|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | | |
| **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | | | | | |
|  | |  | | | |  | | | |  | | |  |
| **КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ** | | | | | | | | | | | | | |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
| Пояснювальна записка | | | | | | | | | | | | | |
| до бакалаврської роботи | | | | | | | | | | | | | |
|  | | на тему: | | | | | | | | | | |  |
| **«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ WEB-ДОДАТКІВ НА БАЗІ РІШЕННЯ WAF»** | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | | Виконав студент 4 курсу, групи БСД-43 | | | | | | | |
|  | |  | | | | спеціальності 125 Кібербезпека | | | | | | | |
|  | |  | | | | освітньо-професійної програми «Інформаційна та | | | | | | | |
|  | |  | | | | кібернетична безпека» | | | | | | | |
|  | |  | | | | (шифр і назва спеціальності) | | | | | | | |
|  | |  | | | | Єкімов І.В. | | | | | | | |
|  | |  | | | | (прізвище та ініціали) | | | | | | | |
|  | |  | | | | Керівник | | Бойко А.О. | | | | | |
|  | |  | | | |  | | | | (прізвище та ініціали) | | | |
|  | |  | | | | Рецензент | | |  | | | | |
|  | |  | | | | (прізвище та ініціали) | | | | | | | |
|  | |  | | | | Нормоконтролер | | | | | |  | |
|  | |  | | | |  | | | | (прізвище та ініціали) | | | |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | | КИЇВ – 2023 | | | | | | | | | | |  |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | | |
| Інститут | | ННІЗІ | | | |  | | | |  | | |  |
| Кафедра | | Інформаційної та кібернетичної безпеки | | | | | | | | | | | |
| Ступінь вищої освіти | | | | Бакалавр | | | | | |  | | |  |
| Спеціальність | | | 125 Кібербезпека | | | | | | |  | | |  |
| Освітньо-професійна програма | | | | | | Інформаційна та кібернетична безпека | | | | | | | |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | | ЗАТВЕРДЖУЮ | | | |
|  | |  | | | |  | | | | Завідувач кафедри ІКБ | | | |
|  | |  | | | |  | | | |  | | | Гайдур Г.І. |
|  | |  | | | |  | | | | “\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | | |
|  | |  | | | |  | | | |  | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | | **З А В Д А Н Н Я** | | | | | | | | | | |  |
|  | | **НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ** | | | | | | | | | | |  |
|  | |  | | | |  | | | |  | | |  |
|  | | | | | | | | | | | | | |
| (прізвище, ім’я, по батькові) | | | | | | | | | | | | | |
| 1. Тема бакалаврської роботи: | | | | | «Дослідження шляхів та розробка рекомендацій | | | | | | | | | |
| щодо захисту WEB-додатків на базі рішення WAF» | | | | | | | | | | | | | |
| керівник бакалаврської роботи | | | | | | Бойко Анна Олександрівна, асистент. | | | | | | | |
|  | |  | | | | (прізвище, ім’я, по батькові, науковий ступінь, вчене звання) | | | | | | | |
| затверджені наказом закладу вищої освіти від «\_\_\_ » \_\_\_\_\_\_\_\_2023 року № \_\_\_\_. | | | | | | | | | | | | | |
|  | |  | | | |  | | | |  | | |  |
| 2. Строк подання студентом бакалаврської роботи | | | | | | | | | | | 28.05.2021 р. | | |
|  | |  | | | |  | | | |  | | |  |
| 3. Вихідні дані до бакалаврської роботи | | | | | | |  | | | | | |  |
| веб-додатки; | | | | | | | | | |  | | |  |
| рішення захисту веб-додатків від Barracuda WAF; | | | | | | | | | | | | | |
| наукова та технічна література, експлуатаційна документація, нормативні | | | | | | | | | | | | | |
|  |
|  | |  | | | |  | | | |  | | |  |
| 4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) | | | | | | | | | | | | | |
| 1. Актуальність проблеми забезпечення захисту веб-додатків. | | | | | | | | | | | | | |
| 2. Аналіз веб-додатків та існуючі загрози. | | | | | | | | | | | | | |
| 3. Методи та засоби забезпечення веб-додатків за допомогою Barracuda WAF. | | | | | | | | | | | | | |
| 4. Рекомендації щодо забезпечення безпечного використання Barracuda WAF. | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. Перелік графічного матеріалу | | | | |  | |  | |
| 1. Тема бакалаврської роботи. | | | | | | | | |
| 2. Об’єкт, предмет, мета та наукові завдання дослідження. | | | | | | | | |
| 3. Результати аналізу класифікації надання послуг WAF сервісів та атак на WAF. | | | | | | | | |
| 4. Результати аналізу методів та засобів забезпечення безпеки веб-додатків | | | | | | | | |
| 5. Призначення та можливості рішення Barracuda WAF. | | | | | | | | |
| 6. Рекомендації щодо забезпечення безпечного доступу до Barracuda WAF. | | | | | | | | |
| 7. Висновки за результатами роботи. | | | | | | | | |
|  | | | | | | | | |
| 6. Дата видачі завдання | | | 15.02.2023 р. | | | | | |
|  | |  | |  |  | |  | |
|  | | **КАЛЕНДАРНИЙ ПЛАН** | | | | |  | |
|  | |  | |  |  | |  | |
| №  зп | Назва етапів  бакалаврської роботи | | | | | Строк виконання етапів бакалаврської роботи | | Примітка |
| 1. | Визначення актуальності проблеми забезпечення безпечного доступу до веб-додатків | | | | | 15.02.2023 р. | |  |
| 2. | Аналіз наукової та технічної літератури з питань теми бакалаврської роботи. | | | | | 22.02.2023 р. | |  |
| 3. | Аналіз методів та засобів забезпечення безпеки веб-додатків | | | | | 26.03.2023 р. | |  |
| 4. | Розроблення рекомендацій щодо застосування рішення Barracuda WAF для забезпечення безпеки веб-додатків. | | | | | 30.04.2023 р. | |  |
| 5. | Оформлення результатів дослідження. | | | | | 18.05.2023 р. | |  |
| 6. | Підготовка доповіді до захисту. | | | | | 28.05.2023 р. | |  |
|  | | | | | |  | |  |
|  | |  | | Студент |  | | | |
|  | |  | |  | (підпис) | | прізвище та ініціали | |
|  | |  | |  |  | |  | |
| Керівник бакалаврської роботи | | | | |  | | Бойко А.О. | |
|  | |  | |  | (підпис) | | прізвище та ініціали | |
|  | |  | |  |  | |  | |

**ВІДГУК РЕЦЕНЗЕНТА**

на бакалаврську роботу

студентаЄкімова Івана Вікторовича

на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту WEB-додатків на базі рішення WAF»

**Актуальність:** Сьогодні користувачі будь-якої із існуючих операційних систем постійно використовують веб-додатки. Робота присвячена одному з найперспективніших напрямків розвитку телекомунікацій – веб-додатки. Веб-додатки дозволяють користувачам виконувати різноманітні завдання та функції у веб-браузері без необхідності встановлення додаткового програмного забезпечення на своєму пристрої.. Сьогодні існує кілька моделей обслуговування та існуючих рішень, кожна з яких має свої переваги та недоліки, а також певну сферу застосування. Тому тема бакалаврської роботи є актуальною і своєчасною.

**Позитивні сторони:**

1. Зміст роботи відповідає завданню. Студент, показав високий рівень знань і ступінь підготовленості до майбутньої роботи за фахом.

2. Обґрунтовано необхідність використання веб-додатків. Достатньо успішно викладено матеріали щодо моделей розгортання та забезпечення безпеки в веб-додатків.

3. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено досить якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

**Недоліки:**

1. В роботі слід було провести більш детальний аналіз до використовувати технічної літератури по темі бакалаврської роботи.

**Висновок:** Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре**, а студент **Єкімов І.В.** – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

|  |  |  |
| --- | --- | --- |
| Якість роботи | | Підпис рецензента (\_\_\_\_\_\_\_\_\_\_\_\_\_\_)  Підпис засвідчую  Підпис особи, що засвідчує (\_\_\_\_\_\_\_\_\_\_\_\_) |
| Виконано на замовлення підприємства |  |
| Виконано за тематикою НДР |  |
| Виконано з макетом |  |
| Виконано з застосуванням ЕОМ та МПТ | √ |
| Має практичну цінність | √ |
| Проект-частина комплексної теми |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | |
| **ПОДАННЯ**  **ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**  **ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ** | | | | | | | | |
| Направляється студент | | Єкімов І.В. | | | до захисту бакалаврської роботи | | | |
|  | | (прізвище та ініціали) | | |  | | | |
| спеціальності 125 Кібербезпека | | |  | | |  | |  |
| освітньо-професійної програми | | | Інформаційна та кібернетична безпека | | | | | |
|  |  | | (шифр і назва спеціальності) | | | | | |
| на тему: | «Дослідження шляхів та розробка рекомендацій щодо захисту WEB-додатків | | | | | | | |
| на базі рішення WAF». | | | | | | | | |
| Бакалаврська робота і рецензія додаються. | | | | | |  | |  |
| Директор інституту | | |  | | | Савченко В.А. | | |
| (підпис) (прізвище та ініціали) | | | | | | | | |
|  |  | |  | | |  | |  |
|  | **Довідка про успішність** | | | | | | |  |
| Єкімов І.В. | | | за період навчання в інституті | | | | | |
| (прізвище та ініціали студента) | | |  | | |  | |  |
| ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:  національною шкалою: відмінно \_\_\_\_%, добре \_\_\_\_%, задовільно \_\_\_\_%;  шкалою ECTS: А \_\_\_\_%; В \_\_\_\_%; С \_\_\_\_%; D \_\_\_\_%; Е \_\_\_\_%. | | | | | | | | |
| Секретар інституту, факультету (відділення) | | | | | |  | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  | |  | | | (підпис) | | (прізвище та ініціали) |
|  | **Висновок керівника бакалаврської роботи** | | | | | | |  |
| Студент ***Єкімов І.В.*** обрав тему роботи, метою якої було дослідження шляхів та розробка рекомендацій щодо захисту WEB-додатків на базі рішення WAF. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Єкімов показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.  Все це дозволяє оцінити виконану бакалаврську роботу студента Єкімов Івана Вікторовича на оцінку **добре** та присвоїти їй кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека. | | | | | | | | |
| Керівник бакалаврської роботи | | | | | |  | | Бойко А.О. |
|  |  | |  | | | (підпис) | | (прізвище та ініціали) |
|  |  | |  | | | “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |
|  | **Висновок кафедри про бакалаврську роботу** | | | | | | |  |
| Бакалаврська робота розглянута. Студент | | | | Єкімов І.В. | | | | |
|  |  | |  | (прізвище та ініціали) | | | | |
| допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії. | | | | | | | | |
| Завідувач кафедри Інформаційної та кібернетичної безпеки | | | | | | |  |  |
| (назва) | | | | | | | | | |
|  |  | |  | | |  | | Гайдур Г.І. |
|  |  | | (підпис) | | | (прізвище та ініціали) | | |
| “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |  | | |  | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **РЕФЕРАТ** | | | | |
|  |  |  |  |  |
|  |  |  |  |  |
| Текстова частина бакалаврської роботи: 69 сторінок, 17 рисунків, 11 джерел.  *Об’єкт дослідження* – Web-додатки та засоби захисту.  *Предмет дослідження* – методи та засоби забезпечення захисту WEB-додатків на базі рішення WAF.  *Мета роботи* – аналіз існуючих загроз WEB-додатків та розробка рекомендацій щодо захисту.  *Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.  В роботі приведено основні відомості Web-додатки.  Проаналізовано різні види загроз та наведено їх класифікацію.  Досліджено методи та засоби забезпечення безпеки Web-додатків на базі рішення WAF.  Досліджено можливості програмного комплексу Barracuda WAF.  Галузь використання – кібербезпека та інформаційна безпека.  WEB-ДОДАТКИ, БЕЗПЕКА, ЗАГРОЗА, WAF. | | | | |
|  | | | | |

**ЗМІСТ**

Стор.

[ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 8](#_Toc135698980)

[ВСТУП 10](#_Toc135698981)

[1. АНАЛІЗ ПРОБЛЕМ ЗАХИСТУ WEB-ДОДАТКІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ 13](#_Toc135698982)

[1.1 Визначення Web-додатку , роль і місце веб-дотатків в інформаційній системі організацій 13](#_Toc135698983)

[1.2 Аналіз основних загроз та вразивостей Web-дотаків OWASP 20](#_Toc135698984)

[1.3 Аналіз загальних методів та загальних веб-ресурсів та аналіз ринку рішень WAF 26](#_Toc135698985)

[2. ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ WEB-ДОДАТКІВ ЗА ДОПОМОГОЮ РІШЕННЯ BARRACUDA WAF 34](#_Toc135698986)

[2.1 Аналіз методів та засобів захисту Baracuda WAF 34](#_Toc135698987)

[2.2 Захист Web-додатків за допомогою рішення WAF 42](#_Toc135698988)

[2.3 Приклад використання Barracuda WAF 53](#_Toc135698989)

[3 РОЗРОБКА РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ BARRACUDA WAF 61](#_Toc135698990)

[3.1 Рекомендації що до встановлення рішення Barracuda WAF 61](#_Toc135698991)

[3.2. Розробка загальних рекомендацій , що до застовсування Barracuda WAF 63](#_Toc135698992)

[ВИСОВКИ 65](#_Toc135698993)

[ПЕРЕЛІК ПОСИЛАНЬ 69](#_Toc135698994)

[ДЕМОНСТАЦІЙНІ МАТЕРІАЛИ (Презентація) 70](#_Toc135698995)

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

WAF – Web Application Firewall

SIEM – Security Information and Event Management

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

API – Application Programming Interface

HTTP/HTTPS – Hypertext Transfer Protocol/HTTP Secure

CRM – Customer Relationship Management

PM – Project Management

ERP – Enterprise Resource Planning

OWASP – Open Web Application Security Project

SQL – Structured Query Language

SSL – Secure Sockets Layer

XSS/XXS – Cross-Site Scripting

XXE – XML External Entity

RCE – Remote Code Execution

URL/URI – Uniforn Resource Locator/U R Identifer

OVA – Open Virtual Application

VMDK – Virtual Machine Disk

XCL – Excel Document

XML – eXtensible Markup Language

REST – Representntational State Transfer

JSON – JavaScript Object Nonation

GWT API – Google Web Toolkit API

CSRF – Cross-Site Request Forgery

DDoS – Distributed Denial of Service

AWS – Amazon Web Services

CDN – Content Delivery Network

SEO – Search Engine Oprimization

# ВСТУП

Дослідження та рекомендації щодо захисту WEB-додатків на базі WAF мають значення. Співпраця та обмін інформацією зі спеціалістами є корисними. Рекомендації повинні охоплювати технічні та соціальні аспекти безпеки. Важливе значення має інтеграція з іншими системами та постійний аудит. Постійне оновлення та покращення рекомендацій є необхідними.

Нарешті, важливо розробити стратегію реагування на інциденти безпеки, включаючи план відновлення після атаки та процедури виявлення та реагування. Моніторинг веб-трафіку та виявлення аномалій також є необхідними. Технології машинного навчання та аналізу даних можуть допомогти в автоматизованому виявленні нових атак.

Дослідження та рекомендації щодо захисту WEB-додатків на базі рішення WAF вимагають постійного оновлення та удосконалення. Співпраця зі спеціалістами та обмін інформацією є ключовими для успіху. Технічні та соціальні аспекти безпеки повинні бути враховані. Інтеграція з іншими системами та постійний аудит гарантують ефективність заходів.

Загальний процес покращення безпеки WEB-додатків на базі WAF включає постійне оновлення рекомендацій та стратегій захисту. Розробка плану реагування на інциденти та навчання персоналу є необхідними етапами. Моніторинг веб-трафіку та виявлення аномалій допомагають запобігти атаці. Технології машинного навчання виявляють нові загрози.

Високий рівень безпеки WEB-додатків на базі рішень WAF досягається завдяки дослідженням, рекомендаціям та постійному удосконаленню. Співпраця зі спеціалістами та іншими зацікавленими сторонами дозволяє обмінюватися інформацією про загрози та захисні методи. Інтеграція з іншими системами та моніторинг трафіку допомагають виявленню аномалій та ефективному реагуванню на них. Навчання користувачів та свідомість щодо наявних загроз залишаються факторами безпеки.

Оновлення рекомендацій та стратегій захисту WEB-додатків на базі WAF є необхідними у зв'язку зі швидким розвитком кіберзагрози та появою нових методів нападу. Це вимагає постійного моніторингу, аналізу та оновлення заходів безпеки.

Постійна співпраця зі спеціалістами, дослідниками та іншими зацікавленими сторонами обмінюється інформацією про нові загрози та вразливості. Це сприяє побудові колективного інтелектуального резерву, що забезпечує більш швидку та точну реакцію на загрози.

Навчальні програми та освітні заходи мають на меті підвищення свідомості користувачів щодо кіберзагроз та навчання їх упізнавати та уникати ризиків. Це включає усвідомлення соціальної інженерії та вплив на користувачів, які можуть призвести до розкриття конфіденційної інформації.

Рішення інтеграції WAF з іншими системами та системами безпеки, такими як системи моніторингу нерівностей, системи управління подіями та інцидентами (SIEM) або системи виявлення включення (IDS/IPS), дозволяє створити комплексну систему захисту, що забезпечує інструмент відновлення та реагування після атаки.

Постійний аудит та оцінка ефективності розгорнутої системи захисту включає перевірку налаштування, аналіз подій журналів, виявлення слабких місць та пошук можливих уразливостей. Це додатково ідентифікує ваші проблеми та забезпечує постійне удосконалення системи захисту.

На заключному етапі необхідно провести ретельний аналіз інцидентів безпеки та реагувати на них вчасно. Це включає збір та аналіз даних про атаки, виявлення причин їх виникнення та розробку стратегій запобігання подібним інцидентам у майбутньому.

Усі ці заходи спрямовані на забезпечення високого рівня безпеки WEB-додатків на базі рішень WAF. Вони допомагають зменшити ризики уразливостей, уникнути втрати конфіденційної інформації через те, чому користувачі можуть бути впевнені у безпеці своїх даних.

У світі де кіберзагрози залишаються все складнішими та поширенішими, постійне розвиток та удосконалення методів захисту WEB-додатків на базі рішення WAF є невід'ємною частиною інформаційної безпеки. Лише шляхом поєднання технологічних та організаційних заходів можна забезпечити надійну захист веб-додатків та запобігти поточним загрозам.

# 1. АНАЛІЗ ПРОБЛЕМ ЗАХИСТУ WEB-ДОДАТКІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

## 1.1 Визначення Web-додатку , роль і місце веб-дотатків в інформаційній системі організацій

Web-додаток - це програмне забезпечення, яке запускається на веб-сервері та надає можливість користувачам взаємодіяти з даними, що зберігаються на сервері, через веб-браузер чи мобільний додаток. Веб-додаток може мати різні функції, наприклад, забезпечувати доступ до інформації, виконувати операції з обліковим записом користувача, забезпечувати можливість купівлі товарів чи послуг тощо.

Веб-додатки є інтерактивними застосунками, що складаються з двох частин. Перша частина завантажується у браузер, коли користувач набирає відповідну команду. Друга частина розміщується на веб-сервері, який містить усі дані, закладені у застосунку. Коли користувач запитує, веб-сервер знаходить відповідну інформацію та відправляє її до браузера.

Веб-додатки створюються з різною метою - як для взаємодії з клієнтами, так і для налагодження бізнес-процесів усередині компанії. Ці інструменти мають безліч можливостей. Наприклад, вони дозволяють обмінюватися інформацією між працівниками та клієнтами, проводити транзакції, купувати та продавати товари/послуги дистанційно, працювати з примітками, списком справ та завдань, керувати файлами, що зберігаються у хмарі, конвертувати валюту та одиниці вимірювання, перекладати тексти та багато іншого .

Одним із переваг web-додатків є можливість працівників створювати онлайн документи, відкривати доступ до них для певної групи людей та працювати над спільними проектами дистанційно. Зберігання всіх даних в одному місці дозволяє керівникам легко відстежувати стан бізнесу та швидко виявляти та усувати проблеми.

Крім того, веб-додатки забезпечують зручний доступ до інформації та функцій з будь-якого пристрою, що має підключення до Інтернету. Користувачі можуть отримувати оновлення та виконувати роботу з будь-якого місця та в будь-яку годину, що дозволяє збільшити продуктивність та ефективність роботи.

Однак використання веб-додатків також має свої недоліки. Залежність від Інтернет-підключення може обмежити доступ до даних та функцій у разі відсутності зв'язку. Крім того, збереження даних на веб-сервері може створювати проблеми з їх безпекою та конфіденційністю, тому необхідно приділяти достатню увагу заходам безпеки та захисту даних.

Загалом веб-додатки мають важливе місце в інформаційній системі організації. Вони дозволяють ефективно взаємодіяти з даними та забезпечувати широкий спектр функціональності для користувачів. Продуктивність, доступність та зручність використання роблять їх необхідним інструментом для підтримки бізнес-процесів та взаємодії з клієнтами.

**Переваги web-застосунків:**

1. Не потребує інсталяції: Веб-додатки не потребують встановлення на пристрій користувача. Вони запускаються безпосередньо у веб-браузері, що дозволяє уникнути необхідності встановлення програмного забезпечення.
2. Автоматичні оновлення: Користувачам не потрібно думати про оновлення веб-додатків, оскільки вони автоматично оновлюються з централізованого сервера. Це забезпечує користувачам доступ до останніх версій програми без необхідності оновлення вручну.
3. Стандартизація: Всі користувачі отримують доступ до однієї і тієї ж версії веб-приложения, що дозволяє уникнути непорозумінь і несумісності між різними версіями.
4. Крос-платформенність: Веб-додатки розробляються з урахуванням сумісності з різними веб-браузерами та операційними системами. Це означає, що вони можуть бути відкриті з будь-якого пристрою або платформи, яка має веб-браузер.
5. Економічні переваги: Веб-додатки зменшують витрати як для бізнесу, так і для кінцевого користувача. Вони вимагають менше ресурсів, таких як робоча сила та обладнання, для їх експлуатації та підтримки.
6. Простота використання: Веб-додатки прості у використанні та не потребують спеціальних знань чи навичок. Це дозволяє користуватися ними широкому загалу аудиторії без обмежень.
7. Рентабельність: Веб-додатки є економічно вигідними, оскільки вони є більш доступними за класичні програмні рішення.

**Принцип-роботи вед-додатку**

Початок роботи відбувається від самого веб-додатку. Користувач створює запит, який повинен буде відправитися на веб-сервер за допомогою запиту в інтернет-браузері, або в самому веб-додатку.

Далі цей запит має направитися на закріплений за цим веб-додатком веб-сервер (центр керування). Після того як сервер отримав запит, він іде до бази даних для формування відповіді на запит користувача. Фінальним етапом йде відправка необхідних даних на Front-частину (веб-сервер) програми, а потім відображення користувачеві на дісплеї.

І так повторюється знову і знову, поки користувач створює запити у веб-застосунку. Хотілося б відзначити, що чим більше і складніше надходитимуть запити, тим довше буде надсилатися відповідь з сервера.

**Роль веб-додатків в інформаційній системі організації**

Web-додатки є важливою складовою інформаційної системи організації. Вони дозволяють організаціям забезпечувати доступ до інформації та послуг для клієнтів, співробітників та інших зацікавлених сторін. Web-додатки дозволяють організаціям збільшувати продуктивність та ефективність роботи, знижувати витрати на інформаційні технології та забезпечувати високий рівень безпеки даних.

Веб-додатки відіграють важливу роль у сучасних інформаційних системах організацій. Вони дозволяють ефективно взаємодіяти з користувачами, обмінюватися даними, зберігати, обробляти та аналізувати інформацію, а також забезпечувати доступ до різноманітних функцій та послуг через веб-браузер.

Одна з головних ролей веб-додатків в інформаційній системі організації - забезпечення швидкої та зручної взаємодії з користувачами. При створенні веб-додатків вони можуть бути розроблені таким чином, щоб вони були легкодоступними та зрозумілими для користувачів, незалежно від їх рівня технічної компетенції. Вони можуть містити інтуїтивний інтерфейс, тобто простим без застосування розуму, при цьому дозволяючи користувачам і взаємодіяти з системою без тріднощів.

Веб-додатки можуть використовуватись як для обміну даними між користувачами та системою, а також між різними користувачами. Це дуже корисно особливо в випадках, коли необхідно, щоб кілька користувачів повинні працювати з однією та іншою інформацією або співпрацювати в режимі реального часу.

Одне з основних переваг веб-додатків в інформаційній системі організації – це можливість зберігання, обробки та аналізу даних. Веб-додатки можуть дозволяти користувачам зберігати дані в централізованій базі даних, що дозволяє ефективно керувати даними та забезпечувати консистентність інформації. Додатково, веб-додатки можуть мати вбудовані аналітичні функції.

**Місце веб-додатків в інформаційній системі організації**

Web-додатки зазвичай використовують для обміну даними між користувачами та сервером, забезпечення доступу до інформації, виконання бізнес-операцій та багатьох інших функцій. Вони можуть бути використані у будь-якому секторі діяльності, включаючи фінанси, рекламу, логістику, медицину та інші. Web-додатки можуть використовуватися як для зовнішньої взаємодії з клієнтами та партнерами, так і для внутрішньої взаємодії між різними департаментами та співробітниками організації.

Веб-додатки мають важливе місце в сучасних інформаційних системах організацій. Вони забезпечують ряд різноманітних функцій, які роблять їх використанням інструментом для забезпечення ефективної роботи організацій.

По-перше, веб-додатки виключають організації безпечним та ефективним доступом до інформації. Вони можуть бути розроблені з інтуїтивним інтерфейсом, що дозволяє користувачам легко взаємодіяти з системою та отримувати необхідну інформацію. Веб-додатки можуть бути доступні з будь-якого місця та пристрою з підключенням до Інтернету, що дозволяє забезпечити мобільність та гнучкість у роботі з інформацією.

По-друге, веб-додатки забезпечують можливість зберігання, обробки та аналізу даних. Вони можуть мати централізовані бази даних, де інформація може бути збережена та оновлена. Це дозволяє забезпечити узгодженість даних та впорядкування в роботі інформації. Веб-додатки також можуть мати вбудовані функції аналітики, які допомагають організаціям аналізувати дані та отримувати цінні сайти для прийняття рішень.

По-третє, веб-додатки можуть бути використані для автоматизації різноманітних бізнес-процесів. Вони можуть включати різні функції, такі як обробка замовлень, керування клієнтськими відносинами

**Основні компоненти веб-додатку**

Основними компонентами веб-додатків є клієнтська сторона (frontend) та серверна сторона (backend). Клієнтська сторона включає в себе веб-браузер та інтерфейс користувача (API), який забезпечує взаємодію із сервером через HTTP-запити. Серверна сторона складається з веб-сервера, який оброблює HTTP-запити та відповідає на них, бази даних для зберігання даних та бізнес-логіки, яка оброблює запити користувачів.

**Переваги використання веб-додатків для організацій**

Одним із найбільших переваг використання веб-додатків є можливість доступу до даних та послуг з будь-якого місця та на будь-якому пристрої, яке має доступ до Інтернету. Крім того, веб-додатки дозволяють організаціям знижувати витрати на інформаційні технології та збільшувати продуктивність та ефективність роботи.

**Недоліки використання веб-додатків для організацій**

Одним із найбільших недоліків використання веб-додатків є залежність від Інтернету. Якщо Інтернет-з'єднання відсутнє або недостатньо стабільне, користувачі можуть мати проблеми з доступом до даних та послуг. Крім того, веб-додатки можуть бути більш повільними в порівнянні зі стандартними десктопними додатками, оскільки вони залежать від швидкості Інтернет-з'єднання та пропускної здатності серверів.

Ще одним недоліком є проблема безпеки. Веб-додатки можуть бути під ударом хакерів, які намагаються отримати несанкціонований доступ до конфіденційної інформації користувачів. Крім того, залежно від якості програмного забезпечення, веб-додатки можуть містити вразливості, які можуть бути використані хакерами для злої системи.

Нарешті, використання веб-додатків може бути обмежене з точки зору можливостей та функціональності. Деякі завдання можуть вимагати великої кількості ресурсів або просто неможливі для веб-додатків, що робить їх непридатними для деяких видів діяльності.

Всі ці фактори можуть зменшити ефективність веб-додатків у бізнесі та їх здатність задовольняти потреби користувачів. Тому, перед тим, як використовувати веб-додатки для бізнесу, необхідно уважно проаналізувати їх переваги та недоліки та забезпечити необхідну інфраструктуру та захист від можливих загроз.

**Види веб-додатків для органіізацій**

Веб-додатки для організацій можуть мати різноманітні призначення та функціональність. Основні види веб-додатків для організацій включають:

Корпоративний портал: Це веб-приложение, яке надає спільний доступ до різноманітної інформації та ресурсів усім співробітникам організації. Корпоративний портал може включати такі функції, як внутрішній чат, календар, систему управління документами, спільні проекти, обмін файлами та інші інструменти для співпраці та комунікації всередині організації.

Система управління відносинами з клієнтами (CRM): Цей тип веб-додатків допомагає організаціям керувати взаємодією з клієнтами. CRM-система надає функції для збору, аналізу та управління даними клієнтів, замовленнями, продажами, контактною інформацією та іншою важливою інформацією. Вона допомагає підвищити ефективність роботи з клієнтами, удосконалити продаж та підтримку клієнтів.

Система управління проектами (PM): Цей тип веб-додатків допомагає організаціям керувати та контролювати проекти. Система управління проектами надає інструменти для планування проектів, призначення завдань, відстеження прогресу, спілкування команди, управління ресурсами та витратами. Вона сприяє підвищенню продуктивності, організації роботи команди та досягненню поставлених цілей.

Інтранет - це веб-приложение, яке надає внутрішній доступ до інформації та ресурсів організації її співробітникам. Він може включати в себе внутрішні новини, оголошення, відділи та контакти, документи та шаблони, розклади роботи, процедури та політики, інформацію про внутрішні проекти та багато іншого. Інтранет допомагає забезпечити співпрацю між відділами, обмін знаннями, підвищити ефективність комунікації та зручний доступ до важливої інформації для всіх співробітників організації.

Система управління ресурсами підприємства (ERP): Цей тип веб-додатків допомагає організаціям керувати різними аспектами своєї діяльності, такими як фінанси, логістика, виробництво, кадри та інше. Система управління ресурсами підприємства надає централізовану базу даних та інструменти для автоматизації бізнес-процесів, планування ресурсів, забезпечення ефективного використання ресурсів та оптимізації операцій організації.

Електронна комерція (eCommerce): Цей вид веб-додатків дозволяє організаціям здійснювати продаж товарів чи послуг через Інтернет. Вони включають функції створення та управління веб-магазином, обробки платежів, управління складом, замовленнями та доставкою. Електронна комерція надає можливість організаціям розширити свій бізнес, залучити більше клієнтів.

Внутрішній портал співробітника: Це веб-приложение, призначене для особистого використання співробітниками організації. Він надає доступ до особистої інформації, а саме від розкладу роботи, оплати праці, відпусток, обліку робочої години, корпоративних новин та ресурсів. Внутрішній портал сприяє покращенню ефективності співробітників, самоорганізації та доступу до важливих внутрішніх ресурсів організації.

Аналітична система: Цей тип веб-додатків забезпечує організації інструментів для збирання, аналізу та візуалізації даних з різних джерел. Аналітична система допомагає здійснювати глибокий аналіз бізнес-даних, створювати звіти та візуалізації для прийняття керівництвом організації обґрунтованих рішень. Вона може включати функції бізнес-інтелекту (BI), аналітики даних, прогнозування та інші аналітичні інструменти.

Ці види веб-додатків для організацій представляють лише деякі з можливих варіантів. Залежно від потреб та специфіки організації, веб-додатки можуть бути настроєні та розроблені для виконання конкретних завдань та вимог.

## 1.2 Аналіз основних загроз та вразивостей Web-дотаків OWASP

OWASP TOP 10 є набором рекомендацій та керівництвом для розробників, тестувальників та адміністраторів веб-додатків, спрямованих на запобігання та виявлення основних загроз та вразливостей. Декларованою послугою OWASP TOP 10 є надання керівництва щодо визначення основних ризиків безпеки та рекомендації щодо захисту веб-додатків від цих ризиків.

OWASP TOP 10 пропонує наступні підходи та рекомендації для боротьби з основними загрозами та вразливістю:

Використання безпечного кодування: Розробники повинні використовувати безпечні практики кодування, такі як унікальні використання ненадійних даних у SQL-запитах (SQL-інкціонах) або веб-запитах (крос-сайтові скриптові атаки) та застосування механізмів захисту, таких як фільтрація та валідація вхідних даних.

Використання сильної аутентифікації та авторизації: Розробники повинні використовувати належні механізми аутентифікації та авторизації, такі як багаторівнева аутентифікація, використання правових ролей та дозволів, а також застосування принципів найменшого дозволу.

Застосування захисту на рівнях інфраструктури: адміністратор повинен керувати серверами та мережами з використанням належних заходів безпеки, таких як коректна конфігурація файлів, застосування оновлень та патчів для операційних систем та програмного забезпечення, використання SSL-шифрування та інші заходи.

Аудит безпеки та виявлення вразливостей: Здійснення регулярних аудитів безпеки веб-додатків може допомогти виявити ваші вразливості та вчасно вжити заходи щодо їх усунення. Ваш OWASP TOP 10 містить рекомендації щодо використання автоматизованих інструментів сканування вразливостей та тестування на проникнення, які можуть допомогти вирішити деякі проблеми з безпекою.

Захист від зловмисників: OWASP TOP 10 рекомендує використовувати заходи захисту від зловмисників, такі як захист від злому паролів (наприклад, вимагання складних паролів, обмеження кількості невдалих спроб входу), захист від атак на сесії, обмеження можливостей використання небезпечних функцій, таких як виконання видалених кодів (Віддалене виконання коду), та інші заходи.

Захист від витоку даних: OWASP TOP 10 наголошує на необхідності застосування заходів для запобігання витоку конфіденційної інформації, таких як валідація та фільтрація вихідних даних, захист від витоку даних через SQL-запити, використання захищених каналів комунікації та інші заходи.

Ефективний моніторинг та реагування на інциденти: OWASP TOP 10 рекомендує використовувати ефективні механізми моніторингу та реагування з можливістю безпеки інцидентів. Це може включати ведення журналів (реєстрацію) дій користувачів, моніторинг вразливостей, спостереження за активністю користувачів та автоматизованим реагуванням на огляд активності.

Неперервне оновлення та виправлення: OWASP TOP 10 регулярно наголошує на необхідності оновлення веб-додатків та виправлення вразливостей, виявлених у процесі моніторингу. Використання останніх версій фреймворків, бібліотек, платформ та операційних систем є основним заходом для забезпечення безпеки веб-додатків.

Безпека із захисту даних: OWASP TOP 10 рекомендує використовувати заходи захисту даних, такі як шифрування, хэшування, маскування, резервне копіювання даних та інше обладнання, яке може захистити конфіденційну інформацію від несанкціонованого доступу.

Навчання та освіта: OWASP TOP 10 підкреслює важливість навчання та освіти всіх відповідних для розробки, впровадження та реалізації веб-додаток. Закладання культури безпеки в командах розробників та впровадження практичних розробок з результатів безпеки можуть допомогти усунути багато наявних загроз та вразливостей уже на етапі розробки.

OWASP TOP 10 також активно співпрацює зі співтовариством розробників, без пековими експертами, вендорами та організаціями з метою підвищення обізнаності про загрози та невразливість веб-додатків та поширення кращих практичних засобів безпеки. Це включає проведення навчальних заходів, розробку документації, публікації статей та розповсюдження досліджень з безпеки веб-додатків.

Узагальнюючи, OWASP TOP 10 рекомендує комплексний підхід до захісту веб-додатків, включаючи захист від відомих загроз та вразливостей, таких як крос-сайтовий скриптінг, SQL-ін'єкції, крос-сайтові поділений доступ та інші. Це включає впровадження технічних заходів, таких як контроль введених даних, валідацію, автентифікацію та авторизацію, а також процесів моніторингу, оновлення та патчінгу.

На основі цього, розробники повинні розуміти та використовувати кращі практичні веб-додатки безпеки, такі як використання безпечних фреймворків та бібліотек, захист конфіденційних даних, резервування, використання безпечних налаштувань серверів та баз даних, тестування на вразливість та інші. Навчання та освіта всіх відповідних для розробки веб-додатків також є елементом захисту від загроз.

OWASP TOP 10 також рекомендує впровадження комплексних заходів захисту веб-додатків на всіх етапах їхнього життєвого циклу, включаючи планування, розробку, впровадження, експлуатацію та підтримку. Це включає такі дії, як аналіз ризиків, визначення та застосування заходів безпеки, аудит, моніторинг, виявлення та реагування на загрози та інші.

Загалом, OWASP TOP 10 є місцем документа, який визначає основні загрози та вразливі веб-додатків та дає рекомендації щодо їхнього захисту. За допомогою використання рекомендацій, наданих OWASP TOP 10, можна надати допомогу розробникам та організаціям у впровадженні заходів безпеки для захисту веб-додатків від відомих загроз та уразливостей. Це може включати впровадження механізмів фільтрації та валідації вхідних даних, використання захищених засобів налаштування комунікацій, безпечних параметрів аутентифікації та авторизації, регулярне оновлення веб-додатків та їх залежностей, використання також захищених налаштувань серверів та інфраструктури, а також навчання персоналу безпеки веб-додатків та змін. виявляти та реагувати на деякі загрози.

OWASP TOP 10 також відзначає важливість регулярного моніторингу та аудиту веб-додатків для виявлення нових загроз та вразливостей. Це може включати використання системи вторгнення, журналювання подій, аналіз вихідних кодів та тестування на вразливість. Ці заходи дозволено вчасно виявляти та реагувати за допомогою загрози, забезпечуючи високий рівень безпеки веб-додатків.

Крім того, OWASP TOP 10 наголошує на важливості взаємодії між розробниками, тестувальниками, адміністраторами системи та іншими стейкхолдерами з розширення співпраці, перевірки та виявлення невразливостей. Регулярні код-ревю та тестування на вразливості можуть допомогти вирішувати проблеми та вчасно їх виправити.

Узагальнюючи, OWASP TOP 10 надає комплексний підхід до захисту веб-додатків від найпоширеніших загроз та вразливостей. Використання рекомендацій, включених до цього списку, може допомогти розробникам та адміністраторам системи ефективно захистити ваші веб-додатки від відомих атак і знизити ризик їхньої компрометації. Подальші кроки можуть включати впровадження механізмів моніторингу та аналізу, регулярне оновлення заходів безпеки на основі нових загроз та вразливостей, а також щодо навчання персоналу кращих практичних веб-додатків безпеки.

Окрім цього, OWASP TOP 10 також сприяє залученню співтовариства розробників та експертів з виявлення безпеки та вирішення невразливостей. Це може включати активну участь у програмах виявлення вразливостей, загального вивчення та обговорення нових загроз та заходів захисту, а також внесення вкладок до веб-документації та підтримки спільноти OWASP.

Однак важливо зауважити, що OWASP TOP 10 є документом, який постійно використовується, останні загрози та невразливість веб-додатків змінюються з часом. Тому розробники та адміністратори системи повинні постійно виконувати останнє оновлення OWASP TOP 10, вдосконалювати свої заходи безпеки та використовувати найкращі практики захисту веб-додатків від сучасних загроз та вразливостей.

Загалом, OWASP TOP 10 є місцем документа, який дає рекомендації щодо захисту веб-додатків від найпоширеніших загроз та вразливостей. Впровадження рекомендацій із цього списку в поєднанні з іншими кращими практиками безпеки може допомогти розробникам та адміністраторам системи забезпечити високий рівень безпеки своїх веб-додатків. Деякі способи, якими OWASP TOP 10 допоможуть боротися із загрозами та неприємностями, включають:

Повідомлення: OWASP TOP 10 ви отримаєте свідомість про найпоширеніші загрози та неприємності веб-додатків серед розробників, адміністраторів та інших зацікавлених сторінок. Це може допомогти підвищити рівень важливості та розуміння безпеки веб-додатків, а також заохотити використання кращих практичних засобів безпеки.

Реалізація заходів безпеки: OWASP TOP 10 містить рекомендації щодо конкретних заходів безпеки, таких як валідація введених даних, використання безпечних бібліотек, налаштування правого доступу, контроль введення/виведення даних та багато іншого. Розробники та адміністратори можуть використовувати ці рекомендації для впровадження відповідних заходів безпеки у своїх веб-додатках.

Перевірка безпеки: OWASP TOP 10 надає розробникам та адміністраторам можливість перевірити ваші веб-додатки за наявності вразливостей, які входять до списку OWASP TOP 10. Це може допомогти вчасно визначити та виправити вказані проблеми безпеки.

Навчання: ряд OWASP TOP 10 містить рекомендації щодо навчання персоналу щодо безпеки веб-додатків. Це може включати організацію тренінгів, навчальних курсів, вебінарів та інших форм навчання, які допомагають розробникам та адміністраторам засвоїти навички безпечної розробки та адміністрування веб-додатків.

Загальні принципи безпеки: OWASP TOP 10 сприяння впровадженню загальних принципів безпеки в розробку та адміністрування веб-додаток, таких як найменшого принципу доступу, захист від введення користувача, автентифікація та авторизація, захист від крос-сайтового скриптінгу (XSS) та крос-сайтового розділу даних (XSRF/CSRF), шифрування та інше.

Актуалізація: OWASP TOP 10 послідовно оновлювався з урахуванням нових загроз та вразливостей, які працюють у сучасних веб-додатках. Це забезпечує актуальність рекомендацій та заходів безпеки, що відповідають сучасним загрозам та вимогам безпеки.

Співпраця: OWASP TOP 10 сприяння співпраці та взаємодії між розробниками, адміністраторами, тестувальниками безпеки, експертами з безпеки та іншими зацікавленими сторонами для спільного розуміння, виявлення та вирішення проблем безпеки веб-додатків.

Загалом, OWASP TOP 10 надає важливі рекомендації та принципи безпеки, які можуть допомогти розробникам та адміністраторам забезпечити високий рівень захисту веб-додатків від найпоширеніших загроз та вразливостей. Проте варто відзначити, що OWASP TOP 10 є лише одним інструментом в арсеналі безпекових заходів, і важливо використовувати його в поєднанні з іншими методами та підходами для забезпечення безпеки веб-додатків. Для успішного застосування рекомендацій OWASP TOP 10 розробники та адміністратори повинні виявляти та обробляти контекстні особливості своїх веб-додаток, такі як тип додатка, рівень конфіденційності даних, особливості архітектури та технічних рішень, використаних у додатку.

Повний додаток TOP 10 надає більше звітної інформації про шкіру з десяти загроз та вразливостей, рекомендації щодо виявлення, запобігання та вирішення цих проблем, а також додаткові ресурси, які можуть бути використані для поглибленого вивчення теми безпеки веб-додатків.

без того, OWASP TOP 10 взаємодіє з іншими проектами та ресурсами OWASP, такими як OWASP Testing Guide, OWASP Secure Coding Practices, OWASP Cheat Sheets та інші, що надає збалансований та комплексний підхід до безпечних веб-додатків.

Загалом, OWASP TOP 10 є кількістю ресурсів, які розробникам та адміністраторам виявляють, захищають та виправляють загрози та вразливість веб-додатків. Він стимулює впровадження найкращих практичних заходів безпеки та підвищення рівня захисту веб-додатків від виявлених загроз. Проте, варто пам’ятати, що безпека веб-додатків є постійним процесом, який вимагає постійного та вдосконалення заходів безпеки відповідно до оновлення ландшафту загроз та розвитку технологій.

## 1.3 Аналіз загальних методів та загальних веб-ресурсів та аналіз ринку рішень WAF

Найкращі веб-програми брендмауерів у 2023 році.

Брандмауер веб-сайту Sucuri

Він пропонує захист від хакерів, які намагаються використати топ-10 уразливостей OWASP, включаючи SQLi, XSS і CSRF.

Він також включає пом’якшення атак Distribution Denial of Service (DDoS) за підтримки постійного моніторингу. Sucuri Website Firewall **перехоплює та перевіряє всі вхідні** запити HTTP/HTTPS сайту.

Sucuri пропонує захист від шкідливих трафіків і має особливу інтеграцію з WordPress. Хоча він не пропонує спеціальних правил, він має політику швидкого реагування на **вразливості нульового дня**. Щойно вразливість стає загальнодоступною, інженери Sucuri виправляють ваше середовище, щоб блокувати атаки, які намагаються використати цю вразливість.

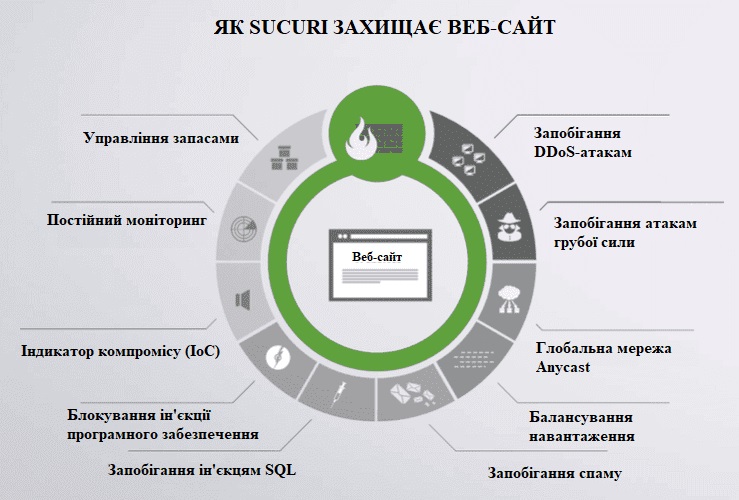


Рис. 1.1. Способи захисту веб-сайтів від Sucuri

Prophaze WAF

[Prophaze WAF 3.0](https://prophaze.com/products/cloud-waf/) надає захист веб-додатків за допомогою справжнього WAF/WAAP/Bot/DDoS API Security Solution, яке повністю створено на [Kubernetes](https://geekflare.com/kubernetes-and-docker-monitoring/) і має зворотну сумісність із усіма видами існуючих веб-служб і веб-додатків/API. Простота розгортання та висока якість взаємодії з користувачами завдяки розгортанням Prophaze WAF.

Prophaze — це перша розподілена архітектура WAF, що підтримує роботу з додатками, з меншою кількістю помилкових спрацьовувань, ніж будь-який інший постачальник рішень WAF.

WAF як послуга використовується хмарними провайдерами та Telcom, щоб пропонувати рішення своїм клієнтам. Prophaze доступний у вигляді хмарної WAF, локальної моделі WAF, разом із контролером Cloud Native Kubernetes Ingress для розгортання у вузлі Kubernetes.

AppTrana

[AppTrana](https://www.indusface.com/products/application-security/web-application-firewall/) поєднує сканування, повністю керовані брандмауери веб-додатків, CDN і служби моніторингу в одному рішенні. Він виявляє загрози на прикладному рівні, включаючи OWASP Top 10 і Zero-Day уразливості, прискорює веб-активи та захищає від експлойтів, а також надає керовані правила на постійній основі, щоб не відставати від нових ризиків і векторів загроз.

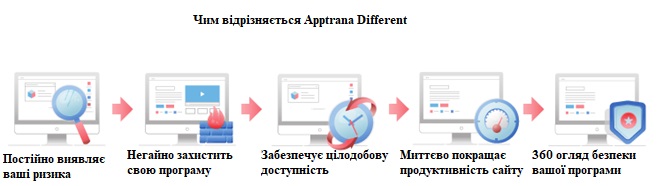


Рис. 1.2. Обобливості [AppTrana](https://www.indusface.com/products/application-security/web-application-firewall/)

Моніторинг у режимі реального часу також захищає веб-додатки від DDoS- і BOT-атак.

AppTrana зосереджений на перевірці наразливостей і захисту від SQL-інекцій, і має можливість інтеграції з різними платформами та API.

Що робить його корисним для малого та великого бізнесу, так це те, що WAF не тільки виправляє вразливості за допомогою синхронізації сканування веб-додатків, але також відстежує дії хакерів у додатку, щоб вивчати нові моделі атак і способи їх виявлення та захисту від них.

Cloudflare WAF

Коли справа доходить до порівняння брандмауера веб-додатків, корисною функцією є колективний інтелект Cloudflare. За винятком захисту OWASP Top 10 і користувацьких правил, цей WAF передбачає надсилання користувацьких правил усім клієнтам, якщо потрібно. По суті, це означає, що ваш веб-сайт також отримує інформацію про безпеку з інших сайтів.

По суті, це означає, що ваш веб-сайт також отримує інформацію про безпеку з інших сайтів.

Cloudflare WAF пропонує захист від широкого спектру атак і має безкоштовний тарифний план, а також можливості CDN і API-інтеграції.

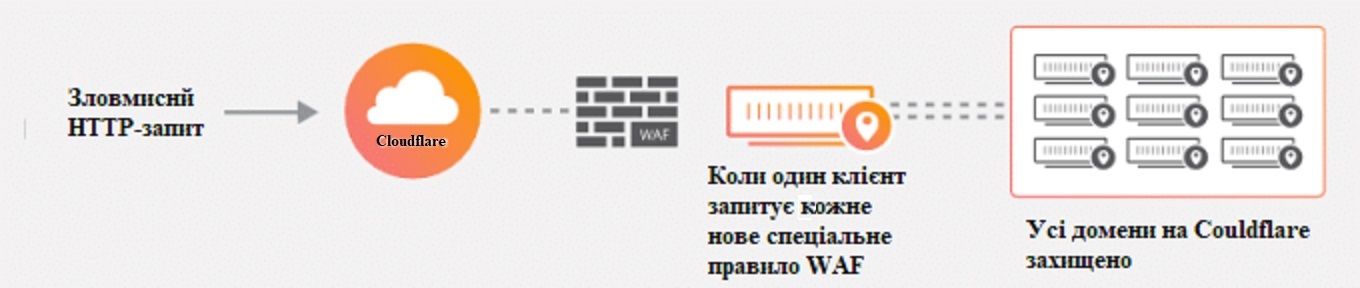
[Cloudflare](https://geekflare.com/cloudflare-implementation/) стверджує, що підтримує мільйон доменів і, отже, має багато даних про розвідку безпеки та те, як це може вплинути на бізнес та/або його клієнтів. 

Рис. 1.3. [Cloudflare](https://geekflare.com/cloudflare-implementation/) принцип захисту та роботи

AWS WAF

Amazon Web Services (AWS) є платною послугою тому потрібно платити за те, що використовуєте послуги [WAF](https://aws.amazon.com/waf/). Він блокує всі стандартні атаки рівня 7, які підривають безпеку або доступність програми.

Переваги цього WAF включають фільтрацію трафіку (на основі IP-адрес, заголовків HTTP, тіла HTTP або рядків URI), хмарну інтеграцію та підтримку AWS, а також аналітику практично в реальному часі.

AWS WAF надає можливість налаштування правил фільтрації трафіку та інтеграції з Amazon Web Services.

AWS WAF — ідеальне рішення для окремих осіб і компаній, які хочуть керувати своїм WAF за допомогою консолі керування AWS.

Akamai WAF

[Брандмауер веб-програм Kona](https://www.akamai.com/uk/en/resources/waf.jsp) від Akamai знижує ризик крадіжки даних, простоїв та інших порушень безпеки. Його моніторинг у реальному часі також забезпечує видимість подій безпеки, щоб адміністратори могли вжити відповідних заходів.

Він пропонує захист від [найпоширеніших веб-атак](https://geekflare.com/saas-web-vulnerability-scanner/), які використовують ін’єкції, міжсайтові сценарії та виконання шкідливих файлів. Однак захист від DDoS не входить до склада WAF і доступний як додаткова послуга.

Akamai WAF спрямований на захист від різних шарових атак і має можливість CDN-інтеграції. Також пропонує безліч інших рішень для підвищення продуктивності веб-сайтів, включаючи мережу доставки вмісту (CDN), прискорення Інтернету та мобільних пристроїв і керування трафіком.

Qualys WAF

[Брандмауер веб-програм Qualys](https://www.qualys.com/suite/web-application-firewall/) поєднує масштабованість і керованість у своєму наборі продуктів. Це хмарне рішення не тільки забезпечує захист від використання OWASP, але й може керувати ним за допомогою однієї консолі, яка також підтримує сканування веб-додатків і віртуальних машин.

Qualys WAF також інтегровано з рішеннями для сканування веб-додатків, щоб знаходити вразливості та виправляти їх, припиняючи атаки.

Він доступний на Amazon Web Services (AWS) Marketplace і розгортається як для **публічних, так і для приватних хмарних** веб-додатків. Крім того, він пропонує перевірку працездатності веб-додатків і балансування навантаження на сервер для підвищення доступності та продуктивності.

WAF має важливе значення для будь-якого онлайн-бізнесу для **захисту від онлайн-загроз у реальному часі** для безпеки бізнесу та клієнтів. Я сподіваюся, що наведений вище список брандмауерів веб-програм допоможе вам вибрати веб-програми.

True Shield WAF

[Брандмауер веб-додатків True Shield](https://geekflare.com/recommends/sitelock-waf/) дозволяє швидко та легко налаштувати службу WAF. Ви можете легко налаштувати його протягом 5 хвилин після виклику SiteLock. Це служба CDN, яка дозволяє відвідувачам використовувати сайт на 50% швидше, ніж інші.

True Shield також постачається із захистом від пошукової оптимізації (SEO), щоб захистити ваші пошукові зусилля від шкідливих програм. Таким чином, пошукові системи не знаходять шкідливе програмне забезпечення на вашому сайті; тому не блокуватиме його. Крім того, він дуже точний і захищає вас від кібератак із точністю 99,99%.

True Shield WAF забезпечує безпеку веб-додатків і захист від DDoS та має інтеграцію з SiteLock.

F5 Advanced WAF

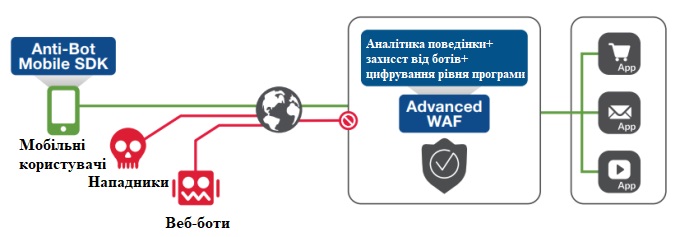
[F5 Advanced Web Firewall Protection](https://www.f5.com/products/security/advanced-waf)  — згідно дослідження вони стверджують, що він може виявляти та захищати від багатьох атак, які не вдається багатьом іншим WAF. Крім того, він поєднує машинне навчання, щоб допомогти захистити ваш веб-сайт і веб-додатки. 

Рис. 1.4. Анти-бот Mobile SDK принцип роботи по захисту данних

Це анти-бот Mobile SDK для захисту мобільних програм від веб-атак за допомогою аналізу поведінки. Він має шифрування даних у браузері для захисту від зловмисного програмного забезпечення, що витягує дані, і захист протоколу REST/JSON, XML, GWT API.

F5 WAF — брандмауер призначений для захисту веб-сайту від різноманітних атак. Завдяки механізму захисту від зловмисного програмного забезпечення та кібератак наступного покоління це досить пристойна служба WAF.

Wallarm

[Розширений хмарний WAF](https://wallarm.com/products/advanced-cloud-native-waf) захищає ваші веб-програми від XSS, XXE, SQL Injections, RCE та інших загроз OWASP. Це повністю автоматизований сервіс, який не потребує налаштування вручну.

Це надійний сервіс із швидкими та надійними вузлами фільтрації. Він пропонує підтримку сучасного стеку технологій, як-от Docker, Kubernetes і WebSockets, якими додатково керує ланцюжок інструментів DevOps. Він також використовує машинне навчання для блокування атак із захистом від загроз у реальному часі та різними варіантами розгортання.

Wallarm також пропонує захист від широкого спектру атак, включаючи захист API, і має можливості API-інтеграції.

Імперва WAF

[Imperva](https://www.imperva.com/products/web-application-firewall-waf/) — брандмауер для веб-програм, який аналізує та перевіряє запити до вашої програми та блокує атаки. Він захищає програми в хмарі та локально. Завдяки відмінним політикам безпеки та управлінню ви можете безпечно перенести свої програми з повним захистом.

Він можете розгорнути Imperva в AWS і Azure, а також у Cloud WAF або локально. Таким чином, розгортання є гнучким і відповідає потребам користувача з певним рівнем обслуговування та безпеки.

Imperva захищає від таких критичних загроз, як міжсайтовий сценарій, [впровадження SQL](https://geekflare.com/find-sql-injection/), доступ до ресурсів, віддалене включення файлів, автоматичні топ-10 або топ-20 загроз та інші загрози OWASP. Їхня дослідницька група завжди стежить за новими загрозами та відповідно оновлює правила. Крім того, він використовує графічні звіти, щоб ви могли легко зрозуміти стан безпеки вашої веб-програми.

Imperva використовує динамічну перевірку програми для виявлення атак шляхом аналізу каталогів програми, URL-адрес і введених користувачами даних. Потім він мінімізує помилкові спрацьовування за допомогою корельованої перевірки атак шляхом дослідження загальних порушень у програмі. Обидва вони об’єднані для захисту та блокування будь-яких атак на вашу програму. Imperva WAF забезпечує захист веб-додатків і захист від DDoS і може інтегруватися з Imperva.

Підведення

WAF має важливе значення для будь-якого онлайн-бізнесу для захисту від онлайн-загроз у реальному часі для безпеки бізнесу та клієнтів. На основі інформації можна зробити кілька висновків:

1.Цінова політика різних веб-брендмауерів розрізняється. Деякі постачальники пропонують безкоштовні тарифи, які можуть бути корисними для невеликих проектів або випробувань, а інші мають платні плани з додатковими функціями та обсягами використання.

2.Кожен веб-брендмауер має свої особливості та функціональність. Наприклад, деякі спеціалізуються на захисті від конкретних видів атак, таких як DDoS або SQL-інтеграції, тоді як інші пропонують широкий спектр захисту від різноманітних загроз.

3.Інтеграція також змінюється від постачальника до постачальника. Деякі веб-брендмауери мають спеціалізовані інтеграції з платформами, наприклад WordPress або CDN-системи, а інші надають API-інтерфейси для зручної інтеграції з природним середовищем.

4.Важливо скористатися потребами вашого веб-сайту або додатком при виборі веб-брендмауера. Оцініть, які конкретні функції та рівень захисту вам потрібні, а також розгляньте свої бюджетні обмеження.

Загальний висновок виникає в тому, що немає універсального найкращого веб-брандмауера. Вибір відповідає конкретним потребам і вашим вимогам проекту. Ретельно оцініть характеристики, ціни та можливості кожного веб-брендмауера, щоб знайти оптимальне рішення для вашої організації.

# 2. ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ WEB-ДОДАТКІВ ЗА ДОПОМОГОЮ РІШЕННЯ BARRACUDA WAF

## 2.1 Аналіз методів та засобів захисту Baracuda WAF

Barracuda Web Application Firewall (WAF) є продуктом компанії Barracuda Networks, який забезпечує захист від уразливостей веб-додатків, таких як атаки на переповнення буфера, ін'єкції SQL, XSS тощо.

Архітектура Barracuda WAF базується на технології обробки поведінки користувачів та здатності розуміти логіку роботи веб-додатків. Блокуючи спроби несанкціонованого доступу до ресурсів додатків, Barracuda WAF розпізнає певні сценарії зловживання, що дозволяє

забезпечити високий рівень захисту веб-додатків.

Архітектура Barracuda WAF включає у собі різноманітні компоненти, такі як сенсори, модулі обробки, аналітики, управління конфігурацією та інші. Сенсори контролюють мережевий трафік, аналізують його на наявність уразливостей і здатні приймати рішення щодо блокування трафіку. Модулі обробки забезпечують фільтрацію трафіку, розпізнавання загроз та відповідність правилам безпеки. Аналітичні компоненти надають звіти про використання системи та виявлення загроз, а управління конфігурацією забезпечує адміністрування системи та налаштування правил безпеки.

Крім того, Barracuda WAF має можливість взаємодії з іншими компонентами мережевої інфраструктури, такими як балансувальники навантаження, мережеві комутатори та інші.

Важливою особливістю архітектури Barracuda WAF є підтримка віртуалізації, що дозволяє запускати кілька віртуальних екземплярів на одному фізичному сервері. Це дозволяє підвищити ефективність використання обладнання та забезпечити високу гнучкість та масштабованість системи.

Одним з ключових елементів архітектури Barracuda WAF є його здатність до автоматичного оновлення, що забезпечує постійне оновлення правил безпеки та захист від нових загроз. Це забезпечує високий рівень захисту веб-додатків та зменшує ризик виникнення критичних проблем із безпекою.

Загалом архітектура Barracuda WAF є добре збалансованою та підтримує високий рівень безпеки для веб-додатків. Багато компаній обирають цей продукт для захисту своїх веб-додатків від широкого спектру уразливостей та загроз, що дозволяє підвищити рівень захисту та знизити ризик виникнення проблем із безпекою.

Крім того, Barracuda WAF має ряд додаткових функцій, які роблять його одним з найбільш повних та розширених продуктів з ринку. Наприклад, він має функцію захисту від DDoS-атак, яка дозволяє захистити веб-додатки від різноманітних атак, спрямованих на забезпечення перевантаження сервера.

Також важливою є функція захисту від витоку даних, яка забезпечує безпеку конфіденційної інформації, такої як паролі, номери кредитних карток та інші особисті дані користувачів.

Іншою корисною функцією є можливість моніторингу діяльності веб-додатків, що дозволяє виявляти та усувати проблеми з безпекою та вразливістю додатків, що покращує загальний рівень безпеки веб-сайту.

Нарешті, Barracuda WAF має інтуїтивно зрозумілий інтерфейс та детальну документацію, що спрощує його використання та налаштування.

Взагалі, Barracuda WAF є високопродуктивним та надійним рішенням для захисту веб-додатків від різноманітних загроз. Він має багато корисних функцій та можливостей, що роблять його одним із найкращих продуктів з ринку. Якщо ви шукаєте надійний та ефективний спосіб захисту свого веб-сайту, Barracuda WAF є одним з найкращих виборів.

Крім того, Barracuda WAF є простим у використанні та налаштуванні, що дозволяє забезпечити безпеку веб-додатків навіть для користувачів без спеціалізованого знання з цієї області.

Одним із головних переваг Barracuda WAF є його здатність виявляти нові загрози та атаки на ранніх стадіях з використанням технології Advanced Threat Detection. Це дозволяє забезпечити високий рівень захисту веб-додатків навіть від невідомих загроз та нових типів атак.

Крім того, Barracuda WAF підтримує інтеграцію з різноманітними сервісами та додатками, такими як Amazon Web Services, Microsoft Azure, Google Cloud Platform та інші, що дозволяє легко використовувати його в різних середовищах та з різними платформами.

Загалом, Barracuda WAF є одним із найкращих рішень для захисту веб-додатків від різноманітних загроз та атак. Він має високу продуктивність, багато корисних функцій та можливостей, що роблять його ідеальним вибором для бізнесів та організацій, які шукають надійний та ефективний спосіб захисту своїх веб-додатків.

Крім того, Barracuda WAF підтримує різноманітні методи захисту, такі як захист від DDoS-атак, SQL ін'єкцій, XSS атак та інших. Також він надає можливість налаштовувати правила доступу для різних груп користувачів, що дозволяє додатково збільшити рівень безпеки веб-додатків.

Одним із значущих переваг Barracuda WAF є можливість адаптації до специфічних потреб та вимог різних організацій. Наприклад, його можна настроїти для роботи зі специфічними додатками, а також для відповіді на конкретні потреби щодо безпеки та управління доступом.

Крім того, Barracuda WAF має інтуїтивно зрозумілий інтерфейс, що дозволяє легко налаштовувати та керувати всіма функціями та параметрами системи. Також, Barracuda WAF забезпечує високий рівень доступності та надійності, завдяки використанню технологій забезпечення відмовостійкості та резервування.

Загалом, Barracuda WAF є потужним та надійним рішенням для захисту веб-додатків, яке надає широкий спектр функцій та можливостей для забезпечення безпеки та доступності веб-додатків. Це рішення дозволяє знизити ризики порушення безпеки веб-додатків та забезпечує високий рівень захисту від різних типів загроз та атак.

Однією з ключових складових архітектури Barracuda WAF є його розподілена структура. Розподілена структура означає, що функції захисту від веб-атак розподілені між різними компонентами системи, що працюють разом для забезпечення безпеки веб-додатків.

**Схема архітектури Barracuda WAF складається з наступних компонентів:**

Клієнтський браузер - це веб-браузер, який використовується користувачем для отримання доступу до веб-додатків.

Веб-сервер - це сервер, на якому розміщені веб-додатки, з якими працює користувач.

Barracuda WAF - це проміжний рівень, який розміщується між клієнтським браузером та веб-сервером. Він фільтрує вхідний трафік, що надходить до веб-додатків, та застосовує правила безпеки для запобігання веб-атак.

База даних - це джерело даних, що використовується веб-прикладами для зберігання та обробки інформації.

Кожен з цих компонентів виконує свої функції, що дозволяє системі Barracuda WAF забезпечувати захист веб-додатків від різних типів веб-атак.

Для забезпечення високої доступності та надійності, архітектура Barracuda WAF також включає резервне копіювання компонентів та використання технологій забезпечення відмовостійкості.

Крім того, архітектура Barracuda WAF включає різні типи фільтрів, які допомагають виявляти та запобігати різним типам веб-атак. До таких фільтрів можуть належати:

Фільтри входу - ці фільтри перевіряють вхідні дані, які передаються до веб-додатку, і переконуються, що вони не містять вредних скриптів або коду.

Фільтри виходу - ці фільтри перевіряють вихідні дані, які надсилаються користувачеві, і переконуються, що вони не містять шкідливих скриптів або коду.

Фільтри URL - ці фільтри перевіряють URL-адреси, які користувач використовує для отримання доступу до веб-додатків, і упевнюються, що вони не містять вредних скриптів або коду.

Фільтри кукі - ці фільтри перевіряють куки, які надсилаються користувачем під час доступу до веб-додатків, і упевнюються, що вони не містять вредних даних.

Фільтри сесій - ці фільтри перевіряють ідентифікатори сесій, які використовують користувачі для доступу до веб-додатків, і упевнюються, що вони не містять вредних даних.

Фільтри перевірки прав - ці фільтри перевіряють дозволи користувача на доступ до різних частин веб-додатку та переконуються, що користувач має право на доступ до відповідних частин додатку.

Загалом, архітектура Barracuda WAF дозволяє забезпечувати безпеку веб-додатків за допомогою розподіленої структури, різноманітних фільтрів та застосування технологій забезпечення відмови.

доступності (DDoS) для запобігання атакам на рівні мережі. Крім того, вона також надає можливості для моніторингу та аналізу трафіку, які дозволяють виявляти та розуміти загрози безпеки, що допомагає в забезпеченні високого рівня безпеки веб-додатків.

Однією з ключових особливостей архітектури Barracuda WAF є її гнучкість та масштабованість. Вона може бути легко налаштована та пристосована до потреб конкретного веб-додатку, а також має можливість масштабування для забезпечення безпеки веб-додатків з високим трафіком та великою кількістю користувачів.

Крім того, Barracuda WAF надає додаткові функції безпеки, такі як захист від SQL-ін'єкцій, перехоплення сесій та запобігання крадіжки даних. Вона також має можливість інтегруватися з іншими системами безпеки, що дозволяє забезпечити комплексний підхід до захисту веб-додатків.

Взагалі, Barracuda WAF є потужним та надежним інструментом для захисту веб-додатків від різних видів веб-атак, що дозволяє забезпечувати безпеку користувачів та даних.

Що стосується схеми архітектури Barracuda WAF, вона складається з кількох ключових компонентів.Перш за все це апаратне забезпечення, яке забезпечує фізичну інфраструктуру для роботи WAF. Він може бути представлений у формі апліансу або віртуальної машини, що дозволяє розміщувати його у різних средах, включаючи хмарні.

Наступним компонентом є програмне забезпечення WAF, яке встановлюється на апаратному забезпеченні. Воно забезпечує захист веб-додатків та має низку функцій, включаючи детекцію та блокування атак, фільтрацію трафіку, контроль доступу та аудит.

Крім того, є компоненти для моніторингу та аналізу трафіку, які дозволяють виявляти та розуміти загрози безпеки, а також аналізувати поведінку користувачів та трафіку для виявлення аномалій. Ці компоненти забезпечують відповідну інформацію та статистику про трафік, що дозволяє операторам WAF вчасно реагувати на можливі загрози безпеці.

Крім того, Barracuda WAF має можливість інтегруватися з іншими системами безпеки, такими як системи ідентифікації та аутентифікації користувачів, системи управління інцидентами безпеки та системи моніторингу безпеки мережі. Це дозволяє забезпечувати комплексний підхід до захисту веб-додатків та мережі в цілому.

Отже, Barracuda WAF має потужну та масштабовану архітектуру, що забезпечує надійну захист веб-додатків та даних від різних видів веб-нападів та зловмисних дій. До переваг його архітектури належать:

Гнучкість: Barracuda WAF може бути розгорнутий як апліанс або віртуальна машина, що дозволяє розміщувати його в будь-якій среді, включаючи хмарні платформи.

Висока продуктивність: архітектура Barracuda WAF має високу продуктивність та може обробляти великі обсяги трафіку без втрати швидкості та якості обробки.

Безпека: забезпечення безпеки є ключовим компонентом архітектури Barracuda WAF. Він має широкий набір функцій для детекції та блокування атак, контролю доступу та аудиту, що дозволяє забезпечити надійну захист веб-додатків та даних.

Легкість управління: інтерфейс управління Barracuda WAF є досить простим та зрозумілим, що дозволяє легко налаштувати та керувати системою без необхідності високої кваліфікації технічного персоналу.

Інтеграція з іншими системами: Barracuda WAF має можливість інтеграції з іншими системами безпеки та мониторингу мережі, що дозволяє забезпечити комплексну захист веб-додатків та даних.

Таким чином, архітектура Barracuda WAF має досить широкий набір компонентів та функцій, що дозволяє забезпечити високу надійність та продуктивність, а також безпеку веб-додатків та даних.

Центральною частиною архітектури Barracuda WAF є механізм фільтрації вхідних запитів, що дозволяє перехоплювати запити до веб-додатків та аналізувати їх на наявність потенційних загроз безпеці. Блокування запитів, які містять вразливість, є однією з ключових функцій Barracuda WAF, яка дозволяє захистити веб-додатки від широкого спектру атак, включаючи SQL-ін'єкції, XSS-атаки та інші.

**До інших компонентів архітектури Barracuda WAF належить:**

Двигун захисту від вторгнень: цей компонент забезпечує виявлення та блокування атак на веб-додатки за допомогою навчання на основі машинного навчання, що дозволяє ідентифікувати нові загрози безпеці.

Контроль доступу: цей компонент дозволяє налаштовувати доступ користувачів до веб-додатків та ресурсів, що забезпечує контроль за привілеями користувачів та запобігає несанкціонованому доступу до конфіденційної інформації.

Журналування: цей компонент дозволяє збирати та аналізувати журнали активності, що дозволяє виявляти та аналізувати аномальну активність та вразливості.

Інтеграція з іншими системами: Barracuda WAF може бути інтегрований з іншими системами безпеки та мониторингу мережі, що дозволяє забезпечити комплексну захист веб-додатків та даних.

Відновлення після катастрофи: цей компонент дозволяє відновити налаштування та конфігурацію Barracuda WAF у разі виникнення катастрофічних ситуацій.

Масштабованість: архітектура Barracuda WAF забезпечує горизонтальну та вертикальну масштабованість, що дозволяє розширювати потужності системи залежно від потреб бізнесу.

Керування налаштуваннями: цей компонент дозволяє налаштовувати параметри захисту веб-додатків, забезпечує збереження та збирання конфігураційних даних та автоматичне оновлення налаштувань з метою забезпечення ефективної захисту.

Аналіз даних: Barracuda WAF дозволяє збирати, аналізувати та відображати дані про активність веб-додатків та потенційні загрози для безпеки, що дозволяє виявляти та вирішувати проблеми безпеки в реальному часі.

Модульність: архітектура Barracuda WAF дозволяє налаштовувати та конфігурувати окремі компоненти системи з метою забезпечення оптимальної продуктивності та ефективної захисту веб-додатків.

API-інтерфейс: Barracuda WAF має API-інтерфейс, що дозволяє налаштовувати та керувати системою за допомогою програмного інтерфейсу, що забезпечує більш гнучкий та зручний спосіб керування захистом веб-додатків.

Загалом, архітектура Barracuda WAF забезпечує комплексну захист веб-додатків та даних від різноманітних загроз безпеці та забезпечує можливості моніторингу та аналізу активності веб-додатків для виявлення потенційних проблем безпеки.

Barracuda WAF має багато переваг у порівнянні з іншими системами захисту веб-додатків. Одним із найбільш суттєвих переваг є його здатність виявляти та блокувати загрози в реальному часі. Це дозволяє уникнути виникнення потенційно небезпечних ситуацій, які можуть поставити під загрозу безпеку веб-додатків та даних.

Крім того, Barracuda WAF має досить простий інтерфейс користувача, що дозволяє виконувати налаштування та керування захистом веб-додатків з легкістю. Наявність API-інтерфейсу дозволяє більш гнучко та зручно налаштовувати систему забезпечення безпеки веб-додатків.

Крім того, Barracuda WAF забезпечує ефективну захист від різних типів атак, включаючи SQL-ін'єкції, кросс-сайт скриптінг, DDoS-атаки та інші. Це дозволяє підвищити рівень безпеки веб-додатків та даних, що зберігаються на серверах.

Узагальнюючи, Barracuda WAF є потужним та надежним засобом захисту веб-додатків від різних типів загроз безпеці. Завдяки своїй архітектурі система забезпечує гнучкість, масштабованість та ефективність, що дозволяє задовольняти потреби бізнесу будь-якого розміру та складності.

## 2.2 Захист Web-додатків за допомогою рішення WAF

Захист веб-додатків за функціональними можливотсями поділяються на основні та додаткові(допоміжні)

Існіє 15 основних функціональні можливості Barracuda (WAF), які допомагають забезпечити безпеку веб-додатків та захистити їх від різних видів атак:

1.Охорона веб-додатків від атак.

2.Виявлення та блокування SQL-ін'єкцій.

3.Виявлення та блокування кросс-сайт-скриптінг (XSS) атак.

4.Захист від уразливостей з використанням розширень веб-додатків.

5.Виявлення та блокування вбудованих зловмисниць.

6.Моніторинг та виявлення ненормальної активності.

7.Інтеграція з іншими системами безпеки.

8.Централізоване управління політиками безпеки.

9.Захист веб-додатків на рівні транспортного рівня.

10.Можливість налаштування власних правил фільтрації.

11.Блокування вторгнень на основі сигнатур.

12. Захист від DDoS-атак.

13.Виявлення та блокування небажаних ботів та сканерів.

14.Захист веб-сайту від уразливостей, пов'язаних з витоком інформації.

15.Можливість налаштування політик доступу для користувачів та груп.

Це основний список представляє основні функціональні можливості Barracuda (WAF), які допомагають забезпечити безпеку веб-додатків та захистити їх від різних видів атак.

Пояснення до основних функціональних можливостей Barracuda (WAF):

1.Охорона веб-додатків від атак: Barracuda (WAF) забезпечує захист веб-додатків шляхом виявлення та блокування різних видів атак, що загрожують їх безпеці.

2.Виявлення та блокування SQL-ін'єкцій: Barracuda (WAF) розпізнає спроби SQL-ін'єкцій, які можуть призвести до компрометації бази даних, та блокує їх, забезпечуючи цілісність та безпеку даних.

3.Виявлення та блокування кросс-сайт-скриптінг (XSS) атак: Barracuda (WAF) ідентифікує та перешкоджає атакам типу XSS, що можуть використовуватися для впровадження шкідливого коду на веб-сторінках та крадіжки інформації від користувачів.

4. Захист від уразливостей з використанням розширень веб-додатків: Barracuda (WAF) забезпечує захист від вразливостей, які можуть бути використані злодійниками через розширення та плагіні веб-додатків.

5.Виявлення та блокування вбудованих зловмисниць: Barracuda (WAF) розпізнає спроби вбудовування шкідливого коду або зловмисного вмісту у веб-додатки та перешкоджає їх виконанню.

6.Моніторинг та виявлення ненормальної активності: Barracuda (WAF) відстежує та аналізує веб-трафік, щоб виявляти ненормальну активність, що може бути пов'язана зі зловісними атаками або аномальною поведінкою користувачів.

7.Інтеграція з іншими системами безпеки: Barracuda (WAF) може інтегруватися з іншими системами безпеки, такими як системи моніторингу мережі, системи ідентифікації користувачів тощо, для спільної роботи та обміну інформацією для забезпечення комплексної захисту.

8.Централізоване управління політиками безпеки: Barracuda (WAF) надає централізований інтерфейс управління, який дозволяє налаштовувати та керувати політиками безпеки для всіх веб-додатків, що захищаються, з одного місця.

9. Захист веб-додатків на рівні транспортного рівня: Barracuda (WAF) забезпечує захист веб-додатків на рівні транспортного протоколу, такого як HTTP або HTTPS, шляхом фільтрації та перевірки трафіку на рівні мережі.

10.Можливість налаштування власних правил фільтрації: Barracuda (WAF) надає можливість налаштовувати власні правила фільтрації трафіку, що дозволяє забезпечити індивідуальні потреби та вимоги безпеки для конкретного веб-додатку.

11.Блокування вторгнень на основі сигнатур: Barracuda (WAF) використовує базу даних сигнатур для виявлення та блокування відомих атак та вторгнень на веб-додатки. Це дозволяє ефективно захищати систему від відомих загроз.

12.Захист від DDoS-атак: Barracuda (WAF) вміє виявляти та мінімізувати вплив розподілених атак з відмовою в обслуговуванні (DDoS), що спрямовані на веб-додатки. Це допомагає забезпечити неперервну роботу веб-сайту навіть за високого рівня трафіку.

13.Виявлення та блокування небажаних ботів та сканерів: Barracuda (WAF) має механізми для виявлення та блокування небажаних ботів та сканерів, які намагаються зламати або сканувати веб-додатки у злочинний спосіб. Це забезпечує додатковий захист від автоматизованих атак.

14.Захист веб-сайту від уразливостей, пов'язаних з витоком інформації: Barracuda (WAF) виявляє та блокує атаки, спрямовані на отримання несанкціонованого доступу до конфіденційної інформації веб-додатків, такої як витоки даних чи крадіжки особистої інформації користувачів.

15.Можливість налаштування політик доступу для користувачів та груп: Barracuda (WAF) дозволяє налаштовувати політики доступу для користувачів та груп, що дозволяє контролювати рівень доступу до веб-додатків та забезпечувати відповідну автентифікацію та авторизацію. Це дозволяє обмежити доступ до конфіденційної інформації.

Додаткові функціональні можливості Barracuda (WAF) включають:

1.Блокування вторгнень на основі сигнатур, що дозволяє ідентифікувати і блокувати відомі типи атак за певними характеристиками атаки.

2.Захист від DDoS-атак, що допомагає утримувати веб-додаток працездатним під великим навантаженням та запобігати перериванням обслуговування.

3.Виявлення та блокування небажаних ботів та сканерів, які можуть намагатися сканувати веб-додаток або виконувати небажані дії.

4.Захист веб-сайту від витоку інформації, що допомагає запобігти неправомірному доступу до конфіденційних даних.

5.Можливість налаштування політик доступу для користувачів та груп, що дозволяє контролювати, які користувачі мають доступ до веб-додатку та які дії вони можуть виконувати.

6.Відстеження та аналіз веб-трафіку для виявлення підозрілої активності, що допомагає ідентифікувати потенційні загрози та вчасно реагувати на них.

7.Захист від зламу акаунтів та підбору паролів, що допомагає утримувати користувачів від несанкціонованого доступу до системи.

8.Інтеграція з системами реєстрації та аутентифікації, що дозволяє використовувати існуючі методи аутентифікації для контроля доступу до веб-додатку.

9.Повідомлення та сповіщення про виявлення потенційної загрози, що дозволяє операторам системи швидко реагувати на потенційні атаки чи порушення безпеки.

10.Захист веб-додатків у режимі реальної години, що забезпечує миттєву реакцію на атаки та небажану активність, забезпечуючи безпеку в реальному часі.

11.Виявлення та блокування атак на протоколи передачі даних, такі як HTTP, HTTPS, FTP тощо, що допомагає захистити веб-додатки від атак, спрямованих на самі протоколи.

12.Захист від маніпулювання сесіями та крадіжки ідентифікаторів сесій, що дозволяє запобігти несанкціонованому доступу до активних сесій користувачів.

13.Можливість налаштування блокування IP-адрес і доменних імен, що дозволяє обмежити доступ до веб-додатку з певних мереж або від певних доменних імен.

14.Виявлення та блокування спроб переповнення буфера, що допомагає запобігти атакам, спрямованим на вразливості, пов'язані з некоректною обробкою даних.

15.Захист від атак, пов'язаних з управлінням файлами та завантаженням, що допомагає убезпечити веб-додатки від вразливостей, які можуть використовуватися для завантаження вредного вмісту.

Зазначені допоміжні функціональні можливості доповнюють основні функціональності Barracuda (WAF) та спрямовані на покращення безпеки веб-додатків та ефективне виявлення та блокування потенційних загроз.

**Різниця між основними та допоміжними функціональними можливостями Barracuda (WAF).**

Основні функціональні можливості Barracuda (WAF) включають функції, які є основою для захисту веб-додатків та забезпечення їх безпеки. Вони мають вирішальне значення для функціонування Barracuda WAF і надають ключовий рівень захисту. До основних функціональних можливостей можна віднести охорону веб-додатків від атак, виявлення та блокування SQL-ін'єкцій, крос-сайт-скриптінг атак, захист від вразливостей з використанням розширень веб-додатків, виявлення та блокування вбудованих злодій, моніторинг та виявлення ненормальної активності, інтеграцію з іншими системами безпеки, централізоване управління політиками безпеки, захист веб-додатків на рівні транспортного рівня та можливість налаштування власних правил фільтрації.

З іншого боку, допоміжні функціональні можливості Barracuda (WAF) доповнюють основні функції, надаючи додатковий рівень захисту та зручності управління. Вони можуть включати такі можливості, як блокування вторгнень на основі сигнатур, захист від DDoS-атак, виявлення та блокування небажаних ботів і сканерів, захист веб-сайту від уразливостей, пов'язаних з витоком інформації, можливість налаштування політик доступу для користувачів та груп, централізований журнал подій, захист від маніпулювання сесіями, інтеграцію із системами реєстрації та аутентифікації, повідомлення та сповіщення про виявлення потенційної загрози, захист від атак у режимі реальної години та інші допоміжні функції.

Допоміжні функціональні можливості Barracuda (WAF) додають додаткові кулі безпеки та зручності управління. Наприклад, блокування вторгнень на основі сигнатур дозволяє виявляти і блокувати відомі атаки за допомогою бази даних сигнатур. Це доповнює загальну захист веб-додатків та забезпечує ефективний контроль над відомими загрозами.

Захист від DDoS-атак виявляє та мінімізує вплив розподілених атак з відмовою в обслуговуванні, що спрямовані на веб-додатки. Ця функція дозволяє забезпечити неперервну роботу веб-сайту навіть за інтенсивного трафіку і запобігає відмовам в обслуговуванні.

Виявлення та блокування небажаних ботів та сканерів є ще однією допоміжною функцією, яка спрямована на захист веб-додатків. Вона дозволяє виявити та блокувати автоматизовані зловмисні програми, що намагаються сканувати або зламати веб-додатки.

Захист від уразливостей, пов'язаних з витоком інформації, є важливою функцією, що забезпечує безпеку конфіденційної інформації веб-додатків. Barracuda (WAF) виявляє та блокує атаки, спрямовані на отримання несанкціонованого доступу до цієї інформації, такі як витоки даних або крадіжки особистої інформації користувачів.

Нарешті, можливість налаштування політик доступу для користувачів та груп дозволяє забезпечити контрольову авторизацію та керувати рівнем доступу до веб-додатків. Ця допоміжна функція дозволяє встановлювати правила та обмеження для різних користувачів та груп, що забезпечує гнучкий контроль за безпекою системи.

Крім того, важливо зазначити, що визначення основних та допоміжних функціональних можливостей Barracuda (WAF) може варіюватися залежно від конкретної версії продукту або налаштувань. Розробники можуть додавати нові функції, покращувати існуючі або пристосовувати їх до потреб користувача.

Всі ці функціональні можливості спрямовані на захист веб-додатків від різноманітних загроз, що забезпечують контроль за безпекою системи та забезпечують безперебійну роботу веб-сайту. Об'єднання основних та допоміжних функціональних можливостей дозволяє користувачам ефективно захищати свої веб-додатки від потенційних атак та зловмисних дій.

Barracuda Web Application Firewall існує 3 способи встановлення :

Barracuda Web Application Firewall (WAF) може бути встановлена в декількох варіантах залежно від вимог вашої інфраструктури та переваг. Ось кілька поширених способів встановлення Barracuda WAF:

Фізичний пристрій Barracuda WAF може бути представлений у вигляді фізичного апаратного забезпечення, яке необхідно встановити у вашій мережі. Ви отримуєте фізичний пристрій, який підключається до вашої мережі та налаштовується за допомогою веб-інтерфейсу.

Віртуальна машина: Barracuda WAF також може бути представлений як образ віртуальної машини, який можна розгорнути на вашій віртуалізаційній платформі, такій як VMware або Hyper-V. Ви завантажуєте образ віртуальної машини, розгортаєте його у своєму середовищі та налаштовуєте за допомогою веб-інтерфейсу.

Хмарне рішення: Barracuda WAF також доступний як хмарне рішення. Ви можете підключитися до Barracuda Cloud Control, створити екземпляр WAF та налаштувати його для захисту ваших веб-застосунків. Хмарна установка забезпечує гнучкість та масштабованість, а також спрощує процес керування та оновлення.

При виборі способу встановлення важливо враховувати особливості вашої мережної інфраструктури, вимоги до продуктивності та доступності, а також можливості керування та обслуговування системи. Рекомендується звернутися до документації Barracuda та отримати консультацію у фахівців, щоб визначити найбільш вдалий варіант установки для ваших потреб.

Barracuda Web Application Firewall (WAF) фізичний пристрій інструкція встановлення

Встановлення фізичного пристрою Barracuda Web Application Firewall (WAF) включає кілька кроків.

Загальна процедура встановлення фізичного пристрою Barracuda WAF:

Підготовка фізичного пристрою: Розпакуйте обладнання, що поставляється, і переконайтеся, що у вас є всі необхідні компоненти, включаючи силовий кабель, мережевий кабель і монтажні кріплення (якщо застосовно). Встановіть пристрій у відповідне місце у стійці або на стіні, дотримуючись рекомендацій виробника.

Підключення до мережі: Підключіть один кінець мережного кабелю до порта пристрою Barracuda WAF та інший кінець до мережного комутатора або маршрутизатора у мережі. Переконайтеся, що у вас є відповідні параметри IP-адреси для зв'язку з пристроєм.

Увімкнення та налаштування: Підключіть силовий кабель до пристрою Barracuda WAF та підключіть його до джерела живлення. Увімкніть пристрій. Воно почне завантажуватися та ініціалізуватись. Під час цього процесу може знадобитися дотримуватися вказівок на дисплеї пристрою або документації, щоб виконати початкове налаштування, встановити паролі та встановити основні параметри.

Конфігурація через веб-інтерфейс: Після завершення ініціалізації можна отримати доступ до веб-інтерфейсу управління Barracuda WAF через веб-браузер. Введіть IP-адресу пристрою в адресному рядку браузера та увійдіть за допомогою облікових даних адміністратора. Потім дотримуйтеся вказівок веб-інтерфейсу для подальшого налаштування пристрою, включаючи мережі, політики безпеки та інші установки.

Зверніться до документації Barracuda та посібника користувача для отримання докладніших інструкцій та специфічних відомостей про модель фізичного пристрою Barracuda WAF.

Barracuda Web Application Firewall (WAF) віртуальна машина інструкція встановлення

Встановлення віртуальної машини Barracuda Web Application Firewall (WAF) включає кілька кроків.

Загальна процедура встановлення віртуальної машини Barracuda WAF:

Підготовка віртуалізаційної платформи: Переконайтеся, що у вас є підходяща віртуалізаційна платформа, така як VMware або Hyper-V, і вона правильно налаштована. Переконайтеся, що у вас достатньо ресурсів, таких як процесор, пам'ять і сховище, для розгортання віртуальної машини Barracuda WAF.

Завантаження образу віртуальної машини: Відвідайте офіційний веб-сайт Barracuda та завантажте образ віртуальної машини Barracuda WAF, який відповідає вашій віртуалізаційній платформі. Образ зазвичай надається у форматі OVA (Open Virtualization Appliance) або VMDK (Virtual Machine Disk).

Створення віртуальної машини: Запустіть віртуалізаційну платформу та створіть нову віртуальну машину. При створенні вкажіть параметри, такі як кількість процесорів, обсяг пам'яті, розмір диска та налаштування мережі, відповідно до рекомендацій Barracuda.

Встановлення образу віртуальної машини: Завантажте образ віртуальної машини Barracuda WAF у створену віртуальну машину. Це зазвичай робиться шляхом вказівки шляху до завантаженого образу віртуальної машини у налаштуваннях віртуалізаційної платформи.

Налаштування віртуальної машини: Запустіть віртуальну машину Barracuda WAF і виконайте початкове налаштування, включаючи встановлення паролів та основних параметрів. Інструкції з налаштування будуть надані у документації Barracuda.

Конфігурація через веб-інтерфейс: Після завершення початкового налаштування ви можете отримати доступ до веб-інтерфейсу керування Barracuda WAF через веб-браузер. Введіть IP-адресу віртуальної машини в адресному рядку браузера та увійдіть за допомогою облікових даних адміністратора. Потім дотримуйтеся вказівок веб-інтерфейсу для подальшого налаштування пристрою, включаючи мережі, політики безпеки та інші установки.

Зверніться до документації Barracuda та посібника користувача для отримання докладніших інструкцій та специфічних відомостей про розгортання віртуальної машини Barracuda WAF у вашій віртуалізаційній платформі.

Важливо також враховувати рекомендації та вимоги виробника щодо ресурсів, мережевої конфігурації та налаштувань безпеки для забезпечення оптимальної роботи та захисту вашої веб-програми.

Потрібно пам’ятати, що після встановлення Barracuda WAF віртуальна машина потребує регулярного оновлення та обслуговування, включаючи встановлення патчів безпеки та моніторинг системи. Потрібно переконатися, що користувач дотримуєтеся інструкцій та рекомендацій Barracuda щодо оновлення та обслуговування, щоб зберегти захищеність вашого середовища.

Якщо у користувача виникнуть труднощі або знадобиться допомога в установці та налаштуванні Barracuda WAF, рекомендується звернутися до служби підтримки Barracuda або консультантам, що спеціалізуються на продуктах Barracuda, які зможуть надати користувачу кваліфіковану допомогу.

Barracuda Web Application Firewall (WAF) Хмарне рішення початок використуовування

Встановлення Barracuda Web Application Firewall (WAF) у вигляді хмарного рішення включає такі кроки:

Зареєструйтесь у Barracuda Cloud Control: Перейдіть на офіційний веб-сайт Barracuda та зареєструйтесь у Barracuda Cloud Control. Створіть обліковий запис та підключіться до вашої організації.

Створіть екземпляр WAF: У Barracuda Cloud Control виберіть можливість створення нового екземпляра Barracuda WAF. Виберіть тип хмарного рішення і налаштуйте параметри відповідно до ваших потреб, таких як розташування даних, продуктивність та масштабованість.

Налаштуйте політики безпеки: Після створення екземпляра WAF вам буде надано доступ до веб-інтерфейсу управління Barracuda WAF через Barracuda Cloud Control. Увійдіть в інтерфейс і настройте політики безпеки для вашого веб-програми, включаючи фільтрацію трафіку, виявлення атак та інші налаштування безпеки.

Налаштуйте налаштування мережі: Вам також потрібно налаштувати налаштування мережі для хмарного екземпляра Barracuda WAF. Це може містити налаштування правил перенаправлення трафіку або налаштування DNS-записів для веб-програми.

Моніторинг та оновлення: Після завершення налаштування вам рекомендується моніторити роботу Barracuda WAF та оновлювати його регулярно для забезпечення захисту вашої веб-програми від нових загроз та вразливостей.

Barracuda Cloud Control надає широкий спектр можливостей для керування та налаштування вашого хмарного екземпляра Barracuda WAF. Посібник користувача та документація Barracuda містять докладніші інструкції та рекомендації щодо налаштування та використання Barracuda WAF у хмарному середовищі.

Як почати використовувати Barracuda Web Application Firewall у браузері?

Для використання Barracuda Web Application Firewall (WAF) у браузері клієнт можете отримати доступ до веб-інтерфейсу управління Barracuda WAF, який забезпечує керування та налаштування системи.

Загальна процедура:

Визначте IP-адресу або доменне ім'я Barracuda WAF, до якого ви хочете отримати доступ. Зазвичай цю інформацію надає адміністратор системи або можна знайти в документації Barracuda WAF.

Відкрийте веб-браузер і введіть IP-адресу або доменне ім'я Barracuda WAF в рядку адреси.

З'явиться сторінка входу. Введіть облікові дані адміністратора, які були надані, у поля для імені користувача та пароля.

Натисніть кнопку "Увійти" або натисніть клавішу "Enter", щоб увійти до веб-інтерфейсу керування Barracuda WAF.

Після успішної аутентифікації ви перенаправите на головну сторінку веб-інтерфейсу Barracuda WAF. Тут ви знайдете різні вкладки та налаштування, які дозволяють керувати системою, налаштовувати політики безпеки, моніторити трафік та багато іншого.

Використовуйте різні функції та налаштування веб-інтерфейсу Barracuda WAF відповідно до ваших потреб та цілей. Можливості включають фільтрацію трафіку, виявлення атак, управління SSL-сертифікатами, налаштування політик безпеки та багато іншого.

Важливо відзначити, що доступ до веб-інтерфейсу Barracuda WAF може бути наданий лише певним користувачам з відповідними привілеями. Якщо у вас немає прав доступу або потрібна допомога, зверніться до адміністратора системи або служби підтримки Barracuda для отримання відповідної допомоги та інструкцій.

## 2.3 Приклад використання Barracuda WAF

Початок роботи в Barracuda WAF починається з головної сторінки тут зображено головний інтерфейс.

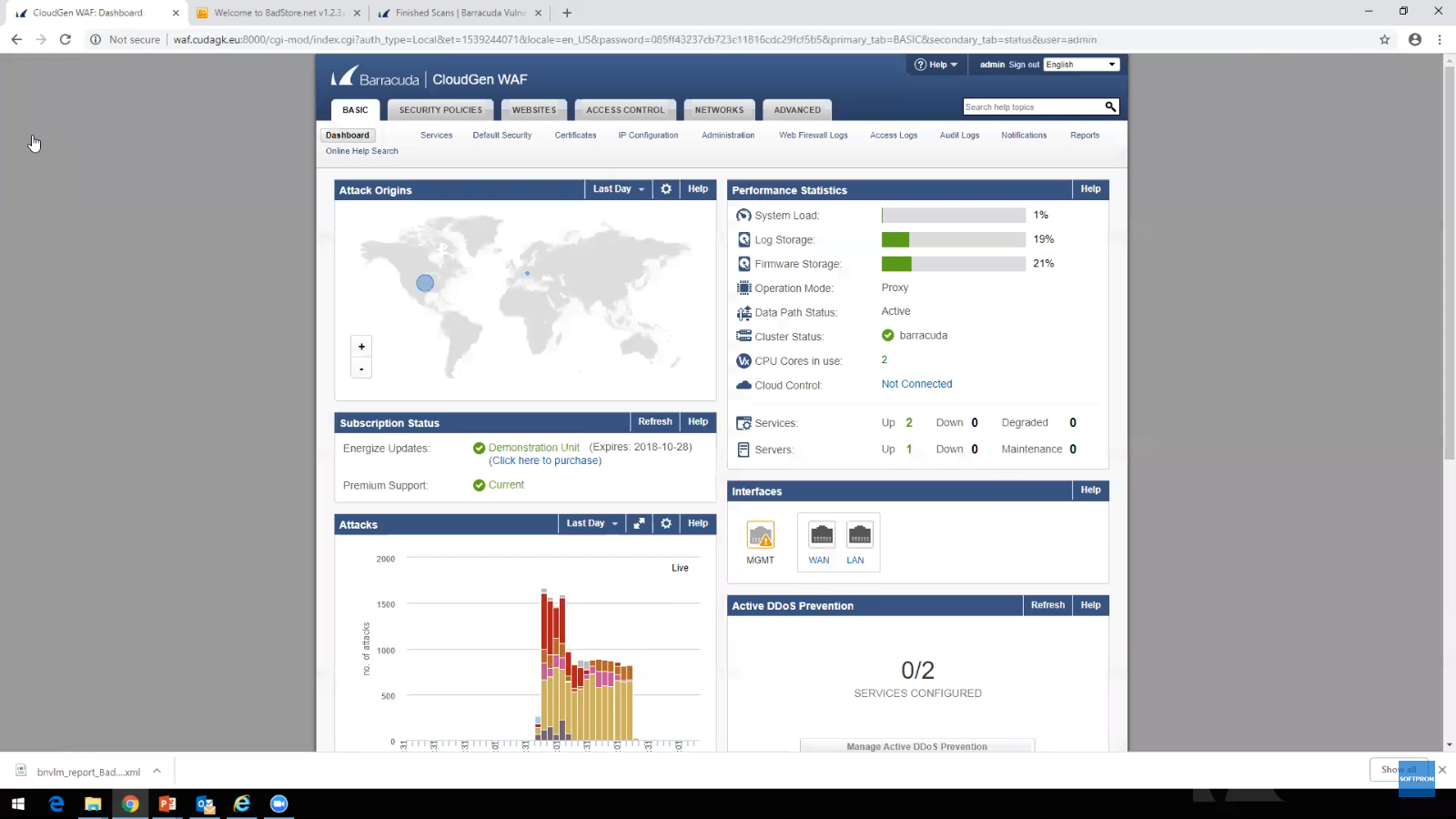


Рис. 2.1. Головна сторінка веб-додатка Barracuda WAF(1)

Витоки атаки, статистика продуктивності, атаки , інтерфейс та активне запобігання DDoS.

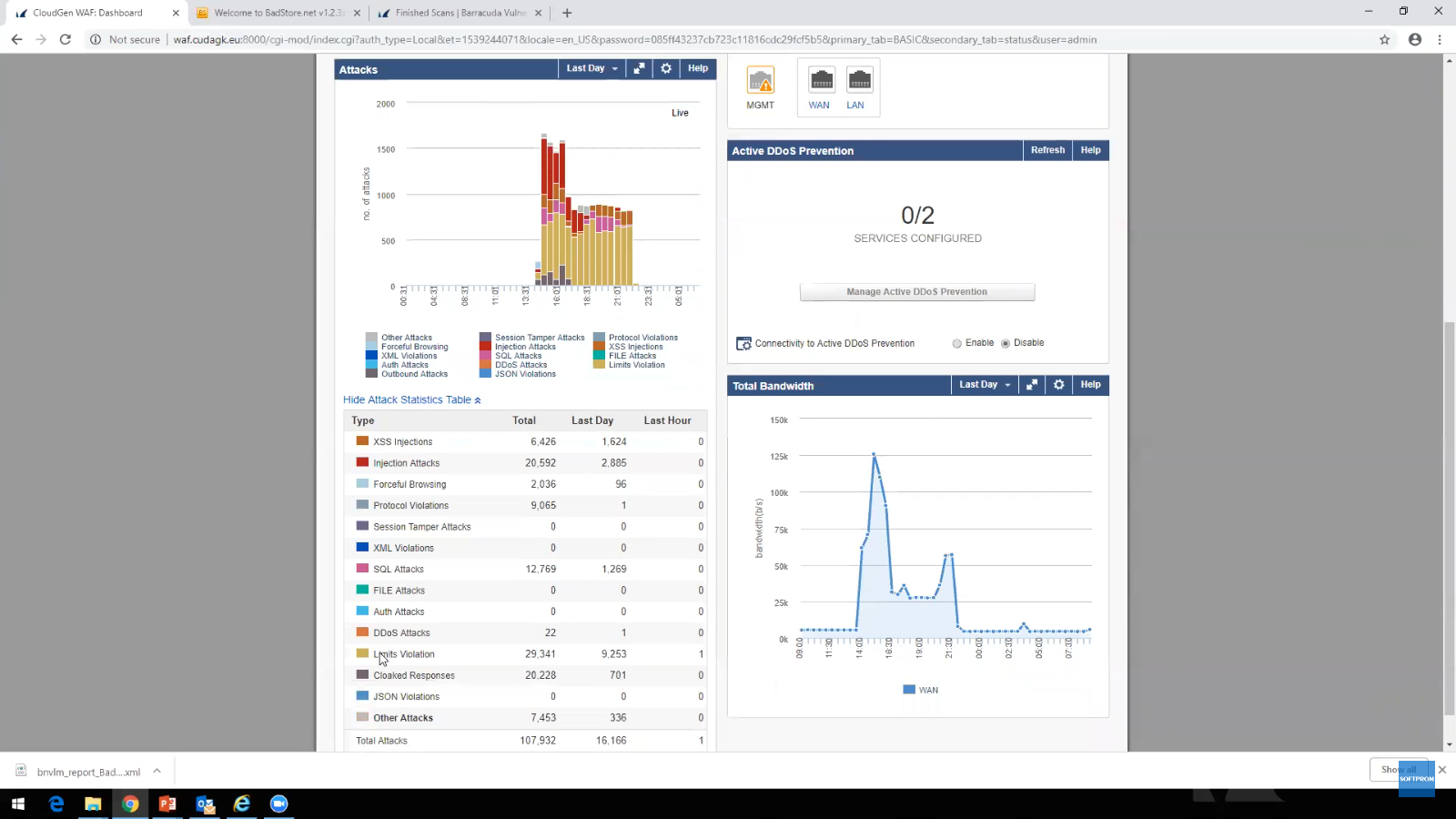


Рис. 2.2. Головна сторінка веб-додатка Barracuda WAF(2)

Графічне зображення статистики з типами атак , які були проведенні , відображення їх елементів , та графік загальної пропускної здатності.

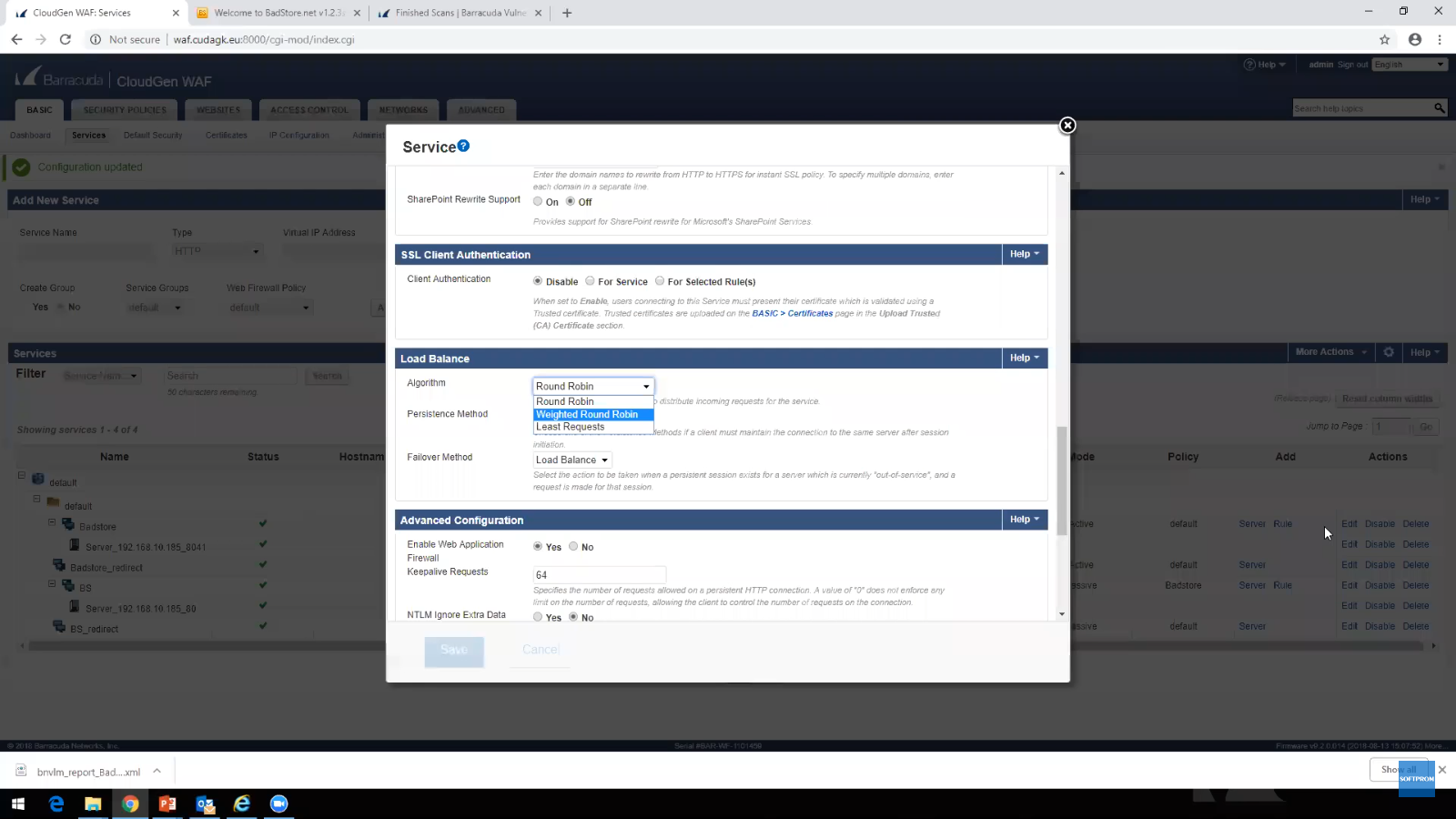


Рис. 2.3.Сторінка послуг, умови для створення власного сервісу

Перехід до послуг, вибір потрібних даних та створення власного сервісу. Після створення сервісу запуск його веб-сторінки та перевірка безпеки без захисту WAF.

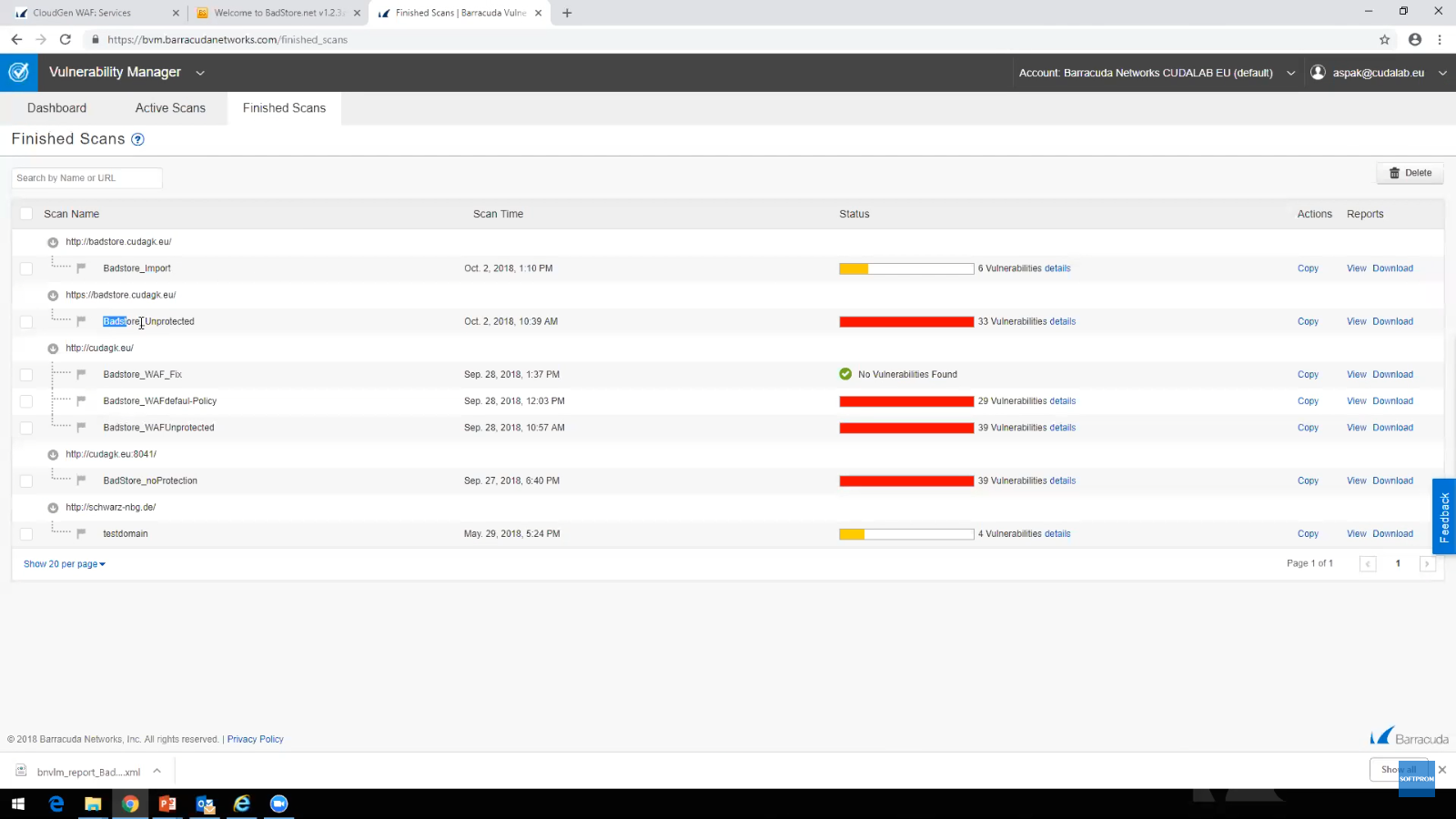


Рис. 2.4.Створена WEB-сторінка після перевірки без захисту WAF

Було виявлено 33 вразливості без захисту.

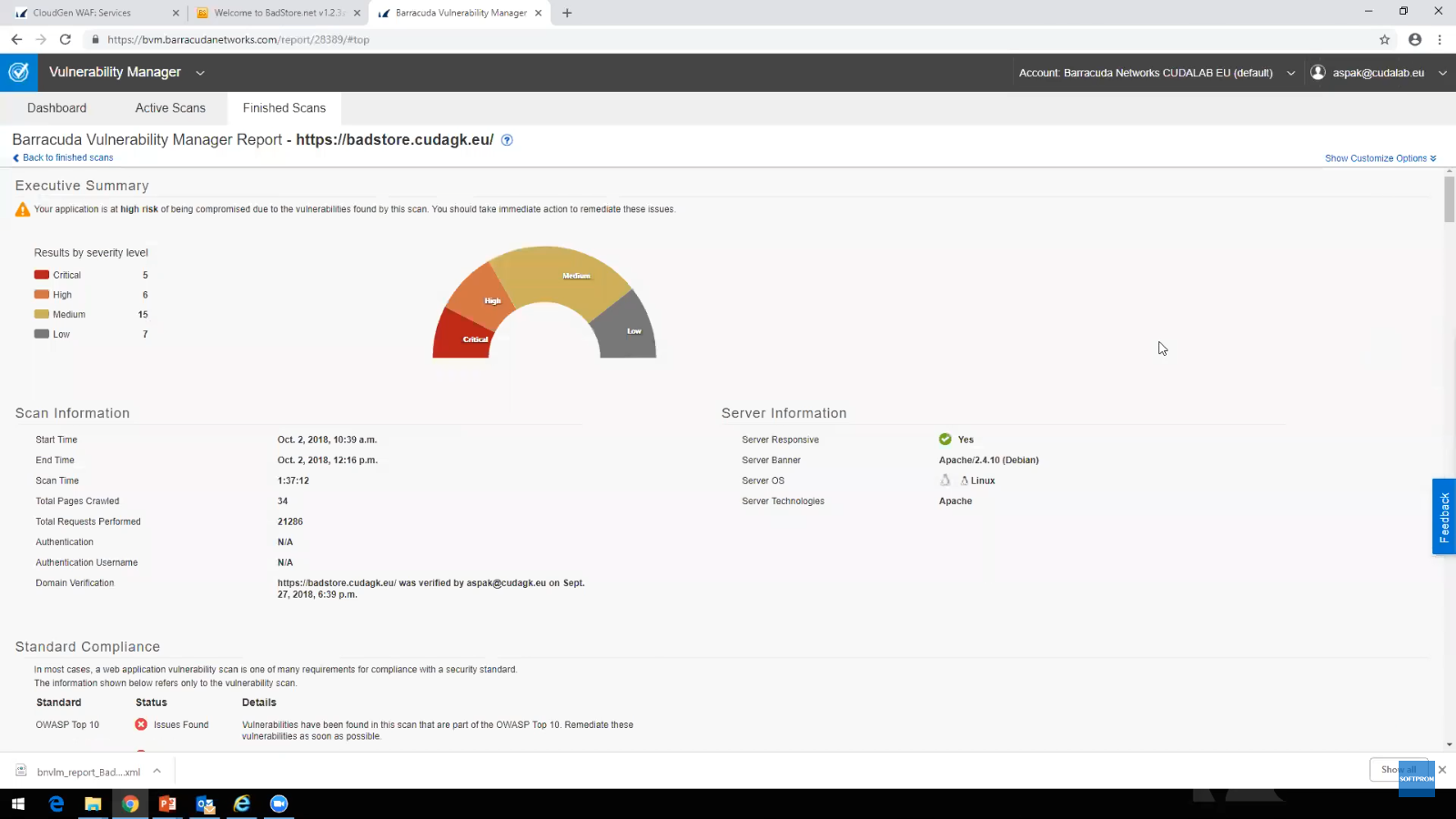


Рис. 2.5. Більш детальна інформація про виявленні вразливості

Надання детального опису 33 уразливостей та їх використання (детальний опис додається).

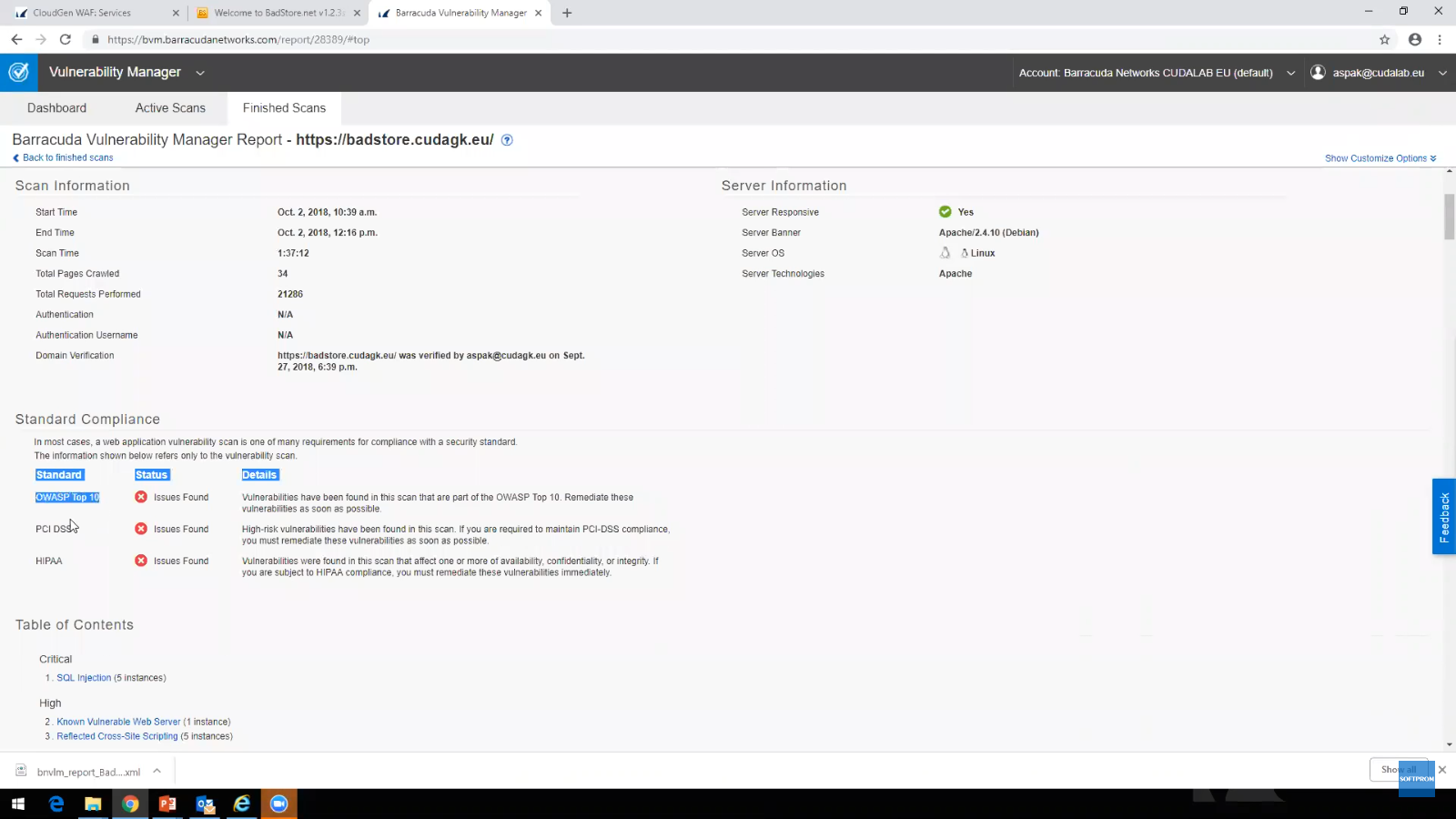


Рис. 2.6.Детальний опис загроз та незбіги процесів

Опис загрози та незбіги процесів.

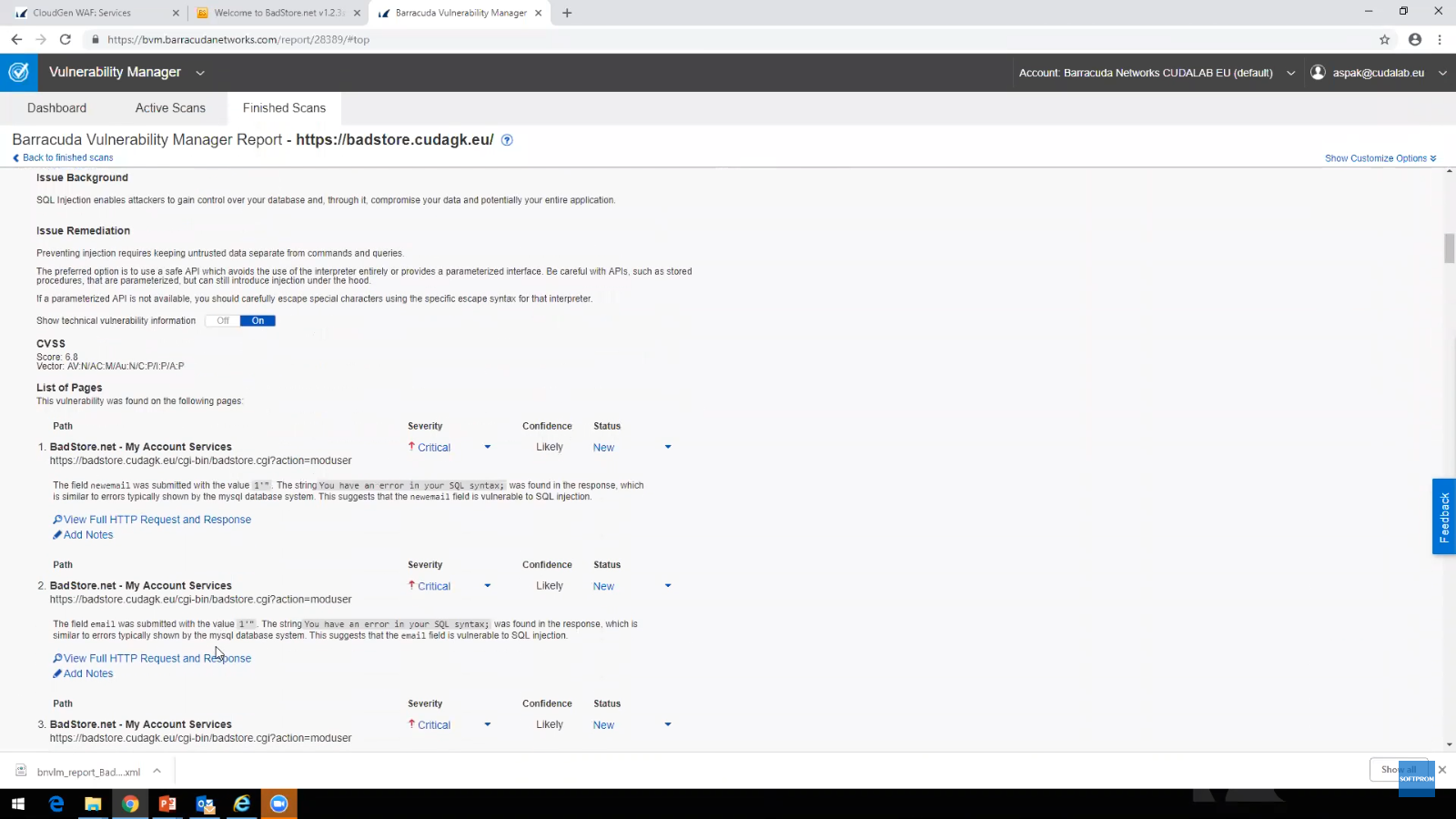


Рис. 2.7. Додаткова інформація про те які вразливості були виявленні, під час сканування загроз

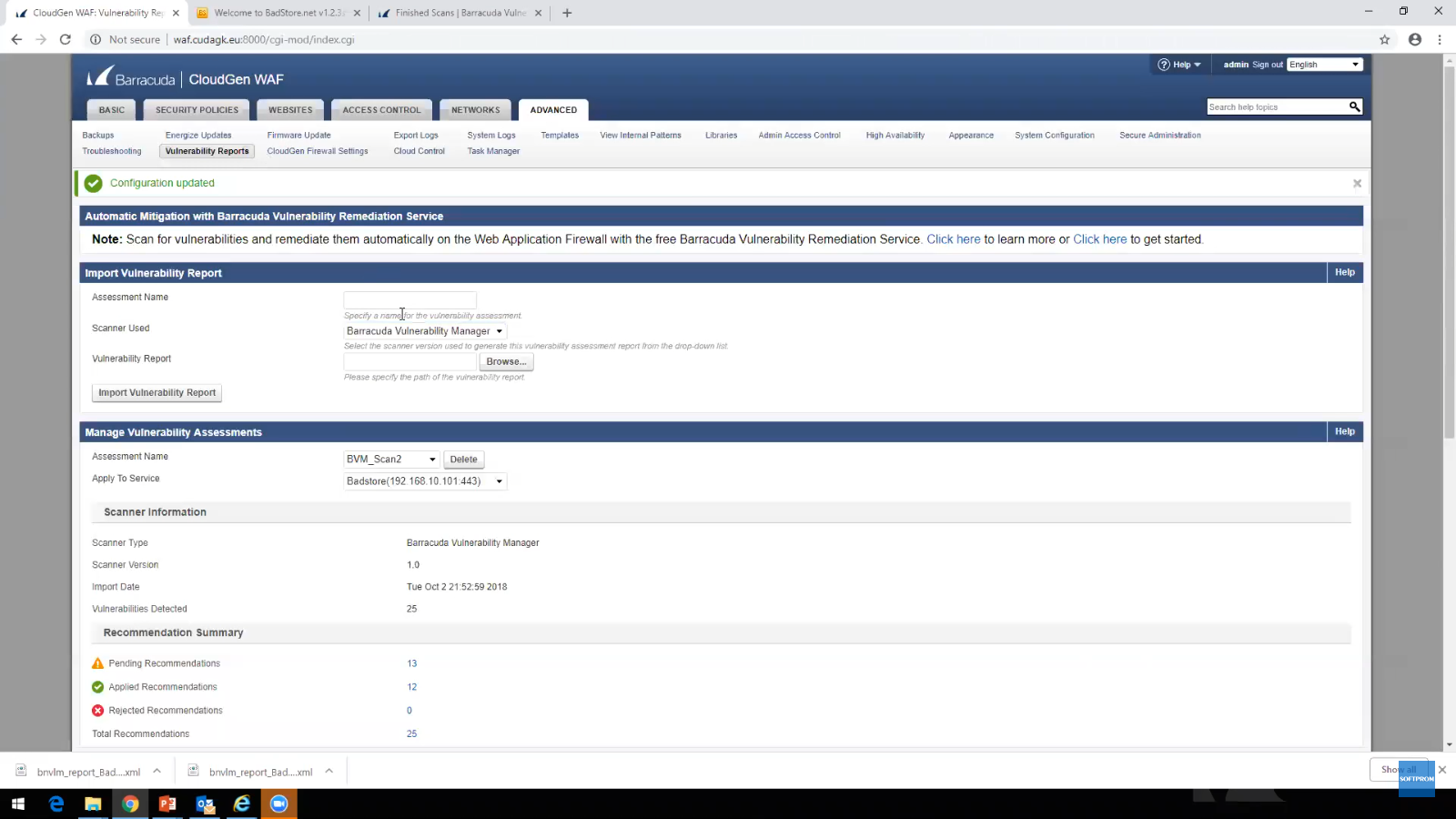
Додаткова інформація щодо запитів, надісланих під час сканування цієї вразливості.

Рис. 2.8.Скачений звіт вразливостей у форматі XCL

Завантажити звіт у форматі XCL та включити його до звіту про вразливість. Надання назви та вибір сканера загроз.

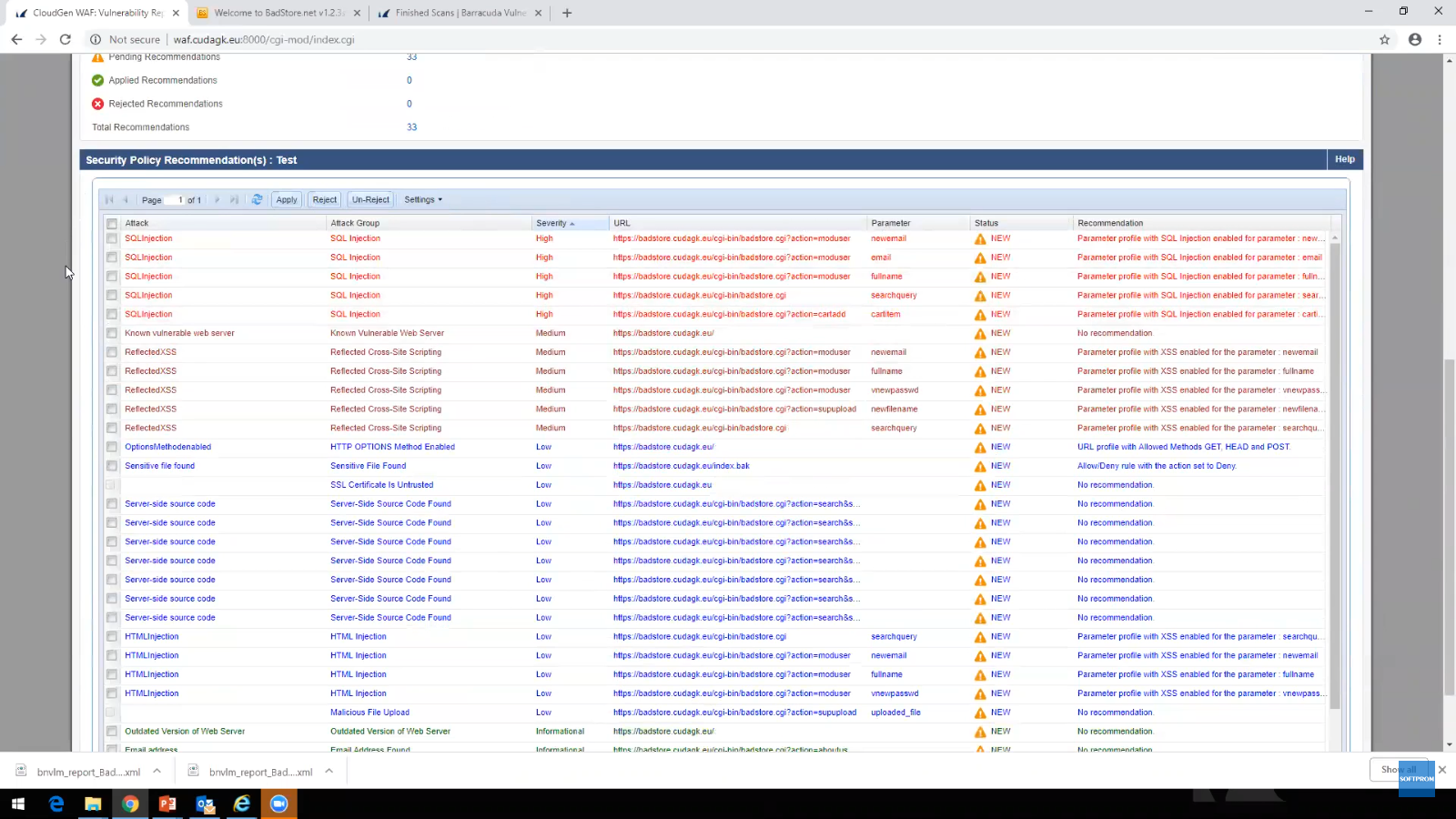


Рис. 2.9. Список вразливостей не доданий до звіту , та рекомендації їх усунення

Відображення уразливостей, які не були включені до звіту, та надання рекомендацій щодо можливих заходів.

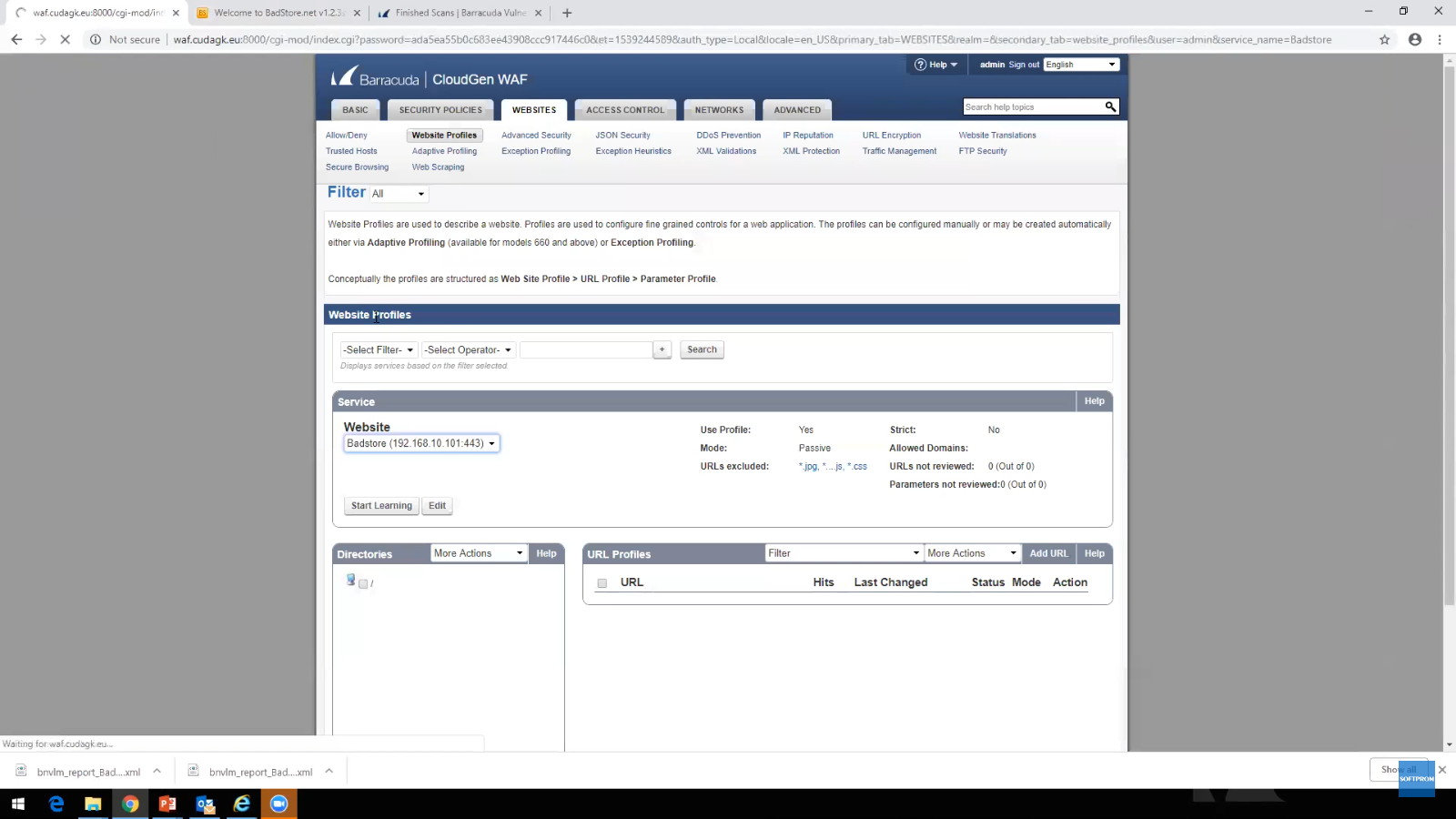


Рис. 2.10.Вибір веб-сайту та його настройки

Вибір веб-сайту та більш конкретний аналіз його запитів.

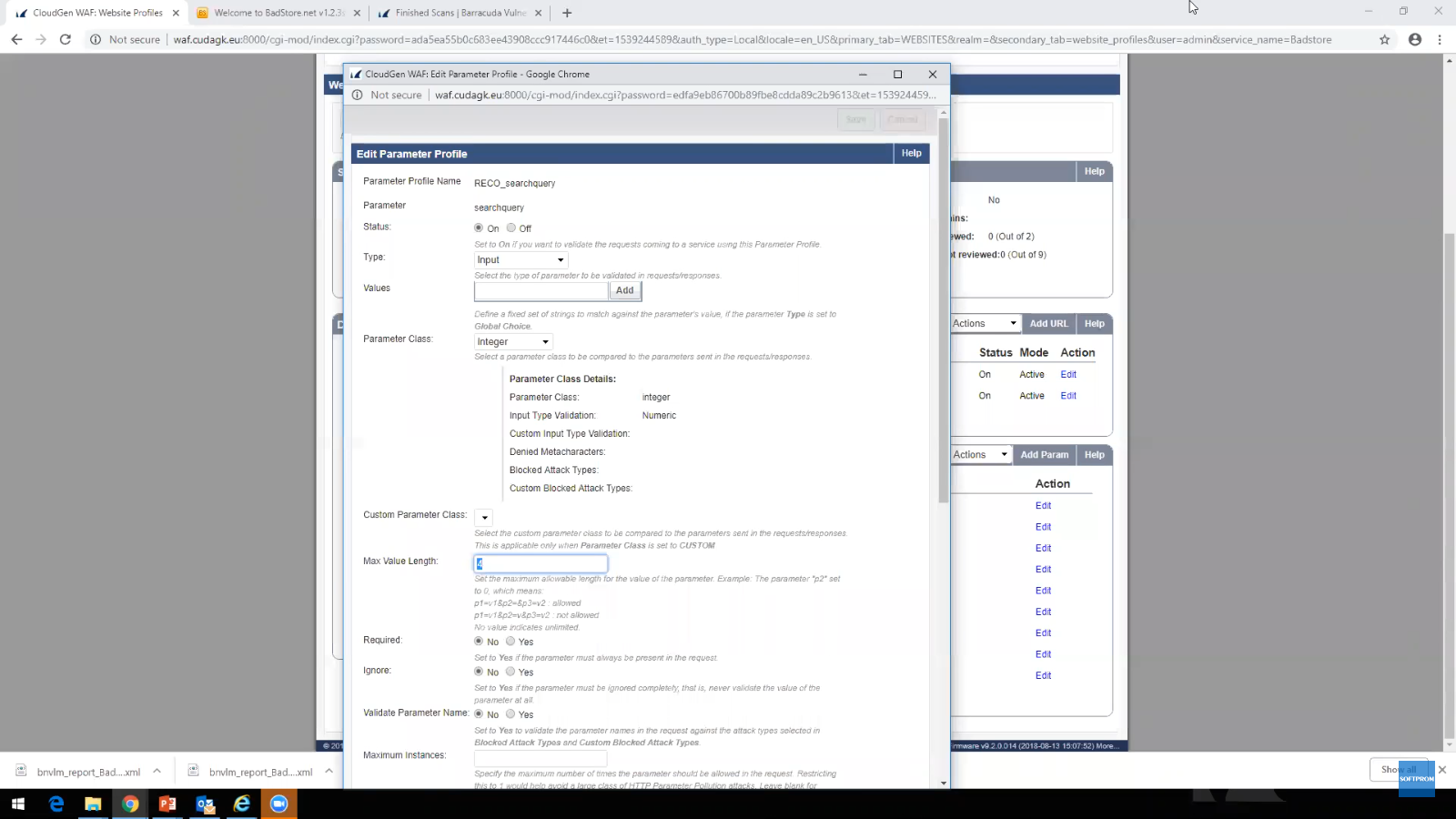


Рис. 2.11. Додаткові настройки для веб-сайту

Вибір профілю, параметр "Max Value Length" зі значенням 4 символи(кататера) .

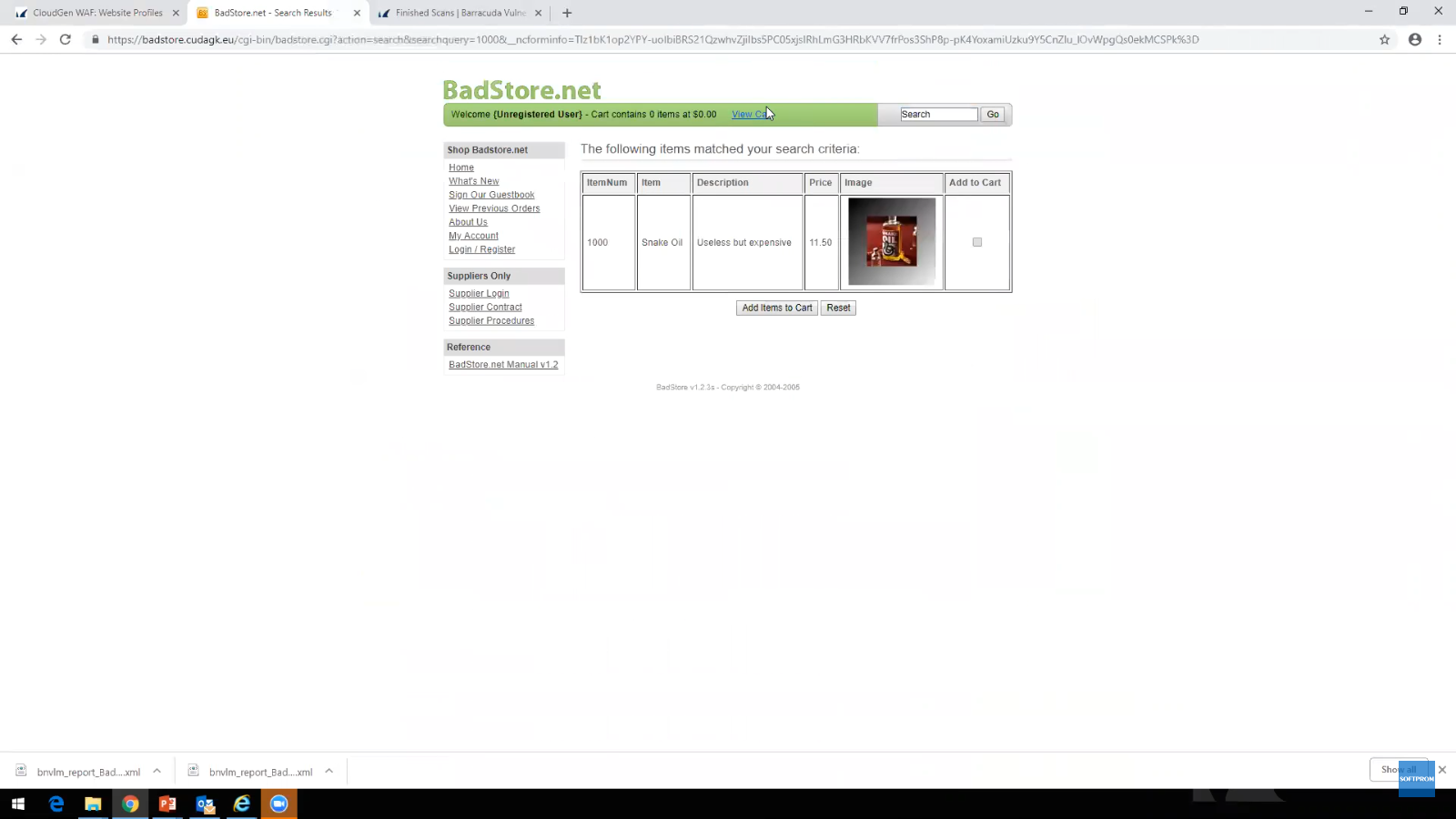


Рис. 2.12. Демонстрація

Демонстрація того, як пошукова система працює відповідно до заданих параметрів.

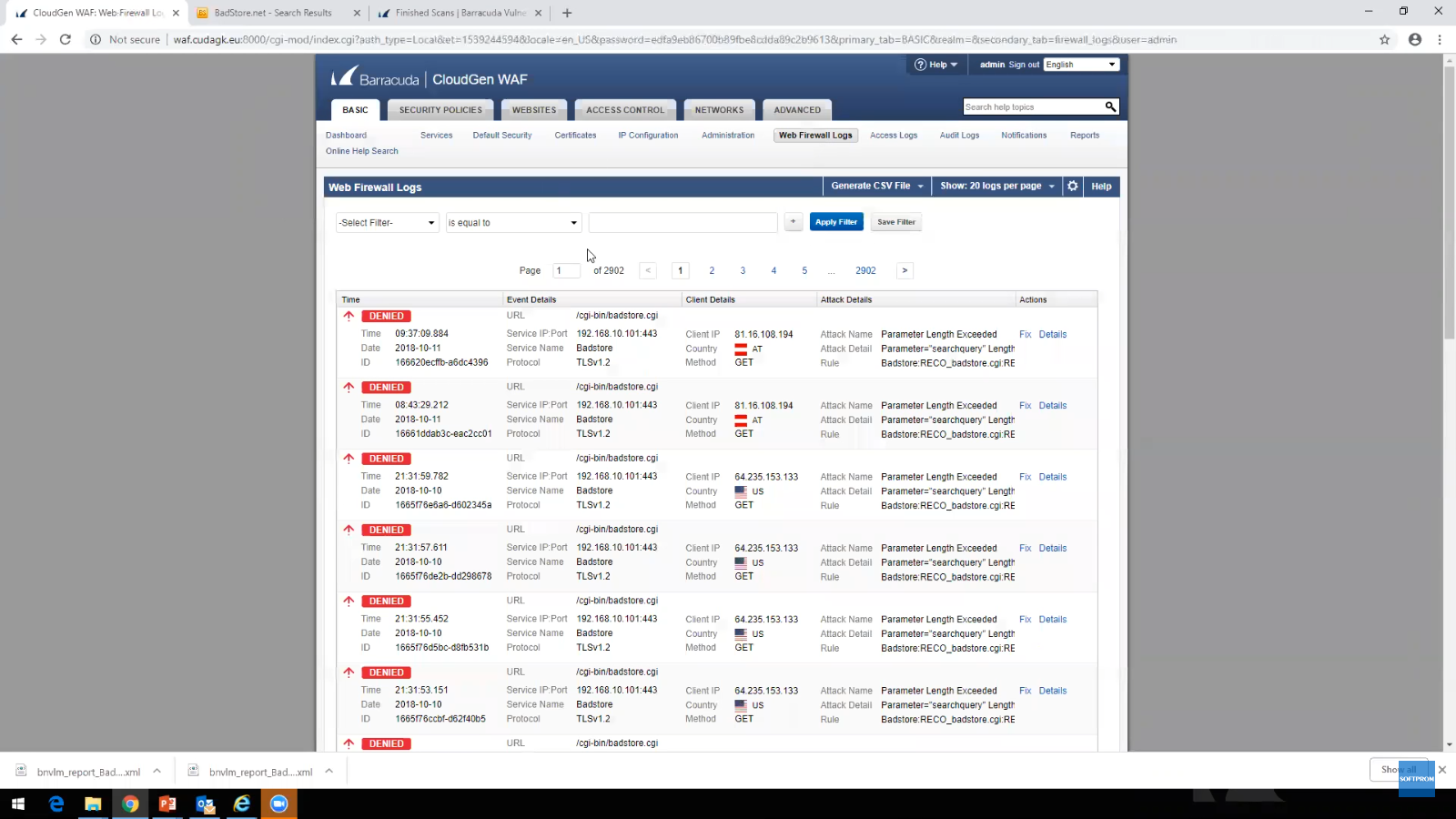
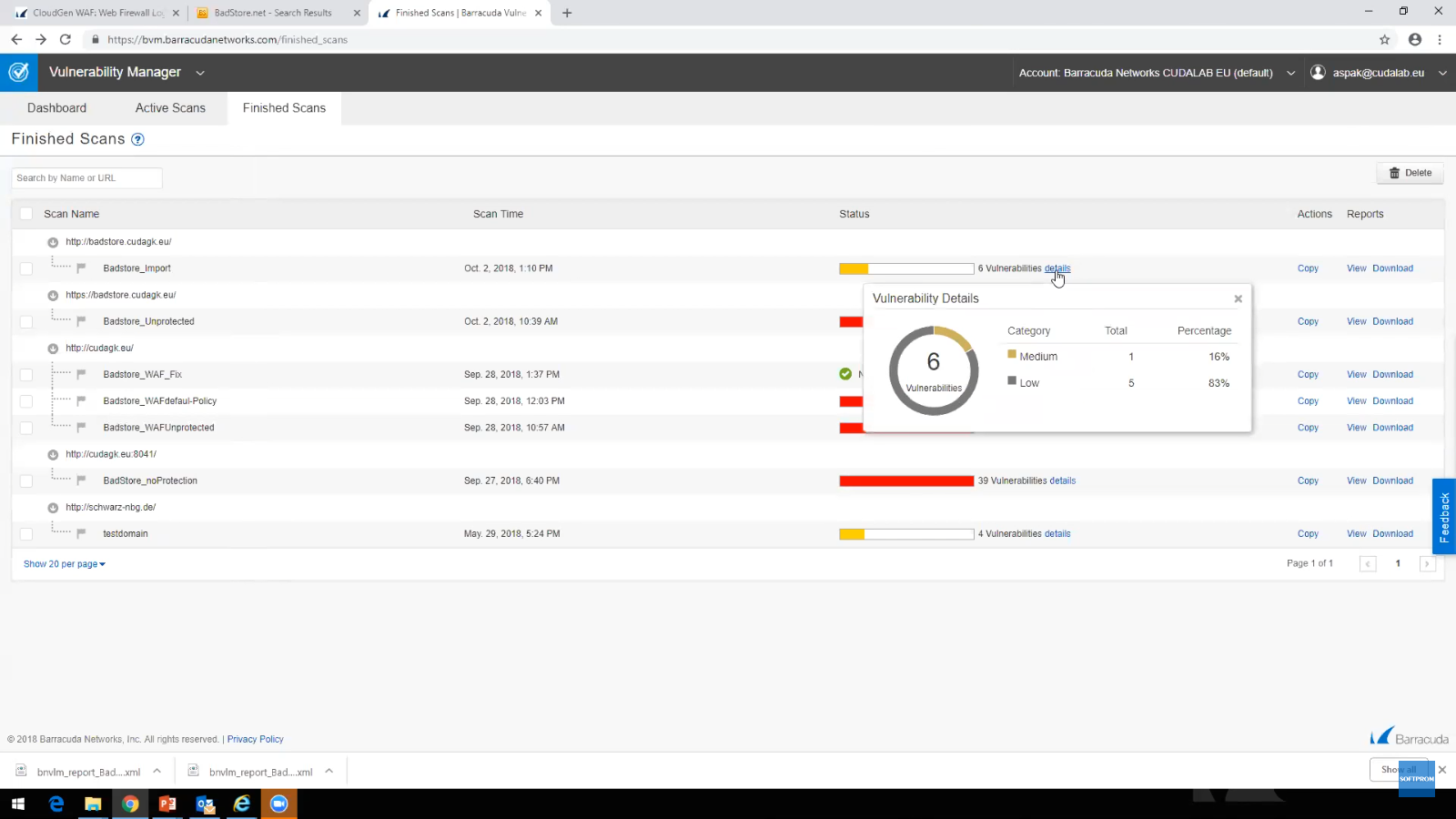


Рис. 2.13. Звітість помилкового користування

Опис невиконання чи помилкового використання звітності.

 Рис. 2.14. WEB-сторінка після перевірки з захистом WAF

Застосування сканера загроз, що зменшило кількість загроз з 33 до 6.

# 3 РОЗРОБКА РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ BARRACUDA WAF

## 3.1 Рекомендації що до встановлення рішення Barracuda WAF

Ось деякі кроки, які можуть допомогти вам перед встановленням будь-якої програми:

Перевірте, чи ваш комп'ютер або сервер відповідає системним вимогам програми Barracuda WAF. Перевірте документацію або програму веб-сайту для отримання детальної інформації щодо вимог.

Зробіть резервну копію важливих даних на вашому комп'ютері чи сервері. Цей важливий крок після встановлення нового програмного забезпечення може призвести до втрати даних або неупереджених проблем. Забезпечення резервного копіювання допоможе зберегти вашу інформацію у безпечному місці.

Перед встановленням програми Barracuda WAF, переконайтеся, що у вас є всі необхідні установчі файли або інсталяційний пакет програми. Як правило, ці файли доступні на веб-сайті розробника або можуть бути надіслані вам як частина ліцензійного або придбаного пакету.

Прочитайте документацію або інструкції, які постачаються із програмою Barracuda WAF. Вони можуть надати важливу інформацію про процес встановлення, деякі налаштування або виявлені проблеми, з якими ви можете зіткнутися.

Дотримуйтесь інструкцій встановлення, які надані з програмою Barracuda WAF. Зазвичай вони включають послідовність кроків, які потрібно виконати для успішного встановлення програми. Упевніться, що дотримуєтеся кожного кроку важливо і не пропускаєте жодного необхідного дійства.

Під час встановлення ви можете бути запитані про різні налаштування та параметри. Важливо прочитати пояснення шкірного параметра та вибрати відповідні значення відповідно до ваших потреб.

Після завершення процесу встановлення Barracuda WAF перевірте, чи все працює належним чином. Запустіть програму та переконайтеся, що вона працює без проблем і відповідає вашому очікуванню. Якщо ви бачите будь-які помилки або проблеми, перегляньте документ або зверніться до служби підтримки Barracuda WAF для отримання допомоги.

Регулярно оновлюйте Barracuda WAF, встановлюючи нові версії програмного забезпечення, які випускаються розробником. Оновлення може сприяти покращенню безпеки, нових функцій або виправленню помилок. Важливо встановити це оновлення, щоб забезпечити оптимальну роботу програми та захист вашої системи.

Якщо у вас виникли труднощі або потреба в додатковій допомозі щодо встановлення Barracuda WAF, рекомендуємо звернутися до програми підтримки офіційних джерел. Це може бути розробник веб-сайту, форум спільних користувачів або контактна інформація для отримання технічної підтримки. Спеціалісти з підтримки фактично готові дати конкретні поради та відповіді на ваші запитання.

Не забувайте про важливість забезпечення безпеки під час встановлення програмного забезпечення. Перевірте, чи завантажений файл або інсталяційний пакет виходить із довіреного джерела. Крім того, використовуйте актуальне антивірусне програмне забезпечення для перевірки наявності шкідливих програм або вірусів.

Зберігайте всі ліцензійні ключі, серійні номери та іншу важливу інформацію, пов'язану з інстальованим Barracuda WAF. Це допоможе вам у майбутньому, наприклад, при перевстановленні програм на новому комп'ютері або втраті даних.

Пам'ятайте про важливість дотримання правил ліцензування програмного забезпечення. Перегляньте, що ви використовуєте Barracuda WAF згідно з ліцензійними умовами та обмеженнями, які встановлені розробником програми.

Якщо у вас є додаткові питання або потреби в конкретній допомозі щодо Barracuda WAF, рекомендуємо звернутися до розробника або офіційного джерела програми підтримки.

Завжди бережіть інформацію про оновлення та патчі для Barracuda WAF. Виробник програми регулярно випускає оновлення, які можуть включати нові функції, виправлення помилок та покращення безпеки. Важливо слідк

Завжди бережіть інформацію про оновлення та патчі для Barracuda WAF. Виробник програми регулярно випускає оновлення, які можуть включати нові функції, виправлення помилок та покращення безпеки. Важливо слідкувати за цими оновленнями та вчасно їх встановлювати, щоб мати доступ до найновіших можливостей та забезпечити безпеку вашої системи.

Використовуйте Barracuda waf відповідно до рекомендацій та передбачених використанням. Ця програма може мати конкретні налаштування, рекомендації щодо використання та вимоги до системи. Важливо дотримуватися цих вказівок, щоб забезпечити найкращу продуктивність та захист системи.

## 3.2. Розробка загальних рекомендацій, що до застовсування Barracuda WAF

Загальні рекомендації, які допоможуть вам максимально ефективно використовувати це рішення:

На базі інсталяції та використання Barracuda WAF, ось загальні рекомендації, які допоможуть вам максимально ефективно використовувати це рішення:

Визначте вимоги та вимоги: перед встановленням Barracuda WAF чітко визначте свої елементи та вимоги щодо безпеки веб-додатків. Це допоможе вам настроїти та створити рішення відповідно до вашої специфіки.

Аналізуйте поточні загрози: введіть аналіз наявних загроз та уразливостей вашої інфраструктури та веб-додатків. Це дозволяє вам встановити ключові області, які потребують захисту, та налаштувати Barracuda WAF відповідно до цих вимог.

Налаштування правил безпеки: Ретельно налаштуйте правила безпеки в Barracuda WAF для виявлення та блокування шкідливого трафіку. Врахуйте особливості вашої організації та веб-додатків, щоб забезпечити ефективну захист.

Перегляньте використання додаткових модулів: Barracuda WAF пропонує різні модулі, які можуть покращити його функціональність. Розгляньте можливість використання додаткових модулів, таких як захист від DDoS-атак, захист від SQL-інекцій тощо, для посилення безпеки вашої інфраструктури.

Забезпечте взаємодію з іншими безпековими рішеннями: Перегляньте, що Barracuda WAF взаємодіє з іншими безпековими рішеннями у вашій інфраструктурі, наприклад, як брендмауери, системи виявлення вторгнення тощо. Це дозволить створити повноцінну систему захисту злагод

Моніторинг та аналіз журналів: Налаштуйте систему моніторингу та аналізу журналів Barracuda WAF для виявлення підозрілої активності, аномалій та невразливості. Слідкуйте за журналами подій, журналами виявлених загроз та іншими виготовленими метриками безпеки. Це допоможе вам швидко реагувати на деякі загрози та отримати необхідні заходи безпеки.

Забезпечення належного планування міграції: перед встановленням Barracuda WAF необхідно спланувати процес міграції. Врахуйте вимоги до простої години, документуйте необхідні зміни в налаштуваннях та виконайте тестування перед впровадженням. Плануйте резервні варіанти та забезпечте підтримку при виникненні проблеми під час міграції.

Навчання персоналу: Забезпечте належне навчання персоналу, який буде відповідальним за управління та підтримку Barracuda WAF. Організуйте навчальні семінари або навчальні матеріали, щоб персонал отримав достатні знання про функції, налаштування та розробку правил безпеки. Упевніться, що всі члени команди мають доступ до документації та ресурсів для вирішення питань щодо Barracuda WAF.

Регулярні оновлення: Підтримуйте інсталяцію Barracuda WAF оновленою, встановлюючи оновлення та патчі безпеки, які надаються виробником. Це допоможе усунути вразливість та підвищити загальний рівень безпеки. Перегляньте, що процес оновлення є частиною вашої регулярної технічної підтримки.

Аудит безпеки: Проведіть регулярні аудити безпеки для перевірки ефективності та надійності Barracuda WAF. Це може включати оцінку правил безпеки, перевірку конфігурації, аналіз журналів подій та виявлення можливих уразливостей. Аудит допоможе визначити слабкі місця та покращити удосконалення системи безпеки.

Реагування на інциденти: Розробте план реагування на інциденти, який включає процедури реагування на якісь загрози та атаки. Оперативно вживайте заходи для мінімізації впливу інцидентів та відновлення системи безпеки. Перегляньте, що весь персонал знає ваші обов'язки та процедури у разі інциденту.

Угода про співпрацю з провайдерами та постачальниками: Забезпечте ефективну співпрацю з провайдерами хмарних послуг, постачальниками програмного забезпечення та іншими постачальниками, які використовують у вашій інфраструктурі. Упевніться, що вони розуміють та підтримують інтеграцію з Barracuda WAF та вимогами безпеки.

Інформація про нові загрози та тренди: Підпишіться на інформаційні ресурси, оновлення та бюлетені про безпеку, щоб бути в курсі нових загроз та трендів у кібербезпеці. Важливо залишатися впевненим, що ви маєте актуальну інформацію та можливість адаптувати свої заходи безпеки до нових викликів.

Регулярні навчання та усвідомлення безпеки: Організуйте регулярні навчальні сесії та тренінги з питань кібербезпеки для всього персоналу. Навчання має охоплювати основні принципи безпеки веб-додатків, ідентифікацію фішингу, використання слабких паролів та інші загрози. Забезпечення свідомості про безпеку серед співробітників допоможе уникнути уразливостей, пов'язаних із соціальним інжинірингом та людським фактором.

# ВИСОВКИ

У результаті проведеного аналізу проблем та загроз, пов’язаних із веб-додатками, виявлено, що ряд небезпек може призвести до порушення конфіденційності інформації, порушення доступності чи недостовірності даних. У багатьох випадках атаки застосовують різні вразливості, зокрема ті, які детально досліджуються та документуються організацією OWASP (Open Web Application Security Project).

Застосування рішення WAF, зокрема Barracuda WAF, є одним із ефективних шляхів захисту веб-додатків. WAF здатністю виявляти та блокувати атаки на рівні додатків, забезпечуючи високий рівень захисту. Він може розпізнавати та блокувати вразливості, SQL-ін'єкції, перехоплення сесії, сканування портів та інші загрози. Завдяки такому рішенню можна попередити вразливість та пошкодити ризик компрометації системи.

Проте, важливо зазначити, що прийняте рішення WAF не повинно бути єдиним заходом захисту. Рекомендації щодо безпеки веб-додаток включають в себе та інші шляхи захисту, такі як регулярне оновлення програмного забезпечення, використання безпечних кодів та методів аутентифікації, обмеження привілеїв користувачів, аудит безпеки та навчання персоналу.

Крім того, проведення аудиту вразливостей веб-додатків є наступним етапом у процесі їх захисту. Ретельний аналіз коду та виявлення ідентифікаційних проблем викликали доповнення ваших слабких місць та невразливості, які можуть бути використані зловмисниками. Результати аудиту допомагають покращити безпеку додатків, вносячи відповідні зміни та застосовуючи рекомендації OWASP.

Узагалі, ефективний захист веб-додатків потребує комплексного підходу, поєднуючи в собі технічні засоби (такі як Barracuda WAF) з процесами управління безпекою та навчанням персоналу. Належне навчання розробників і адміністраторів завершити усвідомлення проблеми та впровадити найкращі практики в процес розробки та безпеки використання веб-додатків.

Отже, шляхи дослідження та розробка рекомендацій щодо захисту веб-додатків на базі рішень WAF, зокрема Barracuda WAF, виявилися доречними та актуальними. Використання цих технологій покращує ефективність та запобігає атакам, забезпечуючи надійний рівень безпеки для веб-додатків та захищаючи їх від наявних загроз. Проте, важливо пам’ятати, що безпека веб-додатків є постійним процесом, який вимагає систематичного оновлення та вдосконалення відповідно до змінних загроз та стандартів безпеки.

Розробка рекомендацій щодо захисту веб-додатків на базі рішень WAF повинна виконуватися нові методи атак, виявлені невразливості та зміни в стандартах безпеки. Наприклад, актуальність рекомендацій можна залежати від оновлення OWASP Top 10, які відображають найбільш розширені атаки на веб-додатки.

Крім того, підходи до захисту веб-додатків на базі WAF мають бути спрямовані на підключення вимкнення та запобігання атак. Попереднє виявлення шкідливих дій та блокування їх перед нанесенням шкоди дозволяє зменшити ризик і запобігти компрометації веб-додатків.

Крім використання рішень WAF, рекомендації також необхідно наголошувати на обов’язковий регулярний моніторинг та аналіз журналів подій, аудит безпеки та планування аварійного відновлення. Ці кроки відмовилися вчасно виявляти аномалії, атаки та вразливості, а також відновлювати роботу веб-додатків у разі інцидентів.

Враховуючи велику кількість загроз, з якими стикаються веб-додатки, важливо зменшити підхід до захисту, забезпечуючи постійну оновленість та адаптацію до нових викликів. Розробка рекомендацій має виконати специфікацію конкретного веб-додатку, його архітектуру та особливості, щоб забезпечити оптимальний рівень захисту.

Враховуючи постійний розвиток технологій та появу нових загроз, необхідність дослідження шляхів та розробки рекомендацій щодо захисту веб-додаток на базі рішень WAF залишається актуальною. Тільки поєднання технічних засобів, ефективного управління безпекою, регулярного аудиту та навчання персоналу забезпечить надійний рівень захисту веб-додатків від широкого спектру загроз.

# ПЕРЕЛІК ПОСИЛАНЬ

1. → Article about web applications [Електронний ресурс] — Режим доступу:

<https://wezom.com.ua/ua/blog/kak-sozdat-veb-prilozhenie>

2. → Article about web applications [Електронний ресурс]:

<https://webcase.com.ua/uk/blog/cho-takoe-web-prilozhenie-vse-vidy/#:~:text=Вебдодаток%20%20це%20програмне%20забезпечення,Chrome%2C%20Mozilla%2C%20Yandex>

3. → Official website of OWASP TOP 10 on vulnerability [Електронний ресурс ] — Режим доступу:

<https://owasp.org/www-project-top-ten/>

4. → Article about the web market 2023 [Електронний ресурс] — Режим доступу:

<https://geekflare.com/web-application-firewall/>

5. → Barracuda official site [Електронний ресурс] — Режим доступу:

<https://www.barracuda.com/products/application-protection/web-application-firewall>

6. → Barracuda WAF documentation [Електронний ресурс] — Режим доступу:

<https://www.barraguard.com.au/datasheets/products/Barracuda_Web_Application_Firewall_TDS_US.pdf>

7. → Features of Barracuda WAF [Електронний ресурс] — Режим доступу:

<https://spro.com.ua/products/barracuda-networks/barracuda-web-application-firewall>

8. → Description of Barracuda WAF [Електронний ресурс] — Режим доступу:

<https://www.ico.kz/catalog/informatsionnaya-bezopasnost/barracuda/656/>

9. → Barracuda WAF firewall as a service [Електронний ресурс] — Режим доступу:

<https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/885844113092849>

10. → Description of Barracuda WAF [Електронний ресурс] — Режим доступу:

<https://www.barraguard.com/964.asp>

11. → How to protect web applications from cyber threats Barracuda WAF? [Електронний ресурс] — Режим доступу:

<https://www.youtube.com/watch?v=1VPqcyPSHq8>

# ДЕМОНСТАЦІЙНІ МАТЕРІАЛИ (Презентація)