретних потреб вашого бізнесу. CloudFlare WAF забезпечує ефективний захист на рівні веб-додатку, AWS Shield/WAF надає комплексний захист для інфраструктури AWS, а AstraSecurity Firewall пропонує потужні функції виявлення та блокування загроз безпеки. Враховуйте складність інтеграції та залежність від інфраструктури при прийнятті рішення. Детальну порівняльну таблицю надано у додатку Б.

2.5 Проектування системи захисту інформації

Система захисту інформації для середнього бізнесу повинна бути розроблена з урахуванням конкретних потреб та характеристик організації. При проектуванні системи захисту інформації, необхідно враховувати різні аспекти, такі як контроль доступу, виявлення і реагування на загрози, шифрування даних, резервне копіювання та відновлення, а також застосування захисного фаєрволу.

Один із ключових компонентів системи захисту інформації - це сканери вразливостей. Сканери вразливостей, такі як Acunetix, Burp Suite Enterprise Edition, Nessus Professional та OpenVAS, використовуються для ідентифікації потенційних вразливостей у системі. Кожен з цих сканерів має свої особливості та можливості.

Ці сканери вразливостей є потужними інструментами для аналізу системи на наявність потенційних уразливостей. Кожен з них має свої переваги та можливості, які можуть бути використані в залежності від конкретних потреб і вимог організації.

Крім сканерів вразливостей, важливим елементом системи захисту інформації є веб-застосунки захисту (WAF). Прикладами WAF можуть бути такі рішення, як Cloudflare, AWS Shield та AstraSecurity Firewall. WAF використовується для виявлення та блокування шкідливого трафіку, захисту веб-додатків від атак та забезпечення цілісності та конфіденційності даних. Кожен з цих WAF має свої особливості та можливості, які можуть бути пристосовані до конкретних потреб організації.

Ці рішення, такі як Cloudflare, AWS Shield та AstraSecurity Firewall, надають комплексний захист веб-додатків та мережі, забезпечуючи фільтрацію, захист від DDoS-атак, контроль доступу та виявлення загроз. Кожне з цих рішень має свої унікальні функції та можливості, які можуть бути використані в залежності від потреб та вимог організації.

Проектування системи захисту інформації передбачає вибір та налаштування відповідних компонентів, враховуючи потреби, бюджет та рівень безпеки організації. Наприклад, можна розглянути використання комбінації сканерів вразливостей та WAF для забезпечення постійного моніторингу та захисту системи.

У кінцевому результаті, проектування системи захисту інформації має на меті створення цілісної і надійної інфраструктури безпеки, яка відповідає потребам та вимогам середнього бізнесу.

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 Вибір тестового середовища: OWASP Juice Shop

Для проведення практичної частини дослідження ми вирішили використовувати OWASP Juice Shop. OWASP Juice Shop є відкритим джерелом інтернет-магазину, спеціально розробленим з метою виявлення та навчання уразливостей веб-застосунків. Цей проект реалізований згідно з рекомендаціями OWASP Top Ten Project описано в [12], що включає в себе десять найбільш критичних уразливостей веб-застосунків.

OWASP Juice Shop підходить для тестування безпеки, оскільки він містить численні уразливості, що дозволяють емулювати реальні загрози безпеки та атаки на веб-застосінки. Завдяки різному рівню складності уразливостей, OWASP Juice Shop може бути використаний для оцінки здатності сканерів безпеки виявляти та реагувати на різні типи загроз описано в [13].

Для встановлення та налаштування OWASP Juice Shop у тестовому середовищі, використовуємо Docker - платформу для розробки, розгортання та управління контейнерів. Docker дозволяє легко створювати, розгортати та управляти ізольованими контейнерами з застосунками та їх залежностями, що спрощує процес тестування.

3.2 Результати тестування сканерів вразливостей

Acunetix. Результати сканування OWASP Juice Shop за допомогою Acunetix виявили ряд уразливостей різного ступеня серйозності. Серед них два випадки SQL-ін'єкцій з високим рівнем серйозності та декілька інших уразливостей, таких як помилки застосунку, вразливі JavaScript-бібліотеки, проблеми з безпекою налаштування файли cookie та відсутність заголовка X-Frame-Options, що стосуються Clickjacking. Ці уразливості можуть мати від низького до середнього ступеня серйозності.

Додатково, Acunetix виявив ряд інформаційних уразливостей, які можуть вказувати на можливі проблеми з безпекою та потребу в подальших дослідженнях. Серед них – можливі атаки Cross-Site Scripting (XSS), відсутність заголовка Content Security Policy (CSP) та дисклозура внутрішньої IP-адреси. Окрім того, було виявлено, що для Juice Shop використовується зворотній проксі-сервер та веб-застосунок має файрвол. Ці результати демонструють здатність Acunetix виявляти широкий спектр уразливостей, що можуть стосуватися різних аспектів безпеки веб-застосунків.

Таблиця 3.1 – Список знайдених вразливостей Acunetix

№	Severity	Vulnerability	Score Board
1	High	SQL injection	Так
2	High	SQL injection	Так
3	Medium	Application error messages	Так
4	Low	Vulnerable JavaScript libraries	
5	Low	Clickjacking: X-Frame-Options header	
6	Low	Cookies with missing, inconsistent or contradictory properties	
7	Low	Cookies without HttpOnly flag set	
8	Low	Cookies without Secure flag set	
9	Low	HTTP Strict Transport Security (HSTS) not implemented	
10	Informational	Unrestricted access to Prometheus Metrics	
11	Informational	(Possible) Cross site scripting	Так
12	Informational	(Possible) Cross site scripting	

13	Informational	(Possible) Cross site scripting	
14	Informational	(Possible) Cross site scripting	
15	Informational	(Possible) Cross site scripting	
16	Informational	(Possible) Cross site scripting	
17	Informational	(Possible) Cross site scripting	
18	Informational	(Possible) Cross site scripting	
19	Informational	(Possible) Cross site scripting	
20	Informational	Access-Control-Allow-Origin header with wildcard (*) value	
21	Informational	Content Security Policy (CSP) not implemented	
21	Informational	Internal IP address disclosure	
21	Informational	Permissions-Policy header not implemented	
21	Informational	Reverse proxy detected	
21	Informational	Web Application Firewall detected	

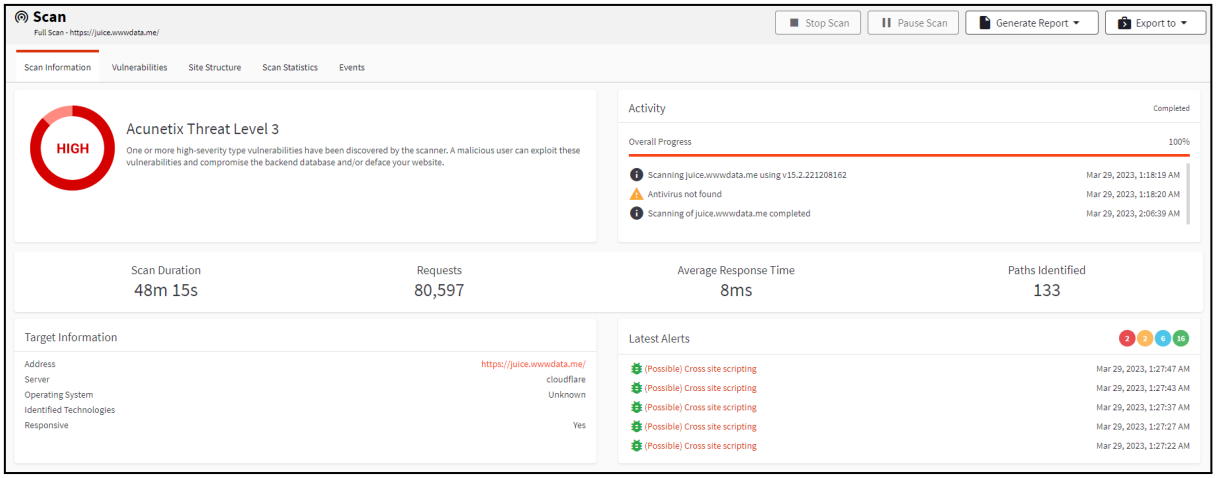

Рисунок 3.1 – Скріншот результату сканування Acunetix

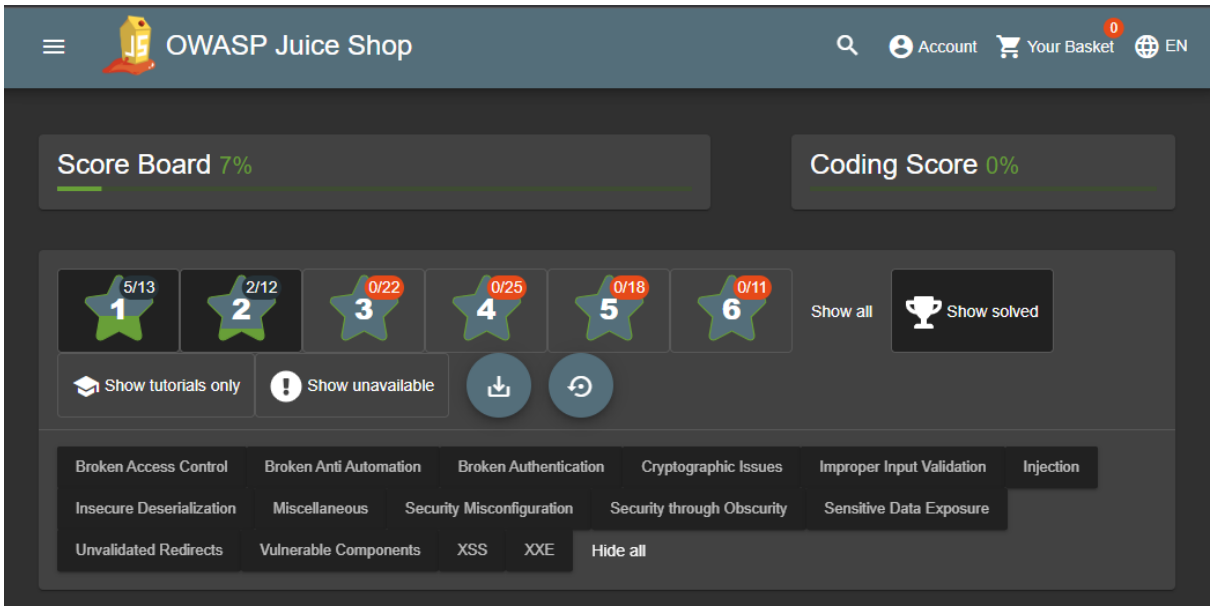

Рисунок 3.2 – Автоматичне виявлення знайдених вразливостей Acunetix

Burp Suite Enterprise Edition. Під час сканування OWASP Juice Shop за допомогою Burp Suite Enterprise Edition було виявлено ряд вразливостей різного рівня серйозності. Серед них виявлені декілька вразливостей низького рівня, таких як не використання строгого транспортного захисту (Strict Transport Security), відкрите перенаправлення, уразливі JavaScript-залежності та DOM-засноване відкрите перенаправлення.

Також була знайдена вразливість середнього рівня - міжсайтовий запити з підробкою (Cross-site request forgery). Окрім цього, сканер Burp Suite виявив декілька інформаційних повідомлень, які можуть бути корисними для розуміння додаткових аспектів безпеки веб-застосунків, таких як витік приватних IP-адрес, наявність файлу robots.txt та інше. Загалом, Burp Suite Enterprise Edition успішно ідентифікував ключові вразливості OWASP Juice Shop, надаючи корисний аналіз безпеки веб-застосунку.

Таблиця 3.2 – Список знайдених вразливостей Burp Suite Enterprise Edition

№	Severity	Vulnerability	Score Board
1	Low	Strict transport security not enforced	
2	Low	Open redirection (reflected)	Так
3	Medium	Cross-site request forgery	
4	Low	Vulnerable JavaScript dependency	
5	Low	Open redirection (DOM-based)	
6	Informational	TLS certificate	
7	Informational	Cross-site scripting (reflected)	Так
8	Informational	Cross-origin resource sharing - 35	
9	Informational	Cross-origin resource sharing: arbitrary origin trusted - 35	
10	Informational	Input returned in response (reflected) - 15	
11	Informational	Cross-domain Referer leakage	
12	Informational	Cross-domain script include	
13	Informational	Backup file 2	
14	Informational	Private IP addresses disclosed	
15	Informational	Robots.txt file	
16	Informational	Cacheable HTTPS response	
17	Informational	HTML does not specify charset	
18	Informational	Path-relative style sheet import	

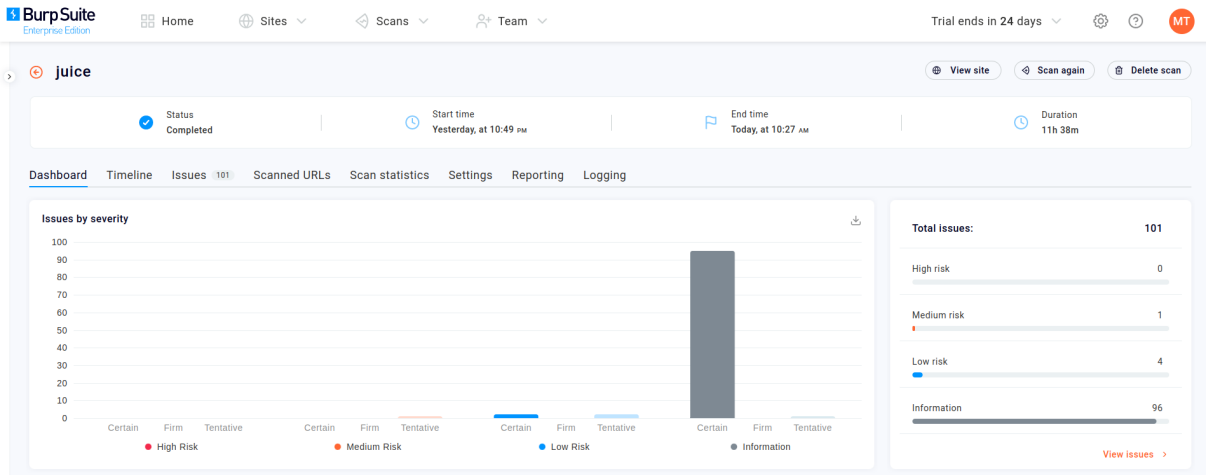

Рисунок. 3.3 – Скріншот результату сканування Burp Suite Enterprise Edition

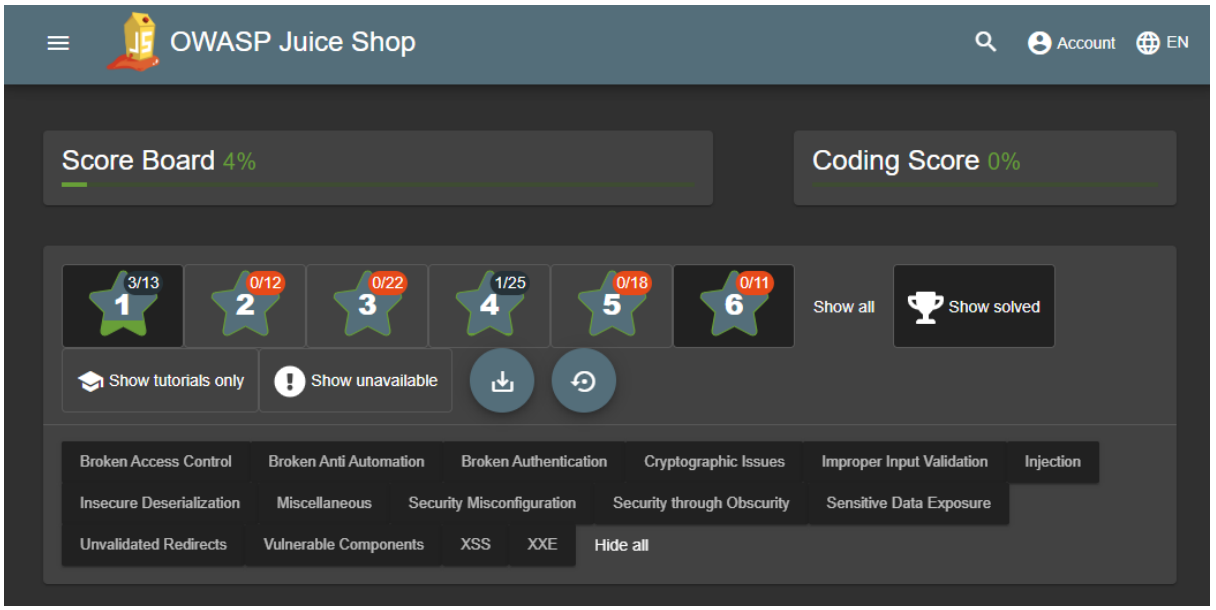

Рисунок. 3.4 – Автоматичне виявлення знайдених вразливостей Burp Suite Enterprise Edition

Nessus Professional. Результати сканування OWASP Juice Shop за допомогою Nessus Professional виявили декілька уразливостей, переважно на інформаційному рівні. Серед них відсутність заголовка Strict Transport Security (HSTS) у HTTPS-сервері, що може призвести до збільшення ризику атак типу "до-чоловіка-посередника" (man-in-the-middle) та інших атак, пов'язаних з протоколом зашифрованого з'єднання.

Додаткові інформаційні уразливості, виявлені Nessus Professional, стосуються дозволених HTTP-методів для кожного каталогу, типу та версії HTTP-сервера, інформації про протокол передачі гіпертексту (HTTP) та інформації про перенаправлення HTTP. Ці результати можуть допомогти спеціалістам з безпеки отримати більш детальну інформацію про налаштування та роботу веб-застосунку, що може бути корисним для подальшого аналізу та виявлення можливих уразливостей.

Загалом, результати сканування за допомогою Nessus Professional виявили менше критичних або серйозних уразливостей порівняно з Acunetix. Однак, цей інструмент також виявив корисну інформацію про веб-застосунок, що може сприяти покращенню безпеки системи, коли враховується в комбінації з результатами інших сканерів.

Таблиця 3.3 – Список знайдених вразливостей Nessus Professional

№	Severity	Vulnerability	Score Board
1	Informational	HSTS Missing From HTTPS Server	
2	Informational	HTTP Methods Allowed (per directory)	
3	Informational	HTTP Server Type and Version	
4	Informational	HyperText Transfer Protocol (HTTP) Information	
5	Informational	HyperText Transfer Protocol (HTTP) Redirect Information	

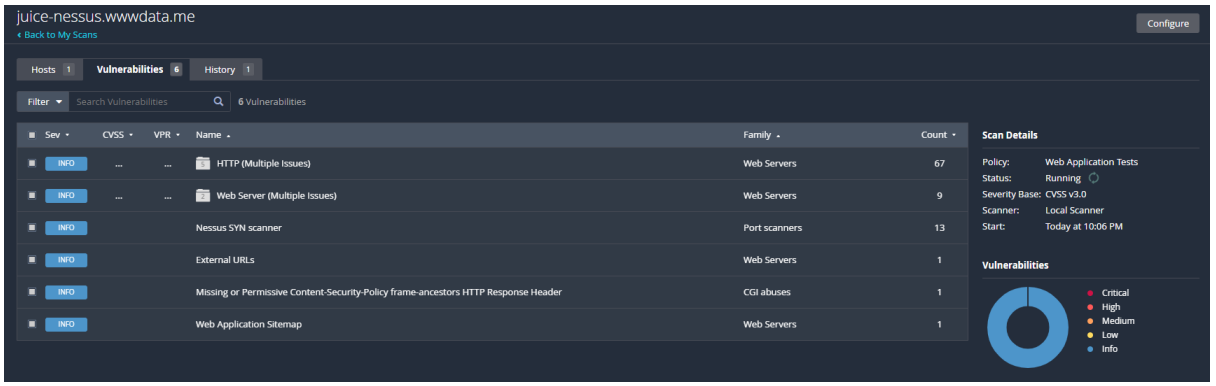

Рисунок. 3.5 – Скріншот результату сканування Nessus Professional

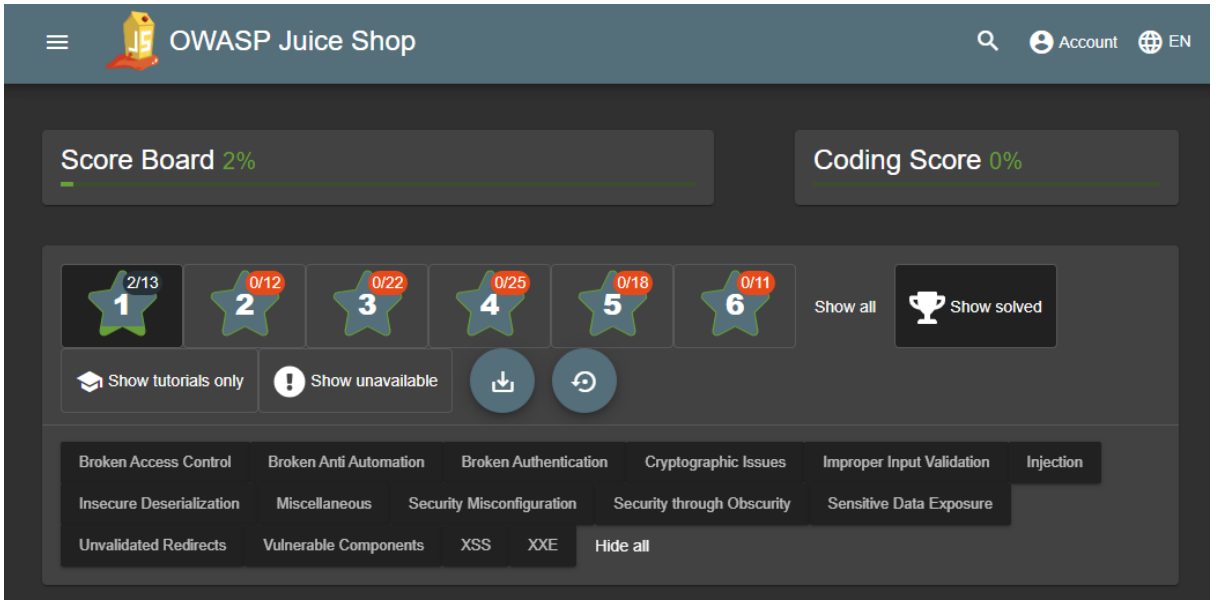

Рисунок. 3.6 – Автоматичне виявлення знайдених вразливостей Nessus Professional.

OpenVAS. Під час сканування OWASP Juice Shop за допомогою OpenVAS було виявлено менше вразливостей, порівняно з іншими сканерами. Проте, варто зазначити, що OpenVAS є більш спрямованим на тестування мережі, а не конкретно веб-застосунків. Він може доповнити результати інших сканерів, допомагаючи виявити можливі слабкі місця на рівні мережі.

Незважаючи на специфіку OpenVAS, він все ж виявив деякі вразливості в OWASP Juice Shop, хоча й не у такій кількості, як інші інструменти. Використання OpenVAS разом з іншими сканерами може забезпечити більш

повний аналіз безпеки, поєднуючи результати веб-сканування та аналіз мережі.

Таблиця 3.4 – Список знайдених вразливостей OpenVAS

№	Severity	Vulnerability	Score Board
1	High	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	

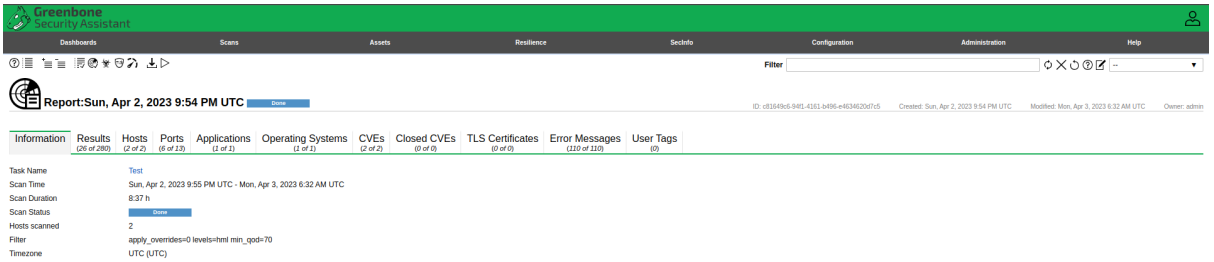

Рисунок. 3.7 – Скріншот результату сканування OpenVAS

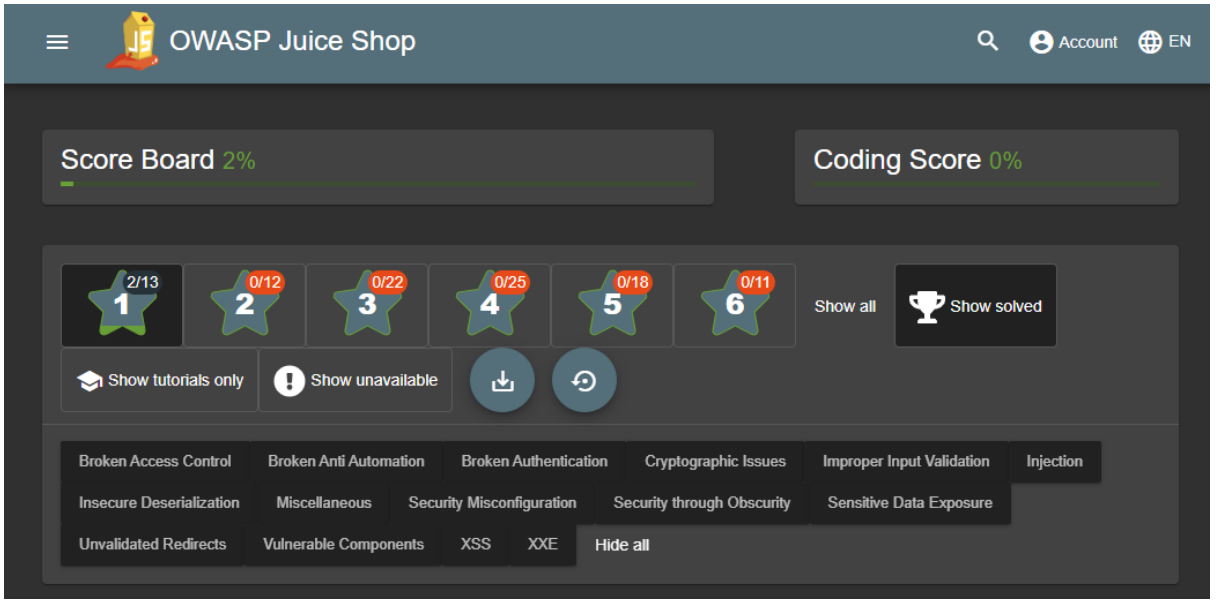

Рисунок. 3.8 – Автоматичне виявлення знайдених вразливостей OpenVAS

3.3 Взаємодія сканерів вразливостей з брандмауерами

В цьому розділі буде проведено тестування різних браундмаерів на основі результатів сканування, отриманих за допомогою Acunetix сканера вразливостей. Оскільки Acunetix продемонстрував високу ефективність у виявленні вразливостей веб-додатків, його результати використовуються як основа для подальшого тестування браундмаерів.

У розділі будуть розглянуті такі браундмаери, як Cloudflare WAF, AWS Shield та AstraSecurity Firewall, та їхня взаємодія з веб-додатком, що був попередньо просканований Acunetix. Для кожного браундмаеру будуть проведені тести, щоб оцінити їхню ефективність у виявленні та блокуванні потенційних загроз та атак на веб-додаток.

CloudFlare WAF. В процесі тестування та взаємодії сканерів вразливостей з Cloudflare WAF використовувався тарифний план Pro від Cloudflare. Цей план надає розширені можливості захисту, включаючи виявлення та блокування шкідливого трафіку, захист від DDoS-атак, покращену управління кешуванням та інші функції безпеки. Він є підходящим вибором для середнього бізнесу, який має потребу в надійному захисті свого веб-додатку від різних загроз та атак.

У процесі взаємодії сканерів вразливостей з Cloudflare WAF було виявлено кілька вразливостей, які були знайдені під час сканування веб-додатку. Серед них є потенційні вразливості міжсайтового скриптінгу (Cross-site Scripting, XSS).

Також було виявлено відсутність налаштування заголовків безпеки, зокрема Content Security Policy (CSP), HTTP Strict Transport Security (HSTS) та Permissions-Policy header.

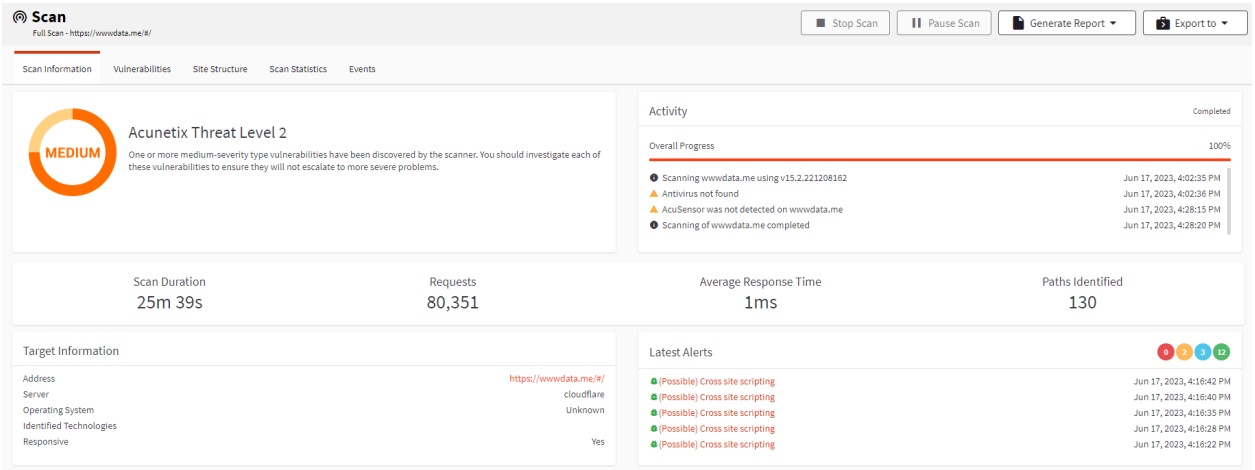

Рисунок. 3.9 – Скріншот результату сканування з використанням CloudFlare WAF Pro

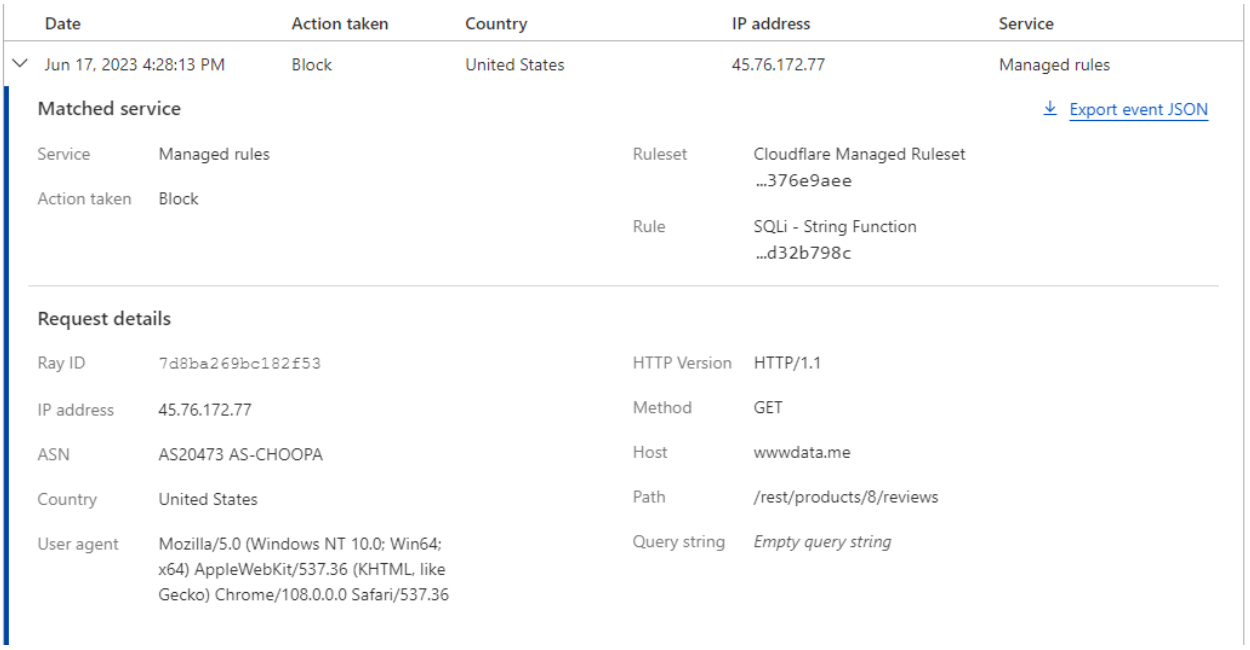

Рисунок. 3.10 – Скріншот сповіщення про блокування запиту на CloudFlare WAF Pro

AWS Shield. AWS Shield та AWS WAF. У процесі тестування та взаємодії сканерів вразливостей з AWS Shield та AWS WAF, використовувалася поєднана захисна стратегія, яка включає дві послуги: AWS Shield та AWS WAF.

AWS Shield є першоверговим сервісом захисту від DDoS-атак на рівні мережі. Він надає захист від широкого спектру DDoS-атак, включаючи атаки

на рівні мережі (Layer 3 and 4), такі як SYN/ACK, UDP-потопи та ICMP-атаки. AWS Shield забезпечує автоматичне виявлення та митигацію DDoS-атак, що дозволяє забезпечити безперебійну роботу веб-додатку.

AWS WAF є рішенням на рівні додатку, яке надає захист від різних типів веб-атак, таких як SQL-ін'єкції, міжсайтовий скриптінг (XSS), небезпечні HTTP-методи та багато інших. AWS WAF використовується для фільтрації та блокування шкідливого трафіку, що надходить до веб-додатку.

У нашому тестуванні ми також використовували AWS WAF з базовим налаштуванням. Це дозволяє захистити веб-додаток від відомих типів атак та фільтрувати трафік на основі правил, які визначаються в залежності від вимог безпеки.

Після проведення тестування виявлено, що застосування AWS Shield та WAF з базовим налаштуванням дозволяє ефективно захистити веб-додаток від широкого спектру атак. Комбінація AWS Shield та AWS WAF надає рівень безпеки на рівні мережі та додатку, що допомагає запобігти DDoS-атакам та забезпечити надійний захист веб-додатку від різних загроз та вразливостей.

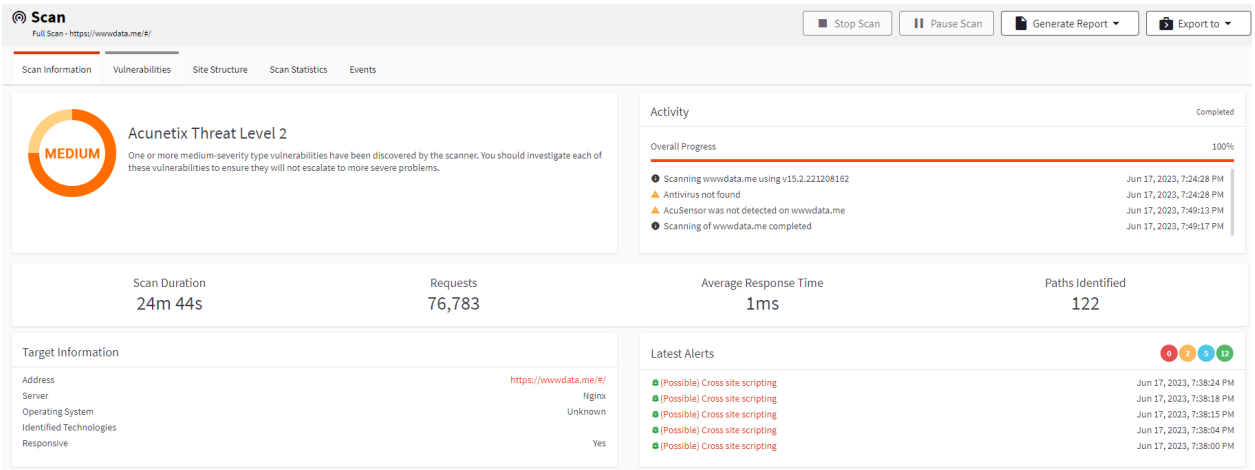

Рисунок. 3.11 – Скріншот результату сканування з використанням AWS WAF

AstraSecurity Firewall - це захисне рішення, спеціалізоване на виявленні та блокуванні загроз безпеки веб-додатків. Воно використовує різноманітні техніки та алгоритми для перехоплення та аналізування трафіку,

що надходить до веб-додатку. AstraSecurity Firewall забезпечує захист від різних типів атак, таких як SQL-ін'єкції, XSS, DDoS-атаки та багато інших.

Однією з переваг AstraSecurity Firewall є його здатність адаптуватись до змінних загроз та вразливостей. Він постійно оновлюється з використанням найновіших розробок у сфері безпеки, що дозволяє ефективно виявляти та блокувати нові атаки. AstraSecurity Firewall також пропонує розширені налаштування та функціонал для аналізу та моніторингу трафіку, що допомагає адміністраторам веб-додатків забезпечити безпеку та надійність своїх систем.

Загалом, AstraSecurity Firewall є потужним інструментом для захисту веб-додатків від загроз безпеки на рівні додатку. Він надає зручний інтерфейс для налаштування та моніторингу безпеки, а також виявляє та блокує різноманітні атаки. Однак, для повноцінного захисту рекомендується комбінувати його з іншими рішеннями, що надають захист на рівні мережі та інфраструктури, а також враховувати індивідуальні потреби та вимоги вашого бізнесу.

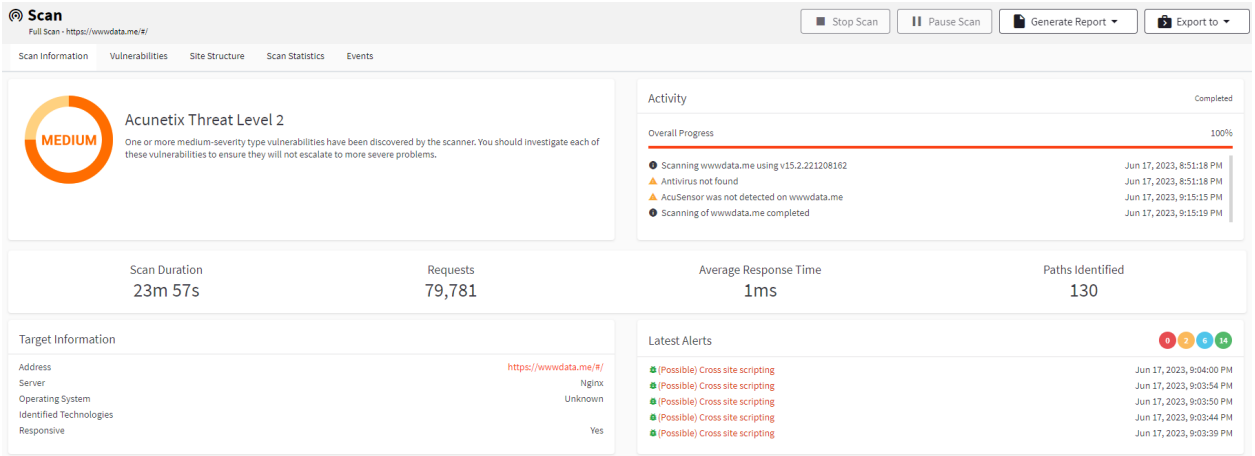

Рисунок. 3.12 – Скріншот результату сканування з використанням AstraSecurity Firewall

3.4 Оцінка ефективності та рекомендації

Враховуючи результати тестування та порівняння ефективності різних WAF-систем, можна зробити висновок, що застосування WAF є ефективним заходом для захисту веб-додатків від різних видів атак та уразливостей. Наведена таблиця демонструє кількість виявлених уразливостей при проведенні тестування без WAF та застосуванні різних WAF-систем.

CloudFlare WAF, AWS Shield та AstraSecurity Firewall продемонстрували позитивні результати в захисті веб-додатків. Використання цих систем зменшило кількість виявлених уразливостей, що свідчить про їх ефективність у виявленні та блокуванні шкідливого трафіку та атак.

Порівнюючи ціни та функціональні можливості різних WAF-систем, можна зробити економічні висновки. CloudFlare WAF включає безкоштовний план, який може бути привабливим для малих бізнесів з обмеженим бюджетом. AWS Shield та AstraSecurity Firewall пропонують платні плани з різними рівнями захисту та функціональності. При виборі WAF-системи, слід ураховувати особливості свого бізнесу, обсяг трафіку та бюджет, а також враховувати рівень захисту, який необхідний для веб-додатку.

Загалом, застосування WAF є ефективним і раціональним рішенням для захисту веб-додатків від широкого спектру атак та уразливостей. Вибір конкретної WAF-системи повинен залежати від конкретних потреб та обмежень вашого бізнесу, таких як розмір компанії, бюджет, потенційні загрози та рівень захисту, необхідний для вашого веб-додатку.

Таблиця 3.5 – Вразливості та WAF: порівняння за кількістю знайдених вразливостей

Назва WAF	Висока	Середня	Низька	Інформаційна
Тестування без WAF	2	2	6	16
CloudFlare WAF	0	2	3	13
AWS Shield	0	2	5	12
AstraSecurity Firewall	0	2	6	14

Усі розглянуті WAF (CloudFlare WAF, AWS Shield та AstraSecurity Firewall) виявилися ефективними засобами захисту веб-додатків. Вони успішно виявили та заблокували багато загроз та вразливостей, знизивши їх кількість до мінімуму. Вибір конкретної WAF-системи повинен залежати від потреб бізнесу, існуючою інфраструктури, бюджету та вимог щодо безпеки. Важливо врахувати ефективність, ціну та інші фактори для забезпечення надійного захисту веб-додатків.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Актуальність безпеки життєдіяльності людини

Безпека життєдіяльності людини стає все більш актуальною в умовах сучасного світу, де технології експоненційно розвиваються, а інформаційний простір постійно збільшується. Системи захисту інформації, які проектуємо та впроваджуємо, неминуче впливають на життєдіяльність людини, а тому необхідно забезпечити, щоб цей вплив був позитивним, а не негативним.

Враховуючи це, безпека життєдіяльності людини включає різні аспекти, зокрема фізичну безпеку, психологічний комфорт, а також безпеку даних і приватності. Кожен з цих аспектів важливий та вимагає уважного ставлення.

Безпека життєдіяльності людини в контексті кібербезпеки може бути розглянута через три ключові складові: фізична безпека, психологічний комфорт, та безпека даних і приватності.

Фізична безпека. Фізична безпека стосується безпекового використання технічних пристроїв, обладнання та інфраструктури, пов'язаних з інформаційними технологіями. Сьогодні використовуються різноманітні пристрої - від персональних комп'ютерів та мобільних пристроїв до великих серверних станцій і дата-центрів. Безпека такого обладнання включає в себе захист від фізичних пошкоджень (від води, вогню, пилу), електробезпеку, забезпечення адекватного охолодження для запобігання перегріву, а також правильну утилізацію відходів.

Також до фізичної безпеки відносяться і біологічні аспекти взаємодії людини з технічними пристроями, де виникають проблеми з випромінюванням від екранів, ергономіки робочих місць, вплив на зір.

Психологічний комфорт. Психологічний комфорт в контексті кібербезпеки стосується створення безпечного і комфортного інформаційного простору для користувача. Сучасна людина проводить значну частину свого

часу в інтернеті: працює, навчається, спілкується, розважається. Все це може впливати на її психологічний стан.

Це включає в себе захист від небажаного контенту, забезпечення приватності, захист від кібербулінгу і тиску соціальних мереж, забезпечення доступу до потрібної та корисної інформації. Часто люди відчувають стрес або навіть страх від можливості втрати даних, крадіжки особистої інформації, використання її з метою шахрайства.

Безпека даних і приватності. Безпека даних і приватності стала одним з найважливіших аспектів сучасної кібербезпеки. Дані стали новим "нафтогазом", цінним ресурсом, за який ведеться боротьба. Безпека даних стосується захисту інформації від небажаного доступу, витоку, втрати, пошкодження, крадіжки.

Від цього залежить не тільки безпека конкретного користувача, але й безпека всього суспільства в цілому. Наприклад, компрометація даних про здоров'я може мати негативні наслідки для людей, яких ці дані стосуються. Витік даних може призвести до фінансових втрат, репутаційних ризиків, проблем з законодавством.

Приватність стала основоположним правом людини в інформаційному суспільстві. Це стосується не тільки права контролювати розповсюдження своїх персональних даних, але й права на анонімність, права на свободу вибору, права на забуття.

Безпека життєдіяльності людини в сучасному світі включає в себе ряд аспектів, починаючи від фізичного здоров'я і закінчуючи захистом приватності та даних. Всі ці аспекти важливі та вимагають вдумливого підходу при проектуванні та використанні інформаційних систем і технологій.

Таким чином, актуальність безпеки життєдіяльності людини в сфері кібербезпеки є очевидною. Наше завдання як спеціалістів в галузі безпеки - це не тільки створити ефективну систему захисту інформації, але й

забезпечити, щоб ця система сприяла загальному благополуччю людей, які її використовують.

4.2 Вплив електромагнітних полів (ЕМП) на людину та заходи щодо зменшення їх впливу на обслуговуючий персонал

Електромагнітні поля (ЕМП) - це поле, яке створюється змінними електричними та магнітними полями. Воно виникає в результаті роботи електричних пристроїв, радіовеж, мобільних телефонів, комп'ютерів, мікрохвильових печей, а також промислового обладнання.

Електромагнітні поля (ЕМП) є скрізь, де є електричний струм. Це включає електричні пристрої, електропроводку в будівлях, і, звичайно, передачу сигналів в радіо і телебаченні. Ось деякі з найпоширеніших джерел ЕМП:

- побутові прилади: багато побутових приладів створюють електромагнітні поля при їх використанні. Це включає телевізори, мікрохвильові печі, холодильники, комп'ютери, мобільні телефони, фени, електричні голівки для гоління та багато інших пристроїв;

- електромережа: електромагнітні поля створюються електричною енергією, яка протікає через кабелі. Це включає не тільки кабелі в мережі, але й в домашньому освітленні, побутових приладах та іншому обладнанні;

- промислове обладнання: Великі машини та обладнання, що використовуються в промисловості, часто створюють великі електромагнітні поля. Це може включати електромотори, генератори, трансформатори, електрозварювальні машини;

- бездротові комунікації: радіо- та телевізійні станції, мобільні телефонні станції, Wi-Fi маршрутизатори, бездротові телефони та інші пристрої для бездротових комунікацій також створюють електромагнітні поля;

- медичні пристрої: багато медичних пристроїв, таких як МРТ, рентгенівські апарати, ультразвукове обладнання, також створюють електромагнітні поля.

Враховується, що інтенсивність електромагнітного поля зазвичай зменшується із збільшенням відстані від джерела. Тому, хоча багато пристроїв можуть створювати електромагнітні поля, рівень впливу цих полів на людей може значно варіюватися в залежності від відстані до джерела.

Вплив ЕМП на людину. ЕМП можуть впливати на біологічні процеси в організмі людини. Вони впливають на клітини, тканини та органи, спричиняючи різні біофізичні та біохімічні зміни. Вплив ЕМП на людину може виявлятися в різних формах, включаючи головний біль, безсоння, зниження концентрації, втрату пам'яті, стрес, зниження імунітету, а також певні хронічні захворювання.

Взаємодія між ЕМП та біологічними системами є складною і до кінця не вивченою. Наслідки впливу ЕМП на людину в багато разів залежать від інтенсивності та тривалості експозиції, частоти ЕМП, а також індивідуальних особливостей організму.

Заходи щодо зменшення впливу ЕМП на обслуговуючий персонал:

- проектування та розміщення обладнання. На етапі проектування системи, необхідно враховувати заходи по зменшенню випромінювання ЕМП. Використовувати обладнання з низьким рівнем випромінювання ЕМП. Правильно розміщувати обладнання, дотримуючись відстані між пристроями та робочими місцями;

- охорона праці. Забезпечувати виконання вимог нормативних документів з охорони праці, проводити періодичні медичні огляди працівників;

- використання засобів захисту. За потреби, використовувати спеціальні захисні пристрої, такі як феритові котушки, екрани, фільтри;

- інформаційна безпека. Проводити регулярне інформування та навчання персоналу з питань безпеки під час роботи з обладнанням, яке створює ЕМП;

- Регулярний моніторинг. Здійснювати постійний контроль за рівнем ЕМП на робочих місцях, за допомогою спеціалізованих приладів.

Таким чином, питання впливу електромагнітних полів на людину, та заходи щодо зменшення їх впливу на обслуговуючий персонал є дуже актуальним і важливим елементом у підготовці бакалаврської роботи з кібербезпеки.

ВИСНОВКИ

У цій кваліфікаційній роботі був проведений порівняльний аналіз сканерів вразливостей та брандмауерів веб-додатків для бізнесу. Основною метою дослідження було визначення ефективності та придатності цих інструментів для забезпечення безпеки веб-додатків у бізнес-середовищі.

Під час аналізу були розглянуті такі сканери вразливостей як Acunetix, Burp Suite Enterprise Edition, Nessus Professional, OpenVAS. Кожен з цих сканерів має свої переваги та особливості, які можуть бути корисними для певних сценаріїв використання. Наприклад, Acunetix відомий своєю високою швидкістю та надійністю сканування, Burp Suite Enterprise Edition надає широкий спектр функціональності для тестування вразливостей, Nessus Professional має велику базу даних з відомими вразливостями, а OpenVAS є відкритим інструментом з активною спільнотою користувачів.

Також було розглянуто брандмауери веб-додатків, такі як Cloudflare, AWS Shield та AstraSecurity Firewall. Ці брандмауери надають різні рівні захисту, включаючи захист від DDoS-атак, виявлення та блокування зловмисних трафіків, контроль доступу та багато іншого.

В результаті порівняльного аналізу сканерів вразливостей та брандмауерів веб-додатків було встановлено, що вибір інструментів залежить від конкретних потреб і вимог бізнесу. Кожен з них має свої переваги та обмеження, і важливо враховувати контекст використання та характеристики організації при прийнятті рішення щодо вибору.

Дослідження виявило, що безпека веб-додатків для бізнесу є надзвичайно важливою і складною задачею. Використання відповідних сканерів вразливостей та брандмауерів може допомогти уникнути вразливостей та захистити веб-додатки від потенційних атак та зловмисних дій.

Далі дослідження може бути розширене шляхом включення інших інструментів та методів захисту, а також проведення більш детального аналізу ефективності та результативності цих інструментів. Важливо також

розглянути реальні сценарії використання веб-додатків у різних бізнес-середовищах для отримання більш точних і практичних висновків.

Загалом, дане дослідження сприяє поглибленню розуміння процесу захисту веб-додатків у бізнес-середовищі та надає важливу інформацію для прийняття розумних рішень щодо вибору відповідних інструментів та стратегій безпеки. Забезпечення безпеки веб-додатків є невід'ємною частиною розвитку сучасних бізнес-організацій, і правильне використання сканерів вразливостей та брандмауерів може в суттєвій мірі покращити рівень безпеки та надійності веб-додатків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Національний стандарт України "Захист інформації. Вимоги до систем захисту інформації та інформаційно-телекомунікаційних систем". [Електронний ресурс]. Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
2. Whitepaper "Choosing the Right Web Application Firewall (WAF) for Your Organization" від OWASP (Open Web Application Security Project). [Електронний ресурс]. Режим доступу до ресурсу: https://owasp.org/www-pdf-archive/Choosing_the_Right_WAF_Web_Application_Firewall.pdf.
3. "ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements". [Електронний ресурс]. Режим доступу до ресурсу: https://www.iso.org/standard/54534.html.
4. Mitre ATT&CK [Електронний ресурс]. Режим доступу до ресурсу: https://attack.mitre.org/.
5. NIST Special Publication 800-30: Guide for Conducting Risk Assessments [Електронний ресурс]. Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01.
6. All-in-one Web Application Security Scanner [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.acunetix.com/resources/acunetix-brochure.pdf.
7. Burp Suite Enterprise Edition - PortSwigger [Електронний ресурс] – Режим доступу до ресурсу: https://portswigger.net/burp/enterprise.
8. DataSheet Nessus Professional [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://static.tenable.com/marketing/datasheets/DataSheet-Nessus_Professional.pdf.
9. "OpenVAS - Open Vulnerability Assessment System" by Greenbone Networks [Електронний ресурс]. Режим доступу до ресурсу: https://www.greenbone.net/en/openvas/.

10. What is a WAF? | Web Application Firewall explained [Електронний ресурс]. Режим доступу до ресурсу: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/.
11. "AWS Shield - Managed DDoS Protection" by Amazon Web Services [Електронний ресурс]. Режим доступу до ресурсу: https://aws.amazon.com/shield/.
12. OWASP Top Ten [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://owasp.org/www-project-top-ten/.
13. OWASP Juice Shop [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://owasp.org/www-project-juice-shop/.
14. Acunetix vs. Burp Suite [Електронний ресурс]. – Режим доступу до ресурсу: https://resources.whitesourcesoftware.com/blog-whitesource/acunetix-vs-burp-suite.

ДОДАТОК А – Порівняльний аналіз сканерів вразливостей: параметри порівняння, переваги та недоліки

Параметри порівняння	Acunetix	Burp Suite Enterprise Edition	Nessus Professional	OpenVAS
Ціна	Висока	Висока	Висока, є обмежена безкоштовна версія	Безкоштовний
Спрямування	Веб-додатки	Веб-додатки, мережа	Мережа, веб-додатки	Мережа, веб-додатки
Виявлення уразливостей	Так	Так	Так	Так
Деталізація результатів	Висока	Висока	Висока	Середня
Інтеграція	Часткова	Повна	Повна	Повна
Встановлення	Локально, хмарно	Локально, хмарно	Локально, хмарно	Локально
Підтримка	Так	Так	Так	Спільнота
Складність використання	Низька	Середня	Середня	Висока
Покриття тестування	Високе	Високе	Високе	Середнє
Підтримка проксі	Так	Так	Так	Так
Розширені функції	Так	Так	Так	Так
Швидкість сканування	Висока	Середня	Висока	Середня
Користувацький інтерфейс	Інтуїтивний	Інтуїтивний	Інтуїтивний	Складний
Технічна підтримка	Так	Так	Так	Спільнота

Переваги застосування	Автоматизація, сканування API	Широкий функціонал, автоматизація	Багатофункціональність, інтеграція з системами	Відкритий код, гнучкість
Переваги	Висока точність виявлення уразливостей, розширені функції сканування	Висока точність виявлення уразливостей, гнучкість налаштування	Велика база даних уразливостей, інтеграція з іншими інструментами	Відкритий код, безкоштовний
Недоліки	Висока ціна	Висока ціна, складність налаштування	Висока ціна, менш точне виявлення уразливостей веб-додатків	Відсутність технічної підтримки, обмежена база даних уразливостей

ДОДАТОК Б – Порівняльний аналіз WAF: параметри порівняння, переваги та недоліки

Параметри порівняння	CloudFlare WAF	AWS Shield/WAF	AstraSecurity Firewall
Ціна	Комерційна, є обмежена безкоштовна версія	Комерційна, є обмежена безкоштовна версія, що покриває DDoS атаки рівня L3, L4	Комерційна
Охоплення застосувань	Веб-додатки, CDN	Веб-додатки, CDN	Веб-додатки
Захист від DDoS-атак	Так	Так	Ні
Захист від веб-атак	Так	Так	Так
Інтеграція	API	API	API
Підтримка	Так	Так	Так
Складність використання	Низька	Середня	Середня
Надійність	Висока	Висока	Висока
Регулярні оновлення	Так	Так	Так
Сервісний рівень	Підтримка 24/7	Підтримка 24/7	Підтримка 24/7
Гнучкість	Середня	Висока	Висока
Пропускна здатність	Висока	Висока	Залежить від сервера
Аналітика трафіку	Так	Так	Так
Візуалізація	Так	Так	Ні

Контроль доступу	Так	Так	Так
Інспекція SSL/TLS	Так	Так	Так
Політики безпеки	Так	Так	Так
Функція реверсного проксі	Так	Так	Ні
Система виявлення вторгнень	Так	Так	Так
Моніторинг та журналювання	Так	Так	Так
Впровадження	Хмарна платформа	Інфраструктура AWS	Локальний сервер
Сумісність	Мультиплатформений	AWS-орієнтований	Мультиплатформений
Технічна підтримка	Так	Так	Так