ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо захисту веб-сайтів за допомогою WAF Azure»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ярослав ЩЕРБАТЮК
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ЩЕРБАТЮК Ярослав
(прізвище, ім'я)

Керівник д.ф., доцент, МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___" _____ 2024 року

З А В Д А Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Щербатюк Ярослав Сергійович
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розробка рекомендацій щодо захисту веб-сайтів за допомогою WAF Azure»

керівник кваліфікаційної роботи Марченко Віталій, д.ф., доцент
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення захисту веб-сайтів Waf Azure;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблем забезпечення веб-сайтів.
2. Дослідження методів захисту веб-сайтів.
3. Розробка рекомендацій щодо захисту веб-сайтів за допомогою waf azure в інформаційній системі підприємства.

5. Перелік графічного матеріалу

Презентація PowerPoint.

6. Дата видачі завдання 27.02.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту веб-сайтів.	27.02.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.		
3.	Аналіз методів та засобів захисту веб-сайтів на базі Azure WAF.		
4.	Практична реалізація варіанту захисту веб-сайтів на базі Azure WAF.		
5.	Розробка рекомендацій щодо застосування методів та засобів захисту веб-сайтів на базі Azure WAF.		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Ярослав ЩЕРБАТЮК
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ЩЕРБАТЮКА Ярослава
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту веб-сайтів за допомогою WAF Azure»

Актуальність: У сучасному цифровому середовищі веб-сайти є критично важливими для бізнесу, що робить їх привабливими цілями для кіберзлочинців. Щоденно з'являються нові загрози, такі як SQL-ін'єкції та DDoS-атаки. Azure Web Application Firewall (WAF) є ефективним інструментом для захисту веб-додатків від цих загроз. Дослідження актуальне, оскільки розробка рекомендацій щодо впровадження та використання Azure WAF допоможе підприємствам підвищити безпеку веб-сайтів і знизити ризики атак.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми захисту кінцевих точок організації та визначено мету та завдання даного виду забезпечення, а також його складові частини.
2. Досліджено методи та засоби захисту кінцевих точок організації на базі FortiEDR.
3. Запропоновано варіант системи захисту кінцевих точок організації на базі FortiEDR та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз змісту захисту кінцевих точок на прикладі конкретної організації.
2. Запропонований порядок застосування методів та засобів захисту кінцевих точок бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач **ЩЕРАБТЮК Ярослав** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач ЩЕРБАТЮК Ярослав до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту веб-сайтів за допомогою WAF Azure».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ЩЕРБАТЮК Ярослав*** обрав тему роботи, метою якої було дослідити методи та засоби захисту кінцевих точок організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ЩЕРБАТЮК Ярослав*** 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 кваліфікаційну роботу здобувача ***ЩЕРБАТЮКА Ярослава*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ЩЕРБАТЮК Ярослав** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 55 сторінок, 22 рисунки, 17 джерел.

Об'єкт дослідження – захист веб-сайтів за допомогою WAF Azure.

Предмет дослідження – дослідження шляхів та розробка рекомендацій щодо захисту веб-сайтів за допомогою WAF Azure.

Мета роботи є дослідження та розробка рекомендацій щодо захисту веб-сайтів підприємства за допомогою Azure Web Application Firewall (WAF). Основними завданнями є аналіз проблем безпеки веб-сайтів, дослідження методів та засобів захисту на базі Azure WAF, розробка та реалізація рекомендацій щодо ефективного використання цього інструменту для забезпечення безпеки веб-додатків підприємства.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Веб-аплікаційні фаєрволи (WAF) відіграють важливу роль у підвищенні безпеки веб-сайтів організації. WAF призначені для постійного моніторингу та аналізу трафіку веб-додатків. WAF забезпечують видимість активності веб-сайтів у реальному часі, що дозволяє організаціям швидко реагувати на інциденти безпеки.

У роботі досліджено проблему захисту веб-сайтів організації, визначено її мету та завдання. Проведено аналіз існуючих методів та засобів захисту веб-сайтів організації. Досліджено методи та засоби захисту веб-сайтів на базі Azure WAF. Визначено призначення, основні функції та склад рішення Azure WAF.

На основі досліджень, проведених у роботі, запропоновано варіант системи на базі Azure WAF. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів та засобів захисту веб-сайтів організації.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

WAF - Web application firewall

XSS - Cross-Site Scripting

SQLi - SQL injection

API - Application Programming Interface

URL - Uniform Resource Locator

Проксі - proxy

ПЗ -програмне забезпечення.

CMS - Content Management System

SSL-сертифікат - Secure Sockets Layer Certificate

HTTPS - Hypertext Transfer Protocol Secure

SHA - Secure Hash Algorithm

LDAP - Lightweight Directory Access Protocol

XXE - XML External Entity

OS - Operating System

XSSC - ross-Site Scripting

CSRF - Cross-Site Request Forgery

FTP-пароль - File Transfer Protocol

TLS - Transport Layer Security

ВСТУП

Актуальність дослідження. З розвитком цифрових технологій та інтернету веб-сайти стали невід'ємною частиною бізнесу та повсякденного життя. Однак зростаюча залежність від веб-технологій призводить до підвищення рівня кіберзагроз. Злочинці постійно шукають вразливості у веб-додатках, щоб викрасти конфіденційну інформацію, порушити роботу сервісів або завдати репутаційної шкоди. Тому забезпечення безпеки веб-сайтів є критично важливим завданням для будь-якого підприємства.

Azure Web Application Firewall (WAF) є одним з найбільш ефективних інструментів для захисту веб-додатків від широкого спектру загроз. Використання Azure WAF дозволяє виявляти та блокувати різні типи атак, включаючи SQL-ін'єкції, XSS та DDoS-атаки. Це забезпечує високий рівень безпеки та надійності веб-ресурсів.

Актуальність даного дослідження полягає у необхідності розробки рекомендацій щодо впровадження та оптимізації захисту веб-сайтів з використанням Azure WAF. Це дозволить підприємствам ефективно захищати свої інформаційні системи, знижувати ризики кіберзагроз та забезпечувати безперебійну роботу своїх веб-додатків. Результати цього дослідження будуть корисними для спеціалістів з інформаційної безпеки, розробників та IT-адміністраторів, які прагнуть покращити безпеку своїх веб-ресурсів.

Предмет дослідження – Дослідження шляхів та розробка рекомендацій щодо захисту веб-сайтів за допомогою Azure WAF.

Методи дослідження - вивчення наукової літератури, аналіз існуючих технологій захисту веб-сайтів, зокрема Azure Web Application Firewall (WAF), та розробка рекомендацій щодо його використання для підвищення рівня безпеки веб-сайтів.

Практичне значення одержаних результатів – рекомендації щодо використання Azure WAF можуть бути використані для підвищення рівня захисту веб-сайтів від різноманітних кібератак.

1 АНАЛІЗ ВРАЗЛИВОСТЕЙ ВЕБ-САЙТІВ

1.1. Небезпека вразливості сайту

На сьогоднішній день вразливість веб-сайтів є однією з найактуальніших проблем для їх власників. Якщо важлива інформація потрапить до рук зловмисників, це може не тільки зашкодити репутації веб-сайту, але й створити загрозу втрати фінансів, тобто доходу, заради якого сайт і був створений.

Чи існують способи захистити свої інтереси та ресурси? Чи можна уникнути вторгнень зловмисників, метою яких є завдання шкоди конкуренту або отримання чужих грошей нечесним шляхом?

Розглянемо, що таке вразливість веб-сайту. Веб-платформа можна уявити як укріплений замок з високими стінами, охоронюваними воротами, гарматами на вежах і ровом, заповненим водою. Все функціонує ідеально і добре захищено. Однак, зловмисник може знайти спосіб перелізти через стіну, інший може увійти через ворота, видаючи себе за простого торговця, а третій може знайти таємний хід і скористатися ним.

Так само йде справа і з вразливістю веб-сайтів. Ви можете докладати всіх зусиль для забезпечення безпеки кожного модуля сайту, використовуючи найсучасніші інструменти, але в системі все одно можуть виявитися слабкі місця, які стануть загрозою для безпеки ресурсу. Через такі лазівки хакери використовують вразливості та підпорядковують собі чужі сервери.

Вразливість (англ. – vulnerability) означає слабкі місця в коді ресурсу або в програмах, що використовуються сервером. Через них зловмисники можуть проникнути в систему і порушити її роботу.

Звідки беруться ці вразливості? Помилки можуть бути допущені на етапі створення сайту або його програмування. Паролі можуть виявитися недостатньо надійними. Можливі також атаки або використання невдалих скриптів та SQL-ін'єкцій.

Коли система виявляє таке слабке місце, зловмисник може здійснювати дії, які зазвичай не повинні бути дозволені. Суть атаки полягає у впровадженні в програму помилкових кодів або даних, які приймаються як вірні.

На практиці, в більшості випадків, проблеми виникають через прийняття веб-ресурсом погано перевірених даних, введених користувачем. Такі некоректні та небезпечні команди виявляються вставленими в працюючий код. Існують і більш складні ситуації, наприклад, переповнення буфера обміну, коли в нього вставляють надто великі дані, не переконавшись у достатності місця для них.

Деякі вразливості існують лише в теорії, але більшість з них являє собою реальну проблему.

По-перше, ви втрачаєте повний контроль над власним ресурсом, що є серйозною проблемою. Контент, який тепер може бути опублікований, може призвести до того, що пошукові системи внесуть вас до чорного списку. Крім того, права адміністрування (логіни і паролі) можуть потрапити до рук хакерів, які вимагатимуть викуп за відновлення доступу до управління сайтом.

По-друге, зловмисники отримують доступ до баз даних користувачів. Якщо це лише логіни і паролі або списки електронних адрес, то це вже небезпечно, але значно серйознішою проблемою є витік платіжних даних.

По-третє, ваш ресурс може бути використаний як джерело розсилки листів з небезпечним кодом, що призводить до серйозних збоїв у роботі комп'ютерів одержувачів. Щоб адресат точно відкрив такий лист, у ньому можуть міститися повідомлення про цікаві вакансії, великий виграш або нагадування про несплачений штраф.

По-четверте, на зламаному сайті шахраї можуть розміщувати фішингові сторінки, що імітують справжні (соціальні мережі, банківські організації або інтернет-магазини). Користувач, не підозрюючи підступу, залишає на таких сторінках свої фінансові дані, які потім потрапляють до шахраїв.

Ще одна небезпека, пов'язана з вразливістю сайтів, – це можливість зараження інших веб-ресурсів через шкідливі скрипти, впроваджені на зламані

сайти. Вони можуть бути використані ботами як проміжні сервери для організації потужних DDoS-атак.

Варто пам'ятати про можливість розміщення на зламаному сайті так званого редиректу, тобто коду, який автоматично перенаправляє відвідувача на інші сторінки з пропозиціями оформлення платної підписки. Пошукові системи часто розглядають таку примусову переадресацію як приховану рекламу і вносять веб-ресурси з такими кодами до чорного списку.

Користувача можуть перенаправляти і на сторінки з вірусами, використовуючи вразливості операційних систем або програмного забезпечення. Людина завантажує файл з вірусом, який потім встановлює шкідливі програми, що порушують роботу всіх пристроїв у системі.

Крім того, зламаний сайт може втратити позиції у пошукових системах через редиректи, розсилку спаму або некоректний контент. Власнику доведеться витратити значні кошти та зусилля, щоб повернути своєму веб-ресурсу попереднє шановане становище.

1.2. Типи вразливості веб-сайтів

Для захисту веб-сайту від злому недостатньо вирішувати лише технічні аспекти; людський фактор також відіграє значну роль. Тестування веб-сайтів на вразливості показало, які слабкі місця є найбільш небезпечними і можуть спричинити збої в роботі ресурсу будь-якого розміру та профілю. Імовірність злому та швидкість відновлення залежать від того, наскільки успішно ви зможете усунути ці вразливості.

Використання ПЗ з перевірених джерел. Власники ресурсів часто завантажують модулі та плагіни з будь-яких джерел і встановлюють їх на свої сайти, що може призвести до зараження. Щоб уникнути подібних проблем, слід користуватися лише офіційними джерелами для додавання нових елементів дизайну, оновлення CMS тощо. Наприклад, офіційний репозиторій плагінів WordPress є надійним джерелом для цього популярного CMS.

Використання застарілих версій програмного забезпечення. Комп'ютери та їх програмне забезпечення потрібно регулярно оновлювати. Як веб-фахівці прагнуть підтримувати безпеку сайтів, так і хакери постійно намагаються зламати їх і отримати важливі дані. Шанси зловмисників значно знижуються, якщо використовуються нові стабільні версії ПЗ. Найважливішими є компоненти програмного забезпечення, через які здійснюється управління ресурсом, тобто CMS. Їх потрібно оновлювати регулярно. Однак, при цьому можуть виникати проблеми з несумісністю старих компонентів системи з оновленими.

Відсутність SSL-сертифікату на веб-ресурсах. SSL-сертифікат є спеціальним цифровим підписом, який підтверджує використання безпечного протоколу шифрування HTTPS для передачі даних. Якщо сертифікат встановлений, у рядку пошуку користувача поруч з посиланням з'являється значок замка. Придбати SSL-сертифікат можна в спеціальних центрах сертифікації, де пропонуються як платні, так і безкоштовні варіанти. Платні сертифікати мають довший термін дії та можуть гарантувати фінансове відшкодування у разі витоку інформації.

Використання незашифрованих паролів. Паролі слід шифрувати, використовуючи спеціальні алгоритми хешування, такі як SHA. Під час автентифікації до перевірки допускаються лише зашифровані дані користувачів. Для зниження вразливості слід встановлювати вимоги до формування паролів, включаючи мінімальну кількість символів, використання символів різного регістру, букв і цифр тощо. Паролі на кшталт "12345" є дуже слабким захистом. Надійними вважаються комбінації з 20 символів, тоді як паролі з менш ніж 8 символами не допускаються.

Ймовірність злому через ін'єкції.

Якщо користувач вводить неперевірені дані, які потрапляють на сайт, це може призвести до серйозних проблем. Це може статися через дії будь-якого користувача. Найпоширеніші ін'єкції – SQL, LDAP, XXE та OS. Особливо часто трапляються SQL-ін'єкції, через які хакери проникають у бази даних, використовуючи конфіденційну інформацію або змінюючи її. Це стається, якщо

інтерпретатор отримує дані без обов'язкових керівних послідовностей або команд, як-от лапки в SQL.

Ускладнення на етапі автентифікації і управління сесіями.

Багато додатків ідентифікують користувача перед початком роботи. Проте функціональні збої можуть призвести до того, що облікові записи користувачів опиняються в руках шахраїв без введення паролів. Хакери можуть перехоплювати і використовувати ключі та маркери автентифікації для доступу до облікових записів.

Уразливість сайтів XSS (міжсайтовий скриптинг).

Цей вид уразливості більше загрожує браузеру користувача, а не серверу. Cross-Site Scripting (XSS) – це ін'єкції, що працюють через JavaScript. Хакер вписує JS-код в поле введення, і браузер користувача виконує його, вважаючи, що код надійшов із сайту. Для захисту від цього рекомендується використовувати функції типу htmlspecialchars, які екранують спецсимволи.

Втрата контролю над доступом до ресурсу.

Навіть на популярних платформах буває, що дані користувачів стають доступними через помилки адміністрування. Наприклад, файли в кореневому каталозі ресурсу можуть бути відкритими. Файл wp-config.php не буде відкритий без пароля доступу до бази даних, але браузер може відкрити резервну копію з розширенням .swp, створену в редакторі Vim. Інший варіант – збої в коді програми, через які неавторизовані користувачі отримують доступ до конфіденційної інформації.

Неправильні конфігурації.

Аналізи сайтів на вразливості показують, що безпечних конфігурацій недостатньо. Важлива також правильна настройка безпеки сервера, яка вимагає постійної підтримки. Налаштування за замовчуванням не завжди надійні і потребують регулярного оновлення.

Передача конфіденційних даних у незахищеному вигляді.

Це часто трапляється на веб-сайтах при використанні певних API та додатків. Відкрита передача даних, які повинні бути конфіденційними, створює ризик їх

крадіжки або зміни хакерами через атаку "людина посередині". Для захисту таких даних слід використовувати шифрування HTTPS.

Слабка захищеність від атак.

Для запобігання атакам недостатньо перевірити логін і пароль. Потрібні спеціальні інструменти, яких у багатьох додатків і API немає. Серйозний захист включає виявлення, звірку з протоколами та блокування спроб вторгнення. Веб-майстри повинні мати можливості для своєчасного оновлення захисних механізмів.

CSRF-уразливості.

Cross-Site Request Forgery (CSRF) полягає в тому, що браузер користувача надсилає запит у слабкозахищений додаток. У таких запитах можуть міститися автоматично додані дані, файли, cookie тощо. Хакер формує запити від імені користувача, і додаток не сприймає їх як підроблені. Наприклад, користувач клацає на посилання, і його обліковий запис може бути видалено або надіслано спам його друзям.

Встановлення компонентів з вразливими місцями.

Веб-ресурси використовують компоненти, подібні до додатків, такі як фреймворки та бібліотеки. Вразливість у таких модулях може надати хакерам доступ до ваших даних і дозволити втручання у роботу сервера. Тому використання таких компонентів створює загрозу для безпеки додатків та API.

API без спеціального захисту.

У більшості веб-додатків є клієнтські програми та API-інтерфейси, що працюють через JavaScript. Вони доступні через пошукові системи або мобільні пристрої. Протоколи для їх використання – REST/JSON, SOAP/XML, GWT, RPC тощо. Вразливості можуть бути у самих API, що робить систему вразливою до атак.

Захист веб-ресурсів від зловмисників залежить від технологій і компонентів, що використовуються при створенні веб-додатків, а також від можливих уразливостей цих компонентів. Існують різні класифікації вразливостей, і кожна атака має свої особливості. Причиною цих уразливостей є помилки в розробці, реалізації та застосуванні компонентів веб-додатків. Тому необхідно шукати вразливості та оперативно реагувати на інформацію про їх місцезнаходження.

Широкий спектр інструментів дозволяє здійснювати пошук вразливостей, але ефективність їх використання залежить від алгоритмів дій, які необхідно застосовувати під час цього пошуку. Алгоритми дій можуть включати спеціальні методи, що охоплюють різні аспекти кібербезпеки, такі як тестування безпеки фізичного середовища, операційних систем, бездротових мереж. Це потребує додаткового часу для аналізу існуючих методів і вибору компонентів. Тому існує потреба в розробці методології тестування проникнення, яка враховувала б міжнародний досвід у тестуванні веб-додатків і містила б перелік можливих інструментів тестування.

1.3. Джерела загроз системам захисту веб-сайтів

Основним джерелом загроз для інформаційної безпеки веб-сайтів є зовнішні зловмисники. Зовнішній зловмисник — це особа, яка зазвичай має комерційний інтерес і можливість доступу до сайту компанії. Ця особа, хоча й не знайома з конкретною інформаційною системою, має високу кваліфікацію в галузі мережевої безпеки та значний досвід у проведенні мережевих атак на різні типи інформаційних систем.

Основну загрозу для безпеки сайту становлять хакерські атаки. Вони можуть бути цілеспрямованими або хаотичними, за принципом «атакую все підряд, що-небудь та зламається». У першому випадку зловмисник виявляє максимально можливу кількість векторів атаки для складання та реалізації потенційно успішних сценаріїв злому. У другому випадку атаки проводяться масово, зазвичай використовуючи кілька поверхневих вразливостей.

Види загроз

Загрози для безпеки веб-сайтів пов'язані з кількома факторами:

1. Вразливості сайтів або їх компонентів

Вразливості в веб-сайтах часто призводять до виконання коду на віддаленому сервері. Сервери обробляють дані, передані користувачами, і використовують їх при складанні команд для генерації динамічного вмісту. Якщо при розробці не

враховуються вимоги безпеки, зловмисник може модифікувати виконувані команди. Прикладом таких вразливостей є SQL-ін'єкції.

2. Використання механізмів перевірки ідентифікації

Атаки, спрямовані на методи перевірки ідентифікатора користувача, служби або програми, а також на методи, що використовуються веб-сервером для визначення прав доступу користувача. Прикладами таких атак є підбір паролів, обхід авторизації, небезпечне відновлення паролів, передбачуване значення сесії або її фіксація.

3. Атаки на самих користувачів та клієнтську частину

Під час відвідування сайту між користувачем і сервером встановлюються довірчі відносини. Користувач очікує отримати легітимний вміст і не передбачає атак з боку сайту. Зловмисники можуть використати цю довіру для атак на клієнтів сервера. Такі атаки можуть бути частиною складних сценаріїв або атакувати клієнтську частину, наприклад, через XSS (міжсайтовий скриптинг).

4. Витік або розголошення критичної інформації

Це включає розголошення даних про сайт, його компоненти, платформу і складові, а також витік конфіденційної інформації через неналежний захист. Може відбутися розкриття забороненої інформації або витік даних через неправильне налаштування сайту або веб-сервера.

5. Логічні атаки

Логічні атаки спрямовані на експлуатацію функцій сайту або логіки його роботи. Логіка веб-додатку передбачає очікуваний процес виконання програми при виконанні певних дій, таких як відновлення паролів, реєстрація облікових записів, транзакції в системах електронної комерції. Зловмисник може обійти або використати ці механізми у своїх цілях. До таких атак належать атаки класу відмови в обслуговуванні (DoS).

Види атак на веб-додатки

Цільові атаки - це атаки, спеціально націлені на сайт або групу сайтів, що об'єднані однією ознакою (сайти однієї компанії, відносяться до певної сфери діяльності, або об'єднані кількома ознаками). Небезпека таких атак полягає саме в

«замовному» характері. Виконавцями таких атак стають, як правило, зловмисники, що мають високу кваліфікацію в області безпеки веб-додатків (рис.1).

Рис.1.1 Повідомлення про надання злочинних послуг

Метою таких атак, зазвичай, є отримання конфіденційної інформації, яка може бути використана недобросовісними конкурентами або злочинцями для отримання прибутку.

Нецільові атаки - це атаки, які проводяться фактично навмання, а її жертвами стають випадкові веб-сайти незалежно від популярності, розміру бізнесу, географії або галузі. Нецільова атака на сайт - це спроба отримання несанкціонованого доступу до веб-ресурсу, при якій зловмисник не ставить за мету зламати конкретний сайт, а атакує відразу сотні або тисячі ресурсів, відібраних за певним критерієм. Наприклад, сайти, що працюють на певній версії системи управління сайтом. Такого роду атаки намагаються охопити максимальну кількість сайтів при мінімумі витрат (рис.2).

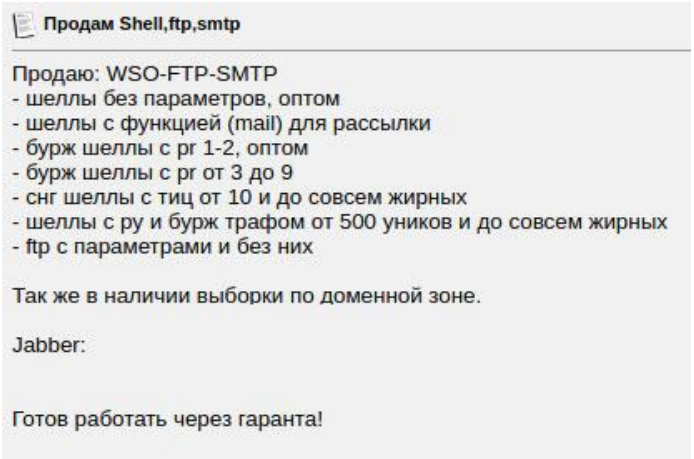

Рис.1.2 Повідомлення про надання злочинних послуг

При вдалій атаці зловмисник прагне отримати вигоду: закріпитися на сайті, завантажити хакерський скрипт (Web Shell, Back Door), додати нового адміністратора, впровадити шкідливий код або отримати необхідну інформацію з бази даних. Цільові атаки проводяться приховано і зазвичай досягають своєї мети. Нецільові атаки, навпаки, є досить "гучними" і часто не досягають поставлених цілей, але все ж можуть створити значні проблеми для власника веб-ресурсу.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВЕБ-САЙТІВ

2.1. Знаходження вразливості на сайті

Перевірка сайту на вразливості проходить кілька етапів. Неможливо просто натиснути кнопку і миттєво виявити всі слабкі місця - важливо отримати якомога більше детальної інформації про них. Процес включає такі кроки:

1. Збір даних. Необхідно зібрати максимально можливу інформацію про мережу або сервери, які використовуються.

2. Аналіз і сканування виявлених на веб-ресурсах вразливостей.

3. Пробна експлуатація. Цей етап виконується лише тоді, коли необхідно продемонструвати потенційну небезпеку.

4. Коригування. Вживаються заходи для усунення виявлених на веб-платформі слабких місць.

На кожному з цих етапів необхідно виконати ряд дій, застосовуючи відповідні інструменти. Практика показує, що використання кожної з програм-тестерів окремо не так ефективно, як їх комбінування у вигляді цілісного середовища для тестування на можливі загрози. Тому перевірку сайту на вразливості можна виконати через Kali Linux. Це дуже зручно - достатньо мати флешку зі збереженою системою і запустити її встановлення на жорсткий диск пристрою.

Збір відомостей.

На початковому етапі пошуку вразливостей мета полягає в тому, щоб з'ясувати, які дані можуть стати доступними стороннім. Для цього існує спеціальний інструмент - nmap. Він показує інформацію про працюючі на сервері сервіси (і їх версії), використані порти та версію самої операційної системи.

Наприклад для перегляду працюючих портів в своєму пристрої необхідно в KaliLinux запустити наступну команду:

nmap –sS 192.168.91.249

Цифрова послідовність – це IP ресурсу. В результаті буде видно, які порти відкриті і які сервіси використовує система. Однак і цих відомостей вже досить щоб зробити певні висновки. Наприклад, якщо на комп'ютері працює SSH-, веб-, проксі-сервер і ще, наприклад Samba (інструмент для обміну файлами), то зрозуміло, що вони цілком можуть містити в собі вразливості. Для більш глибокої розвідки відмінно підійде опція А сканера Nmap. Команда виглядає так:

nmap -A 192.168.91.62

Даний інструмент надає більше відомостей. Можна побачити, яка операційна система використовується системою, версії спеціальних сервісів, як встановлюється контент, час в системі. Програма відразу покаже дрібні недоліки, наприклад недостатню надійний FTP-пароль.

Тепер зібравши достатню кількість відомостей, необхідно проаналізувати їх і виконати онлайн-перевірку сайту вразливість за допомогою KaliLinux.

Аналіз і сканування

На даний момент популярним методом для виявлення вразливостей веб-сайтів є так званий fuzzing. Цей метод полягає у навмисному передачі великого обсягу різноманітних даних до веб-ресурсу, щоб виявити слабкі місця в системі. Спостерігаючи, як додатки реагують на такі атаки, можна визначити потенційні вразливості.

Fuzzing дозволяє знайти слабкі місця в системі, але часто складно точно зрозуміти природу помилок у роботі додатків. Ефективнішим підходом є поєднання fuzzing з ручним аналізом, але це вимагає доступу до вихідного коду ресурсу.

Важливо пам’ятати, що fuzzing атаки передбачають передачу великих обсягів інформації, тому цей процес може займати багато часу. Також слід враховувати, що система захисту може реагувати на ці атаки як на реальні загрози.

Перелік інструментів для процедури сканування:

1. WPScan: Спеціальна розробка на основі Ruby для аналізу веб-сайтів на WordPress. Інструмент має відкритий код доступу і простий у використанні. Він підходить для ресурсів, які не часто оновлюються і мають багато планів. WPScan проводить сканування видалено, без доступу до вихідного коду.

2. BurpSuite: Потужний інструмент для виявлення вразливостей веб-сайтів і додатків. BurpSuite аналізує всі форми веб-ресурсу, тестує заголовки, запити, сканує URL, аналізує JavaScript-код і виявляє XSS-вразливості. Це універсальна утиліта з широким спектром функцій, але вона досить складна у використанні.

3. SQLMap: Інструмент для сканування веб-сайтів на наявність SQL-вразливостей. Він виявляє небезпечні місця, де можуть статися SQL-ін'єкції.

Пробна експлуатація

Це завершальний етап у процесі виявлення слабких місць, через які може відбутися злом веб-ресурсу. Якщо вдається усунути небезпеку, задача вважається вирішеною. Однак деякі проблеми вимагають серйозних перевірок, які краще не виконувати на виробничих системах. Для цього рекомендується створити віртуальне середовище і в ньому тестувати всі процеси.

Спеціальний інструментарій для пробної експлуатації:

1. BurpSuite: Використовується для виявлення XSS-вразливостей сайту і їх перевірки шляхом експлуатації.

2. SQLMap: Засіб для виявлення SQL-вразливостей сайту і їх перевірки шляхом експлуатації.

3. Metasploit: Середовище для експлуатації виявлених вразливостей. Metasploit містить готові експлойти для плагінів і сервісів, виявлених на початкових етапах сканування.

Корегування

Завершальний крок. Тепер необхідно вести в систему всі необхідні виправлення. Відомості про вразливість вже зібрані, залишилося тільки ними скористатися. Тому якщо самостійно вдалося виявити небезпечні щілини, то їх легко знайдуть і хакери. Було перераховано лише кілька найбільш популярних сервісів, за допомогою яких виявляються вразливості сайтів. Серед цих програм є

й такі, які представляють собою промисловий стандарт. Проте, будь-які з них здатні забезпечити веб-ресурс або інфраструктуру.

2.2. Інструменти тестування веб-ресурсів

Найпопулярніші сканери вразливостей сайтів. Для служб інформаційної безпеки критично важливо мати спеціалізовані інструменти для тестування систем на наявність вразливостей. Нові загрози з'являються щодня, тому важливо вміти вчасно їх знаходити та усувати.

Завдяки спеціальним технологіям фахівці можуть сканувати всі компоненти системи, включаючи додатки, операційні системи та інше обладнання. Програми для пошуку вразливостей сайтів дозволяють безперервно запускати сканування мережі та виявляти небезпечні місця.

OpenVAS – це програма, яка дозволяє виконувати комплексні перевірки серверів та всіх підключених пристроїв системи. Сканер OpenVAS знаходить IP-адреси, а потім, використовуючи відкриті порти, здійснює пошук незахищених служб. Він виявляє будь-які неправильні конфігурації або "діри" в усіх складових системи.

Програма автоматично формує звіт про виконану роботу і надсилає його власнику ресурсу на електронну пошту, щоб той міг проаналізувати знайдені небезпеки та вжити заходів для їх усунення. Налаштування цього інструменту дозволяють запускати його з зовнішнього сервера, що дозволяє дізнатися більше про зловмисників, зрозуміти, через які порти або програми вони можуть діяти, і вжити екстрених заходів для їх знешкодження. Сканер OpenVAS є відмінним доповненням до системи виявлення та усунення небезпек. Він дозволяє здійснювати якісне тестування мережі та оперативно знаходити місця, доступні для зовнішніх атак.

Tripwire IP360 – це сервіс широкої дії, який сканує всю систему повністю, включаючи її локальні та хмарні контейнерні активи. Tripwire IP360 є популярним і потужним інструментом для перевірки сайтів на вразливість. Для перевірки

ресурсів достатньо виконати невелику кількість операцій. Використання Tripwire IP360 відкриває більше можливостей для адміністраторів та фахівців з інформаційної безпеки, дозволяючи комплексно управляти всією системою. Це можливо завдяки тому, що цей інструмент можна поєднувати з керуванням вразливостями та ризиками.

Nessus – інструмент, розроблений компанією Tenable, дозволяє не тільки виявляти вірусні елементи в усіх складових програмного забезпечення, але й видаляти шкідливі об'єкти та виправляти помилки в налаштуваннях. Сканер Nessus Professional запускає так звану попереджувальну процедуру безпеки, завдяки чому вразливості сайтів виправляються до того, як їх встигнуть використати шахраї. Також програма вносить виправлення в процедуру віддаленого виконання коду, якщо це необхідно.

Comodo HackerProof – інструмент, функціонал якого дозволяє щоденно контролювати наявність вразливостей на сайті.

Є кілька варіантів виконання сканування системи, які включають можливість попередження хакерських вторгнень та технологію SiteInspector для тестування нових веб-ресурсів.

Nexpose - розробка компанії Rapid7, що працює на відкритому вихідному коді і охоплює всі складові системи. Цей сканер є універсальним і зручним для адміністраторів, оскільки його легко інтегрувати з Metasploit. Сканер Nexpose Community визначає, наскільки сайт може бути вразливим до зовнішніх загроз, та пропонує відповідні методи їх усунення. Протягом року цей інструмент можна використовувати безкоштовно, а потім за бажанням придбати платну версію.

Vulnerability Manager Plus - інструмент від ManageEngine, який з'явився на ринку порівняно недавно і має широкий спектр можливостей. Його функціонал дозволяє службам інформаційної безпеки переглядати веб-ресурс очима хакера і визначати потенційні точки вторгнення. Цей інструмент включає автоматичне сканування, оцінку ризиків ПЗ, виявлення та виправлення помилок налаштування безпеки, аналіз впливу. Програма досліджує і усуває вразливості нульового дня,

підсилює захист веб-сервера. Безкоштовна версія дозволяє встановити сканер на 25 об'єктів.

Nikto - безкоштовний інструмент, який дозволяє тестувати функціонал сервера, досліджувати його роботу, виявляти слабкі місця, які можуть бути доступні для атак. Nikto також може перевіряти роботу протоколів HTTPS, HTTPD та HTTP і швидко тестувати кілька серверних портів одночасно.

Wireshark - один з найпотужніших інструментів для сканування, активно використовується на державних підприємствах і в установах охорони здоров'я для забезпечення інформаційної безпеки мереж урядових об'єктів та в інших важливих галузях. Після виявлення загрози, програма блокує її і здійснює перевірку. Підходить для використання на Windows, Linux і Mac OS.

Wireshark вирізняється серед інших аналізаторів завдяки трьохпанельному браузеру пакетів та зручному графічному інтерфейсу. Цей сканер підтримує роботу з різноманітними протоколами, такими як WEP, SSL/TLS, Kerberos.

Aircrack-ng призначений для забезпечення безпеки WiFi-мереж. Він дозволяє проводити аудит, моніторити роботу WiFi-з'єднань, контролювати їх безпеку. Програма також використовується як хакерський інструмент, забезпечена картами та драйверами, необхідними для імітації зовнішніх вторгнень. Aircrack-ng знаходить загублені ключі та зберігає важливі дані. Вона підходить для роботи з операційними системами Windows, OS X, Linux, NetBSD, Solaris.

Retina Network Security Scanner (Ретина) має відкритий вихідний код, а виявлення та усунення вразливостей сайтів здійснюється з центрального положення. Функціонал програми включає коригування, конфігурацію, формування відповідної звітності, аналіз баз даних, серверів та користувацьких програм. Retina інтегрується з vCenter і віртуальними середовищами для сканування.

2.3. Порівняння продуктів для захисту веб-сайтів

Цей розділ містить огляд існуючих аналогів брандмауерів.

Брандмауер - це мережевий пристрій безпеки, який контролює вхідний і вихідний мережевий трафік, дозволяючи або блокуючи пакети даних відповідно до встановлених правил безпеки. Його основна мета - створити бар'єр між вашою внутрішньою мережею та зовнішніми джерелами трафіку (наприклад, Інтернетом), щоб запобігти проникненню зловмисного трафіку, такого як віруси та хакери.

AWS WAF

AWS WAF (Web Application Firewall) – це брандмауер для веб-додатків, який забезпечує захист додатків і API від поширених мережевих атак і ботів, що можуть впливати на доступність, створювати загрози безпеці або використовувати надмірну кількість ресурсів API чи програми. На рисунку 2.1 представлено інтерфейс AWS WAF.

Рис. 2.1 – Інтерфейс AWS WAF

AWS WAF має як переваги, так і недоліки, які наведені нижче.

Переваги AWS WAF:

- швидкий старт;

- забезпечує повний контроль над тим, як трафік досягає додатків користувача;

- можливість створювати правила безпеки для контролю трафіку від ботів та блокування атак за поширеними шаблонами, такими як SQL-ін'єкції чи міжсайтовий скриптинг;

- можливість налаштування правил фільтрації для певних шаблонів трафіку;

- наявність попередньо налаштованого набору правил, керованих AWS, для вирішення проблем, таких як 10 основних ризиків безпеки OWASP та автоматизовані боти, що споживають зайві ресурси, спотворюють метрики або призводять до простоїв. Ці правила регулярно оновлюються з появою нових загроз;

- повнофункціональний API для автоматизації процесів створення, розгортання та обслуговування правил безпеки;

- можливість масштабування додатків відповідно до поточних потреб користувача, що здійснюється автоматично без необхідності додаткових даних від адміністраторів.

Недоліки AWS WAF:

- обмежена інтеграція з деякими сторонніми продуктами;

- висока вартість;

- додаткові сервіси мають доступ до інформації про трафік.

Imperva WAF

Imperva Web Application Firewall (WAF) – це брандмауер, який захищає веб-додатки від кібератак. Imperva WAF постійно адаптується до нових загроз, знижує ризик витоку даних та запобігає захопленню облікових записів. На рисунку 2.2 представлено інтерфейс Imperva WAF. Далі наведено список переваг та недоліків цього продукту.

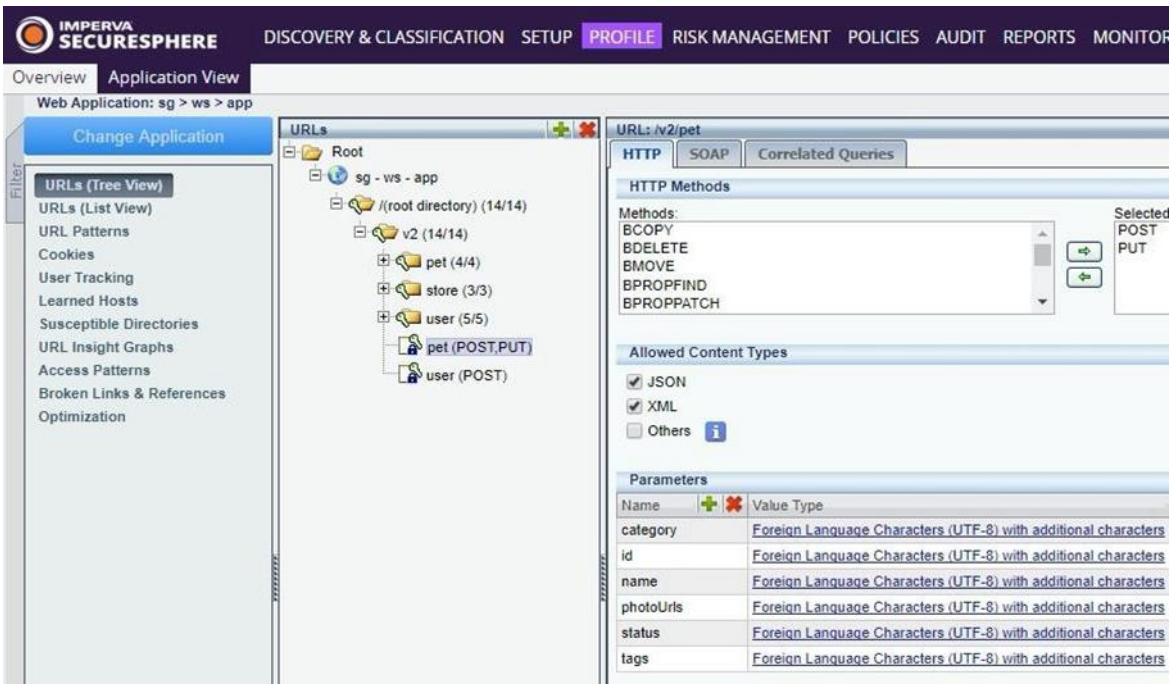

Рис. 2.2 – інтерфейс Imperva WAF

Переваги Imperva WAF:

- містить шаблони, які можуть виявляти зловмисний трафік, включаючи типи запитів, аномальні відповіді сервера та відомі шкідливі IP-адреси;
- використовує алгоритми штучного інтелекту для аналізу поведінкових шаблонів трафіку, що дозволяє виявляти аномалії, які свідчать про атаки. Це дозволяє виявляти атаки, що не відповідають відомим шкідливим шаблонам;
- може визначати типові запити, URL-адреси, значення та дозволені типи даних, що дозволяє ідентифікувати та блокувати потенційно шкідливі запити;
- адміністратори можуть створювати правила безпеки для трафіку програми, що дозволяє налаштовувати роботу WAF відповідно до потреб організації та запобігати блокуванню легітимного трафіку.

Недоліки Imperva WAF:

- складність освоєння керування програмою через велику кількість функціоналу;
- висока вартість;
- орієнтований на великі корпоративні системи.

Azure Microsoft WAF Брандмауер веб-застосунків Azure – це хмарна служба, яка захищає веб-додатки від поширених методів веб-злому, таких як SQL-ін'єкції та вразливості безпеки, як-от міжсайтовий сценарій. На рисунку 2.3 показано інтерфейс Azure Microsoft WAF.

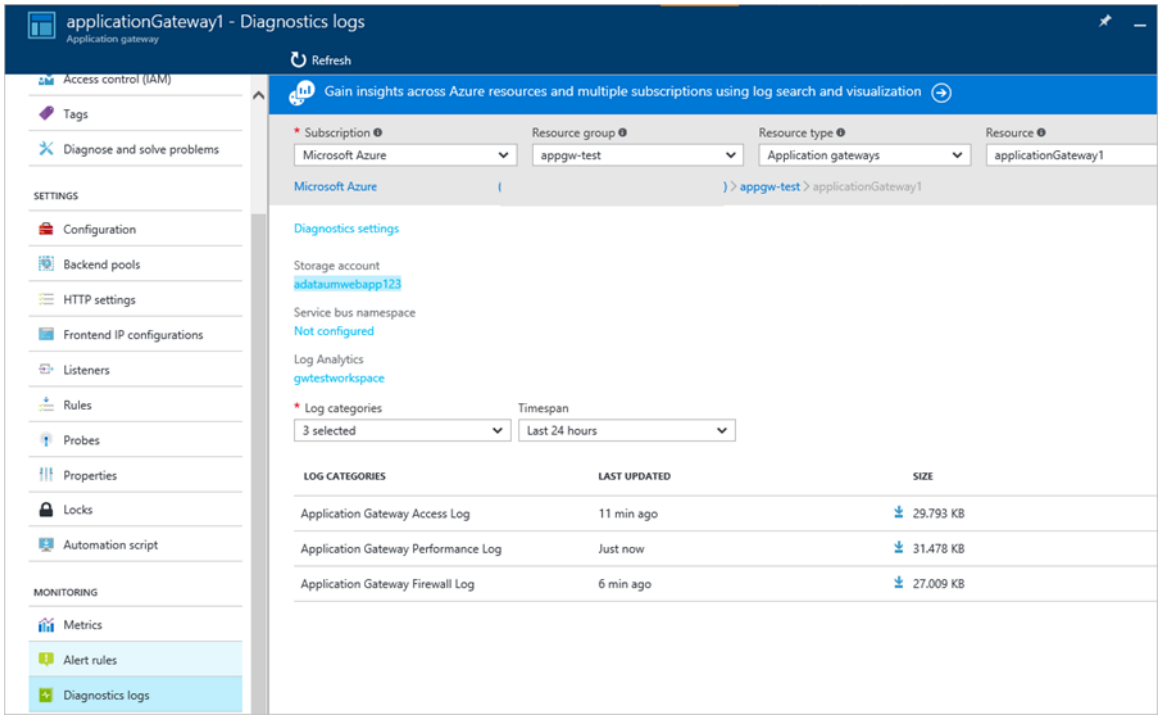

Рис. 2.3 – Інтерфейс Azure Microsoft WAF

Переваги Azure Microsoft WAF:

- можливість одночасного захисту кількох веб-застосунків. Один екземпляр шлюза додатків може включати до 40 веб-сайтів, захищених брандмауером;

- можливість створення налаштованих політик WAF для кількох сайтів під захистом одного WAF;

- можливість захисту веб-застосунків від шкідливих ботів за допомогою набору правил репутації IP-адрес;

- можливість відстеження атак на веб-застосунки за допомогою журналу WAF у реальному часі. Цей журнал інтегрований з Azure Monitor, що дозволяє відстежувати сповіщення WAF та тенденції;

- можливість створення та налаштування правил і груп правил WAF

відповідно до вимог програми.

Недоліки Azure Microsoft WAF:

- розгортання є складним, що ускладнює його освоєння для непрофесіоналів;

- високовартісний продукт.

AWS Shield

AWS Shield — це служба безпеки, яка захищає веб-додатки, розміщені в загальнодоступній хмарі Amazon Web Services, від розподілених атак типу «відмова в обслуговуванні» (DDoS). На рисунку 2.4 показано інтерфейс AWS Shield.

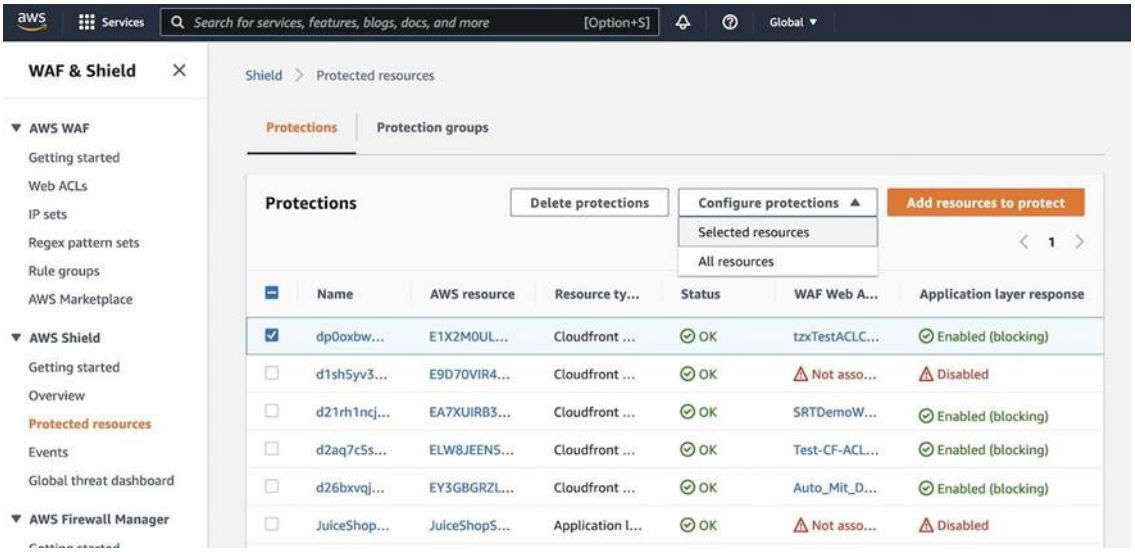

Рис. 2.4 –Інтерфейс AWS Shield

Відповідно до Amazon, AWS Shield виявляє та захищає від трьох типів DDoS-атак: атак на рівні інфраструктури, включаючи затоплення протоколу дейтаграм користувача (UDP); атак виснаження стану, включаючи SYN-флуди; та атак на прикладному рівні, включаючи HTTP-флуди. Для запобігання DDoS-атакам на прикладному рівні, IT-команди повинні написати та впровадити правила за допомогою брандмауера веб-додатків AWS.

Переваги AWS Shield:

- легке розгортання та інтеграція (ви можете безкоштовно користуватися стандартним сервісом Amazon Shield у своєму обліковому записі AWS. Окрім

цього, він легко інтегрується з будь-якою іншою службою AWS, якщо ви використовуєте їх для розробки або керування своїм веб-додатком);

- можливість налаштування потрібного типу/сценарію захисту (якщо ви хочете захистити свою програму від певної ніші атаки DDoS, це дозволить вам налаштувати свої дії та запобігти цій атаці);

- можливість перегляду статистики Live Statistics Insight (інформація про те, які типи трафіку вам направляють зловмисники, звідки вони надсилають його та на що це впливає);

- наявність безкоштовної версії (Amazon Shield має безкоштовну версію з базовим функціоналом, для повного використання можливостей необхідно придбати повну версію);

- хороша документація (Amazon Shield має детальну документацію, яка розписує шляхи використання);

- швидкий старт (вам не потрібні глибокі знання про AWS або інші служби захисту, щоб правильно розгорнути їх і захистити свій бізнес).

Недоліки AWS Shield:

- висока абонентська плата (незважаючи на те, що стандартна версія Amazon Shield є безкоштовною, для найкращого сервісу потрібно оновити до розширеної версії. Плата за реєстрацію становить 3000 доларів США, не враховуючи додаткові витрати);

- мінімальний термін підписки на 1 рік для розширеного плану (для використання платної версії з додатковими функціями потрібно взяти зобов’язання на принаймні один рік);

- найкращий функціонал доступний лише у платній версії (стандартна версія дає змогу лише оцінити рівень захисту, який Amazon Shield може забезпечити. Для повного захисту від DDoS-атак потрібно заплатити за доступ до топових функцій).

Cloudflare WAF

Cloudflare WAF, або брандмауер веб-застосунків, допомагає захистити веб-програми, фільтруючи та відстежуючи трафік HTTP між веб-програмою та Інтернетом. На рисунку 2.5 показано інтерфейс Cloudflare. Зазвичай він захищає

веб-додатки від таких атак, як міжсайтова підробка, міжсайтовий сценарій (XSS), включення файлів і SQL-ін'єкції, серед інших.

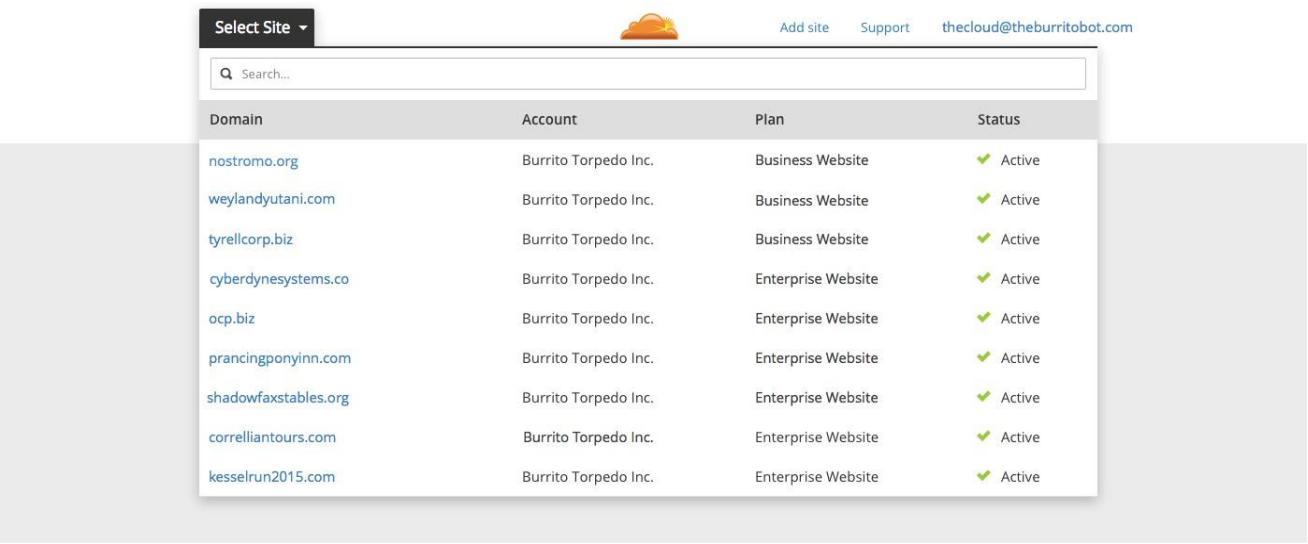

Рис. 2.5 – Інтерфейс Cloudflare

Переваги Cloudflare WAF:

- Cloudflare безкоштовний для простих користувачів і дуже легко налаштовується;

- приховує вашу IP-адресу, що ускладнює хакерам можливість атакувати сервер;

- дозволяє доступ лише “справжнім” користувачам, зберігаючи ресурси веб-сайту та підвищуючи його швидкість;

- захищає сайт від DoS і DDoS атак;

- надає безкоштовний сертифікат SSL.

Недоліки Cloudflare WAF:

- оскільки Cloudflare діє як посередник між сайтом та Інтернетом, якщо він вийде з ладу, веб-сайт також стане недоступним;

- існує ймовірність блокування “справжніх” (легітимних) користувачів сайту;

- неінформативні сповіщення;

- незручні журнали логів;

- дороговартісний для бізнес-користувачів;

- обмежені варіанти безпеки.

Windows Firewall

Брандмауер Windows – це програма Microsoft Windows, яка фільтрує інформацію, що надходить до вашої системи з Інтернету, і блокує потенційно шкідливі програми. Програмне забезпечення блокує роботу більшості програм через брандмауер. На рисунку 2.6 показано інтерфейс Windows Firewall. Він має низку переваг і недоліків.

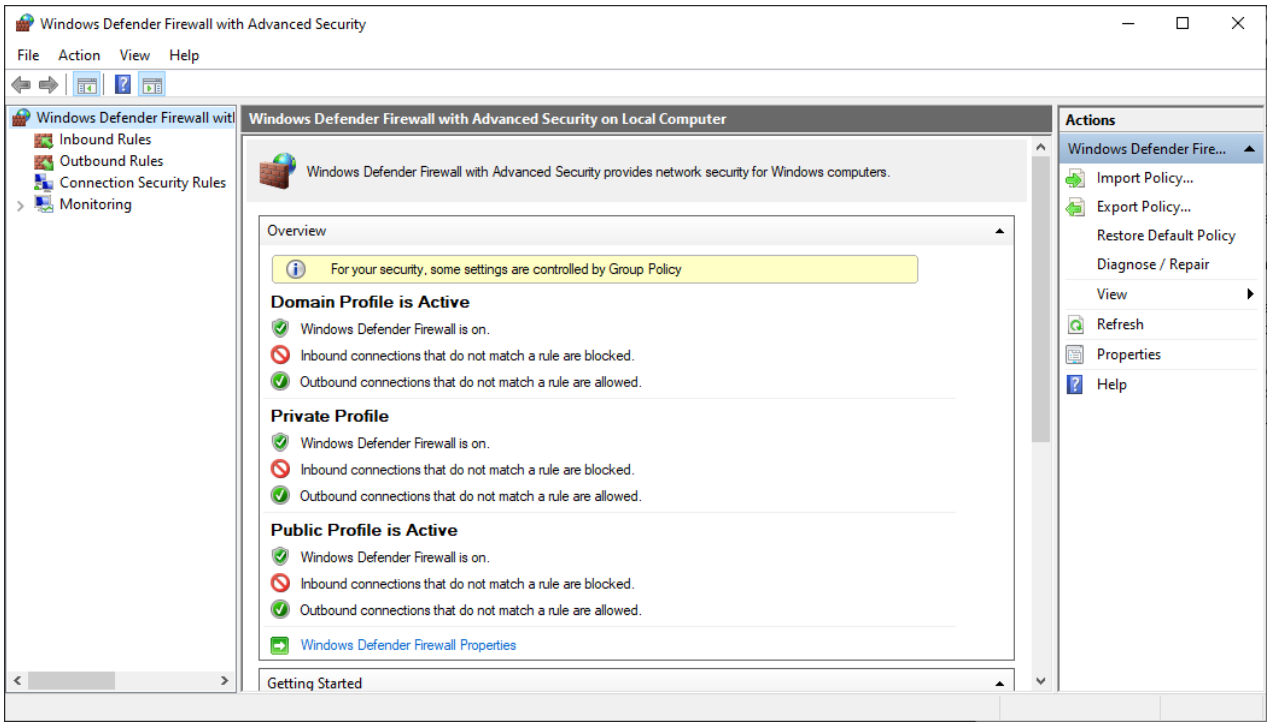

Рис. 2.6 – Інтерфейс Windows firewall

Переваги Windows Firewall:

- покращена ефективність в антивірусних тестах;

- безкоштовний і вбудований для пристроїв Microsoft;

- простота використання;

- комплексні функції для домашнього використання.

Недоліки Windows Firewall:

- відсутність вбудованої інформаційної панелі для всіх пристроїв, що використовують Windows Defender;

- уповільнення встановлення часто використовуваних програм;

- складність налаштування.

Порівняльний аналіз

Далі наводиться порівняльна характеристика аналогів у табличному вигляді (таблиця 2.1).

Таблиця 2.1.

Порівняльна характеристика

Назва	Вартість	Розрахований на	Просто та використання
AWS WAF	дороговартісне	великі системи	+
Imperva WAF	дороговартісне	великі системи	-
Azure MicrosoftWAF	дороговартісне	великі системи	-
AWS Shield	Дороговартісне (є безкоштовна версія)	великі системи	+
Cloudflare	дороговартісне (є безкоштовна версія)	невеликі та великі системи	-
Windows firewall	входить у вартістьОС Windows	невеликі системи (ПК)	-

У таблиці, зображеній вище, проводиться порівняння за такими критеріями:

- вартість (наявність безкоштовної версії може привабити користувачів);

- розмір систем, для захисту яких розрахований застосунок (допомагає визначити коло користувачів – обслуговує великі чи невеликі системи);

- простота використання (чи легко непрофесіоналу почати використовувати застосунок).Продовження таблиці 2.1

Продовження таблиці 2.1

Порівняльна характеристика

Назва	Створення політик	Фільтрація зловмисних запитів	Збір та аналіз даних по трафіку
AWS WAF	+	+	+
Imperva WAF	+	+	+
Azure Microsoft WAF	+	+	+
AWS Shield	-	+	+
Cloudflare	+	+	+
Windows firewall	+	+	+

У таблиці, зображеній вище, проводиться порівняння за такими критеріями:

- наявність можливості створення політик (чи може користувач самостійно налаштовувати політики, що забезпечує гнучкість);

- наявність фільтрації зловмисного трафіку;

- наявність можливості збору та аналізу даних трафіку (дозволяє відстежувати тенденції трафіку та запобігати атакам).політики – це забезпечує гнучкість), наявність фільтрації зловмисного трафіку, наявність можливості збору та аналізу даних трафіку (дозволяє відслідковувати тенденції трафіку, запобігати атакам).

Продовження таблиці 2.1

Порівняльна характеристика

Назва	є API, для автоматизуваазації процесів створення, розгортання та обслуговування політик	Рекомендаціїщодо застосування політик	Обробка даних сервісом, який контролюється користувачем
AWS WAF	+	-	-
Imperva WAF	+	-	+
Azure MicrosoftWAF	+	-	-
AWS Shield	+	-	-
Cloudflare	+	-	-
Windows firewall	-	-	+

У таблиці, зображеній вище, проводиться порівняння за такими критеріями:

- наявність API для автоматизації процесів створення, розгортання та обслуговування політик (дозволяє інтегруватися з іншими сервісами);

- наявність рекомендацій щодо застосування політик (дозволяє захищати сайт на основі аналізу тенденцій трафіку);

- обробка даних сервісом, який контролюється користувачем (дозволяє уникнути викрадення даних про трафік).

У результаті порівняльного аналізу були виявлені сильні та слабкі сторони. Всі аналоги є ефективними продуктами для захисту великих систем, з можливістю створення політик, фільтрації запитів на основі цих політик, а також збору і аналізу трафіку. Однак, більшість з представлених аналогів є досить складними для освоєння звичайним користувачем.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВЕБ-САЙТІВ ЗА ДОПОМОГОЮ WAF AZURE В ІНФОРМАЦІЙНІЙ СИСТЕМІ

3.1. Аналіз функцій Azure WAF

Azure була розроблена Корпорацією Microsoft в 2008 році як платформа хмарних обчислень для створення, розгортання та управління додатками і службами через глобальну мережу центрів обробки даних, керованих Компанією Microsoft.

Azure Web Application Firewall (WAF) є потужним інструментом, який інтегрується в Azure Application Gateway, забезпечуючи комплексний захист веб-додатків від різноманітних загроз. У цьому розділі розглянемо основні функції Azure WAF, які роблять його ефективним засобом для захисту веб-сайтів.

Інтеграція з Azure Application Gateway

Azure WAF тісно інтегрується з Azure Application Gateway, що дозволяє організаціям отримувати переваги від об'єднання функцій балансування навантаження та захисту веб-додатків. Це забезпечує високу доступність та масштабованість веб-додатків, а також спрощує процес управління безпекою.

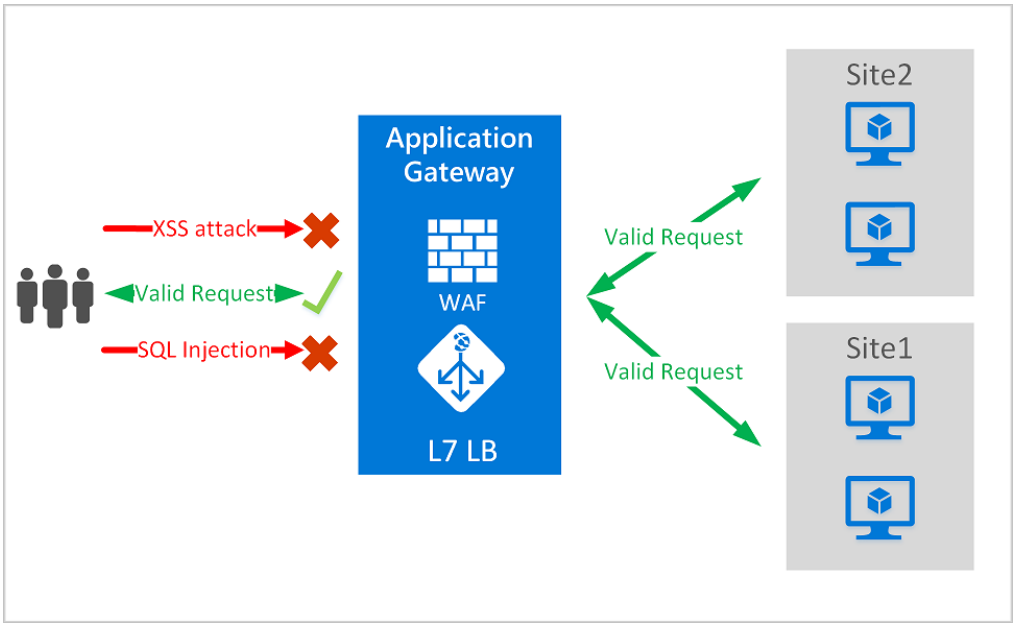

Рис. 3.1 – Azure Application Gateway

Захист від загроз OWASP Top 10

Azure WAF забезпечує захист від найбільш поширених веб-уразливостей, які входять до OWASP Top 10, таких як:

- SQL-ін'єкції
- Міжсайтовий скриптинг (XSS)
- Впровадження коду
- Вразливості безпеки конфігурації
- Вразливості ідентифікації та автентифікації

Це досягається завдяки використанню правил та підписів, які автоматично оновлюються, щоб відповідати новим загрозам.

Автоматичне оновлення правил безпеки

Azure WAF регулярно оновлює свої правила безпеки, що дозволяє оперативно реагувати на нові загрози та уразливості. Це забезпечує актуальний захист без необхідності вручну оновлювати налаштування WAF, зменшуючи адміністративне навантаження на команди безпеки.

Підтримка настроюваних правил

Крім вбудованих правил безпеки, Azure WAF дозволяє створювати та застосовувати настроювані правила для специфічних потреб організації. Це забезпечує гнучкість у налаштуванні захисту відповідно до конкретних вимог веб-додатків та інфраструктури.

Моніторинг та аналітика

Azure WAF забезпечує розширені можливості моніторингу та аналітики через Azure Monitor, Application Insights та інші інструменти. Це дозволяє детально аналізувати трафік, виявляти підозрілі активності та реагувати на інциденти безпеки у реальному часі. Користувачі можуть отримувати звіти та оповіщення про події безпеки, що допомагає оперативно вживати заходів для їх усунення.

Захист від DDoS-атак

Azure WAF забезпечує базовий захист від DDoS-атак шляхом інтеграції з Azure DDoS Protection. Це дозволяє автоматично виявляти та пом'якшувати

DDoS-атаки на рівні мережі та програми, забезпечуючи безперервну роботу веб-додатків навіть під час інтенсивних атак.

SSL/TLS шифрування

Azure WAF підтримує SSL/TLS шифрування, що забезпечує безпеку передачі даних між клієнтами та серверами. Це дозволяє захищати чутливу інформацію від перехоплення та забезпечує конфіденційність даних.

Управління політиками безпеки

Azure WAF дозволяє створювати та керувати політиками безпеки, які можуть бути застосовані до різних веб-додатків та служб. Це забезпечує централізоване управління безпекою та спрощує адміністрування політик безпеки.

Легкість налаштування та масштабованість

Azure WAF має інтуїтивно зрозумілий інтерфейс, що спрощує процес налаштування та управління. Крім того, WAF легко масштабується, що дозволяє адаптуватися до змін у трафіку та потребах бізнесу без зниження рівня захисту.

Вбудована підтримка API

Azure WAF надає вбудовану підтримку API, що дозволяє автоматизувати процеси налаштування та управління через програмні інтерфейси. Це забезпечує гнучкість та інтеграцію з іншими системами безпеки та управління.

Інтеграція з іншими сервісами Azure

Однією з ключових переваг Azure WAF є його інтеграція з іншими сервісами Azure, такими як Azure Security Center, Azure Sentinel та Azure Active Directory. Це забезпечує комплексний підхід до безпеки, дозволяючи користувачам отримувати детальну аналітику, автоматизувати процеси виявлення та реагування на загрози, а також інтегрувати безпекові функції у загальну інфраструктуру Azure.

Моніторинг WAF

Важливо відстежувати працездатність шлюзу додатків. Це можна підтримувати, інтегруючи WAF та програми, захищені за допомогою журналів Microsoft Defender для хмари, Azure Monitor та Azure Monitor.

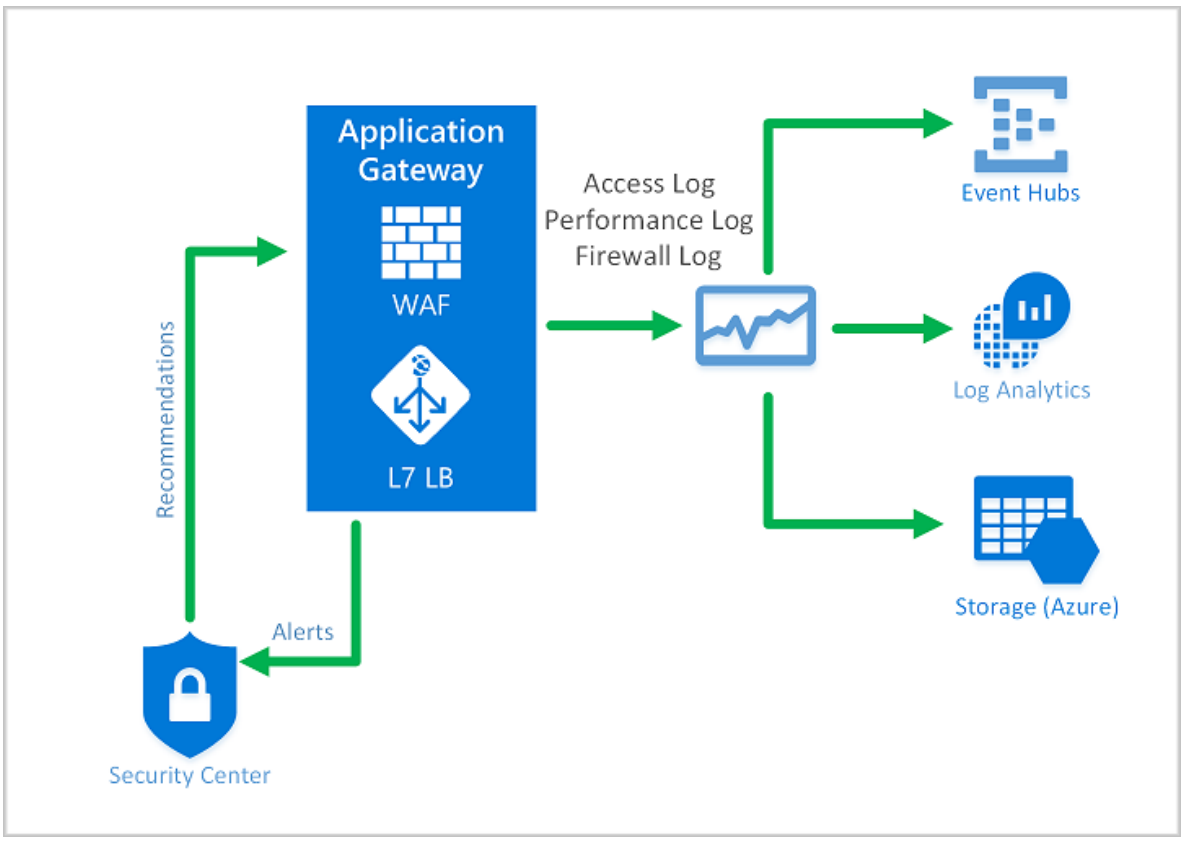

Рис. 3.2 – Моніторинг WAF

Azure Monitor

Журнали Шлюзу додатків інтегровані з Azure Monitor . Це дозволяє відстежувати діагностичні відомості, включаючи журнали та оповіщення WAF. Ви можете застосувати цю можливість на вкладці Діагностика для ресурсу Шлюзу додатків на порталі або безпосередньо через службу Azure Monitor. Для отримання додаткових відомостей див. статтю про діагностику для Шлюзу додатків.

Режими WAF

WAF Шлюзу програм можна налаштувати для роботи в наступних двох режимах.

Режим виявлення: відстежує та реєструє всі оповіщення про загрози. Введення журналу діагностики для Шлюзу додатків можна увімкнути в розділі Діагностика . Також потрібно переконатися, що вибрано та увімкнено параметр ведення журналу WAF. Брандмауер веб-застосунку не блокує вхідні запити, коли він працює в режимі виявлення.

Режим запобігання: блокує вторгнення та атаки, виявлені правилами. Зловмисник отримує повідомлення "403 unauthorized access" (несанкціонований доступ) і таке підключення переривається. У режимі запобігання подібні атаки також заносяться до журналів WAF.

Підсистеми WAF

Підсистема брандмауера веб-застосунків Azure (WAF) — це компонент, який перевіряє трафік і визначає, чи містить запит підпис, який може вказувати на потенційну атаку. Якщо використовується CRS 3.2 або пізнішої версії, WAF працює на базі нової підсистеми WAF , яка забезпечує більш високу продуктивність та покращений набір функцій. Якщо ж використовуються більш ранні версії CRS, WAF працює на старішій підсистемі. Нові функції доступні лише у новому ядрі Azure WAF.

Дії WAF

Ви можете вибрати, яка дія виконується, коли запит відповідає умові правила. Підтримуються такі дії:

Дозволити: запит пропускається через WAF і передається до серверної частини. Жодні правила з нижчим пріоритетом не можуть блокувати такий запит. Дозволити дії застосовні лише до набору правил Bot Manager і не застосовні до набору правил Core.

Блокувати: запит блокується, а WAF надсилає клієнту відповідь, не перенаправляючи запит до серверної частини.

Занести до журналу: WAF записує запит до своїх журналів та продовжує аналіз правил із нижчим пріоритетом.

Оцінка аномалій. Це стандартна дія для набору правил CRS, де загальна оцінка аномалій збільшується при зіставленні правила з цією дією. Оцінка аномалій не застосовується до набору правил Bot Manager.

Microsoft Defender для хмари

Defender для хмари дозволяє запобігати, виявляти загрози та реагувати на них. Він забезпечує більш високу поінформованість про безпеку ресурсів Azure та контроль над ними. Шлюз додатків інтегрований з Defender для хмари .

Defender для хмари перевіряє середовище для виявлення незахищених веб-застосунків. Він може передати до WAF у Шлюзі додатків рекомендації щодо захисту виявлених вразливих ресурсів. Брандмауери створюються безпосередньо в Defender для хмари. Ці екземпляри WAF інтегровані з Defender для хмари. Вони надсилають оповіщення та відомості про працездатність у Defender для хмари для створення звітів.

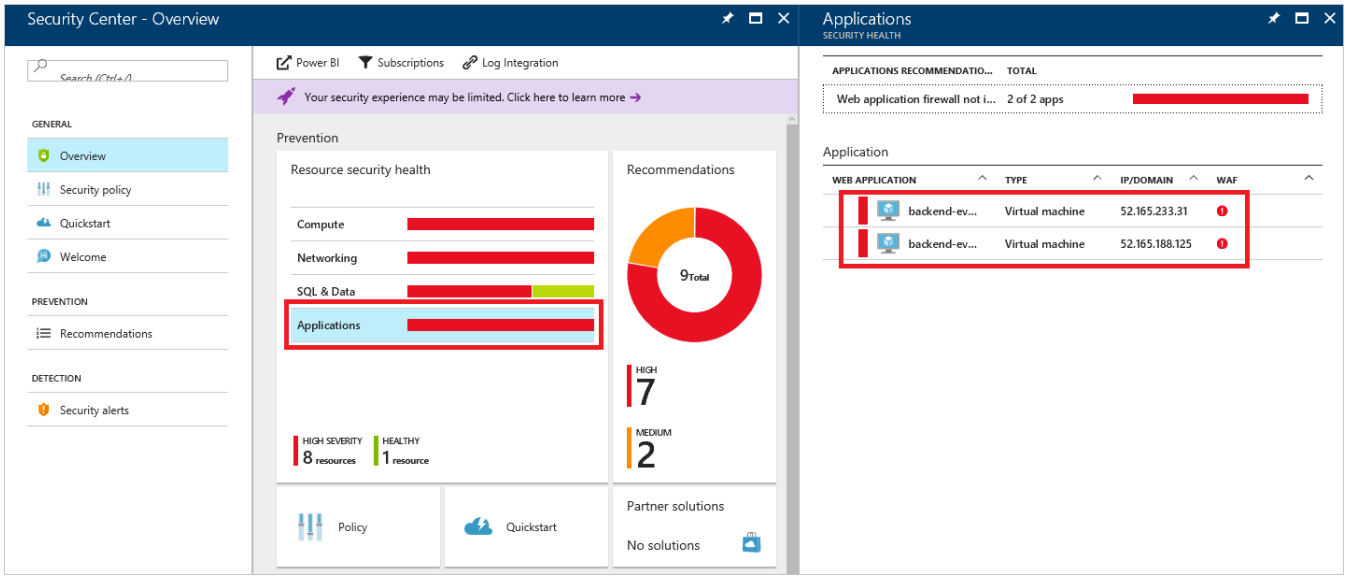

Рис. 3.3 – Приклад оповіщення

Microsoft Sentinel

Microsoft Sentinel – це масштабоване орієнтоване на хмару рішення для управління інформаційною безпекою та подіями безпеки (SIEM), а також автоматичного реагування в рамках оркестрації подій безпеки (SOAR). Microsoft Sentinel забезпечує інтелектуальні засоби для аналітики безпеки та аналітики загроз по всьому підприємству, надаючи єдине рішення для виявлення попереджень, візуального контролю загроз, запобігання полюванню та реагування на загрози.

За допомогою вбудованої книги подій брандмауера Azure WAF можна отримати загальні відомості про події безпеки для WAF. У книзі зберігаються події, застосовані правила та блокування, а також усі дані, які записуються до журналів брандмауера. Нижче наведено додаткові відомості про ведення журналу.

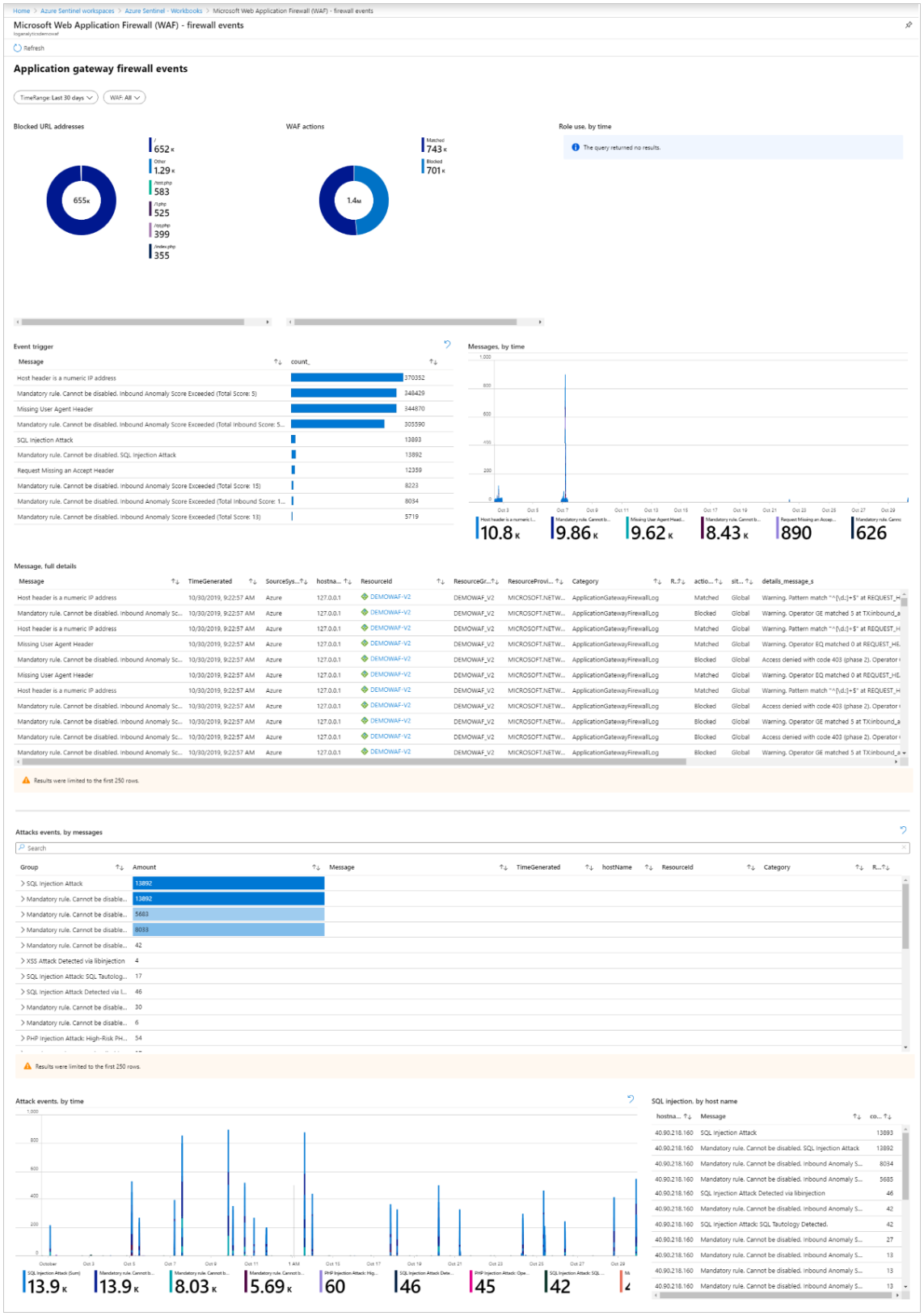

Рис. 3.4 – Книга подій

Ведення журналу

WAF у Шлюзі додатків надає докладні звіти про кожну з виявлених загроз.

Функція ведення журналів інтегрована з журналами агента Діагностика Azure. Оповіщення зберігаються у форматі JSON. Ці журнали можна інтегрувати з журналами Azure Monitor .

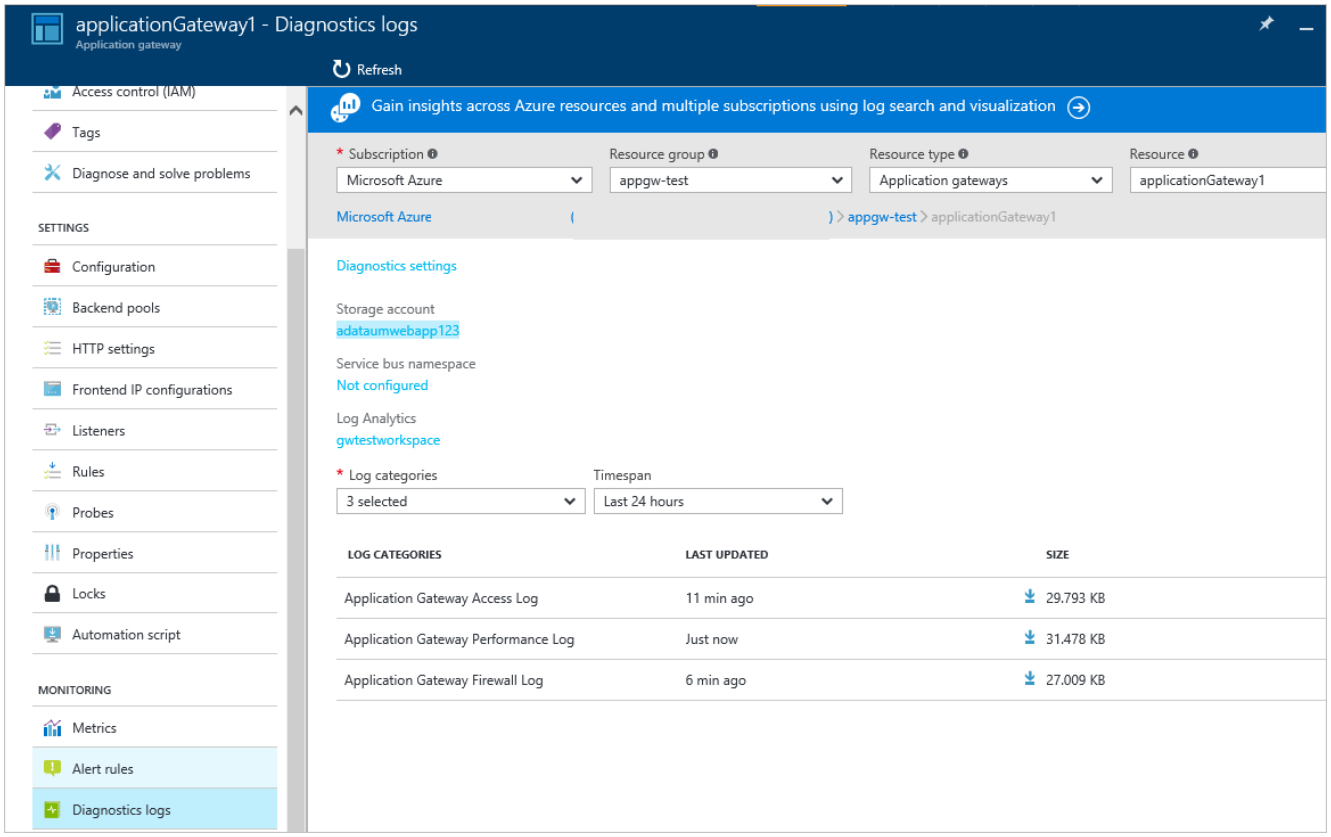

Рис. 3.5 – Ведення журналу

3.2. Налаштування та керування політиками безпеки Azure WAF

Налаштування та керування політиками безпеки є критично важливим аспектом використання Azure Web Application Firewall (WAF). Політики безпеки визначають правила та умови, за якими WAF аналізує та фільтрує вхідний і вихідний трафік, захищаючи веб-додатки від різних типів атак. У цьому розділі ми детально розглянемо процес створення, налаштування та керування політиками безпеки в Azure WAF.

Крок 1: Створення нової політики безпеки

Входимо в Azure Portal:

Відкриваємо браузер і переходимо на портал Azure (https://portal.azure.com). Входимо за допомогою своїх облікових даних.

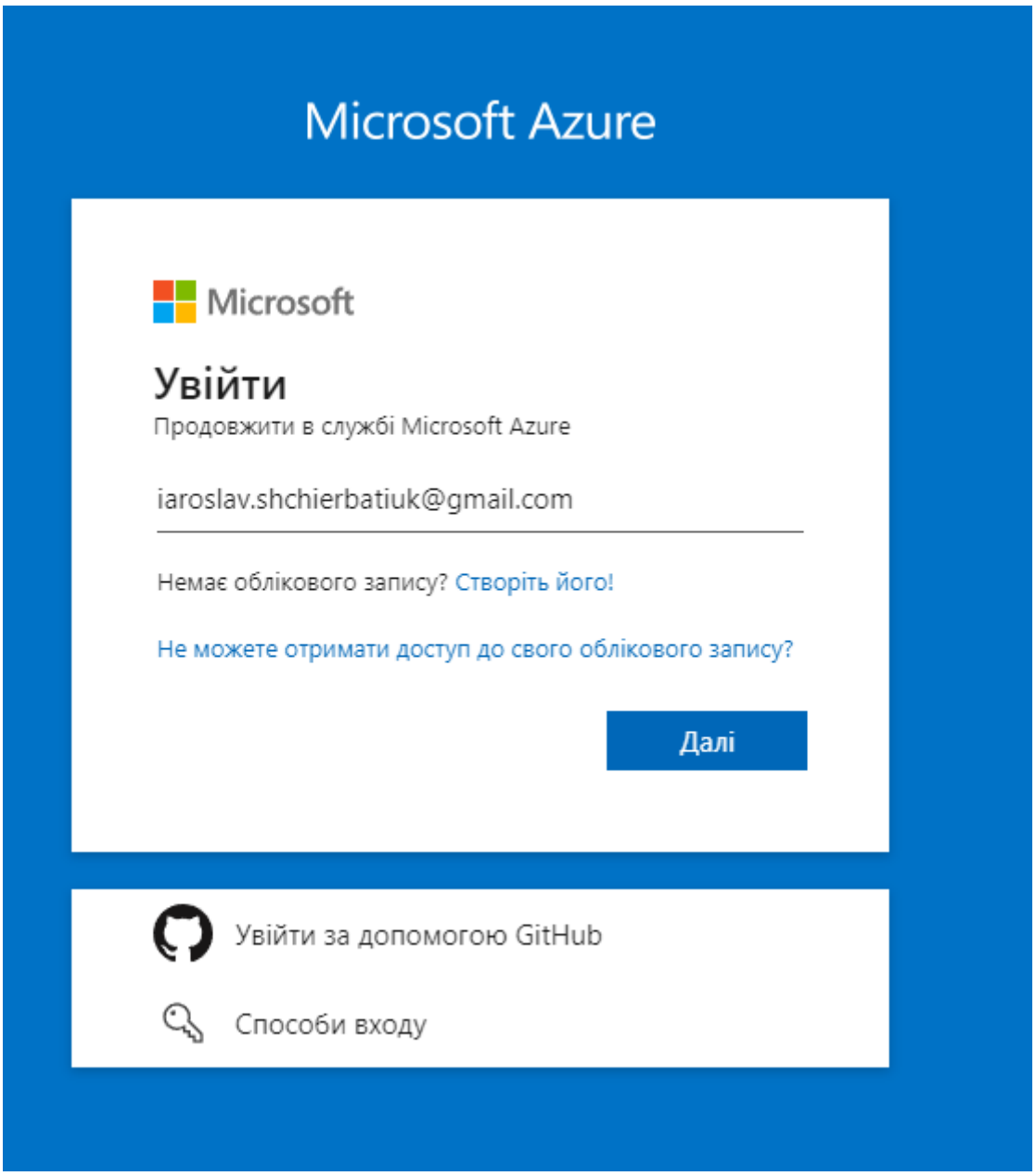

Рис. 3.6 – Ідентифікація в Microsoft Azure

Перехід до Azure WAF:

На головній сторінці Azure Portal знайдіть ваш ресурс Application Gateway або Front Door, до якого додано WAF.

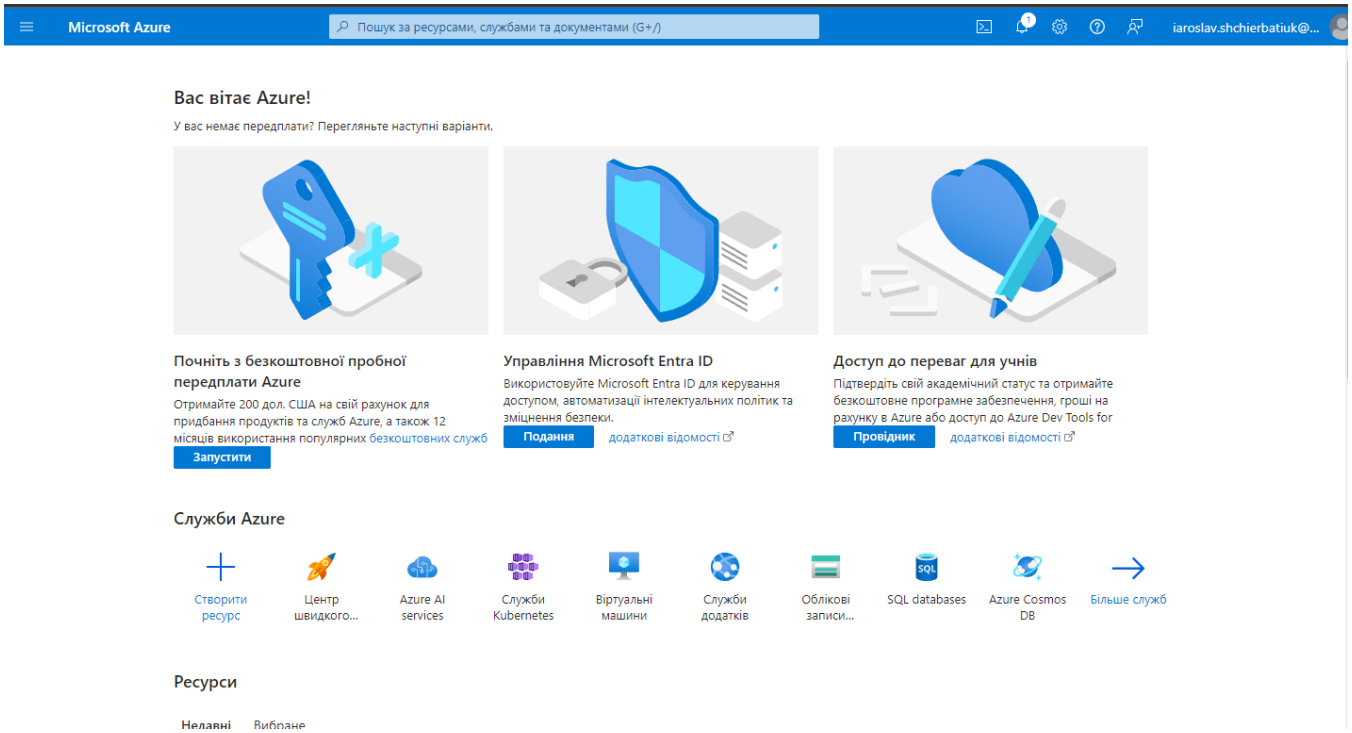

Рис. 3.7 – Головна сторінка в Microsoft Azure

На порталі Azure виберіть Створити ресурс . Введіть брандмауер веб-програми в полі пошуку служби пошуку та Marketplace та натисніть клавішу ENTER. Потім виберіть Брандмауер веб-застосунків (WAF).

На сторінці Створення політики WAF використовуйте такі значення, щоб заповнити вкладку Основні відомості .

Параметр	Значення
Об'єкт політики	Глобальний WAF (Front Door).
Рівень front door	Виберіть Преміум або Стандартний, щоб відповідати рівню Azure Front Door.
Передплата	Виберіть підписку.
Група ресурсів	Виберіть групу ресурсів, де міститься екземпляр Azure Front Door.
Ім'я політики	Введіть назву політики.
Стан політики	Вибрано.
Режим політики	Запобігання.

Рис. 3.8 – Таблиця значень

На сторінці Додавання налаштованого правила використовуйте такі тестові значення, щоб створити правило користувача.

Параметр	Значення
Ім'я правила, що налаштовується	FdWafCustRule
Стан	Активовано
Тип правила	Відповідає
Пріоритет	100
Тип відповідності	IP-адреса
Змінна зіставлення	SocketAddr
Операція	Не містить
IP-адреса або діапазон адрес	10.10.10.0/24
Наступна дія	Заборонити трафік

Рис. 3.9 – Тестові значення, щоб створити правило користувача

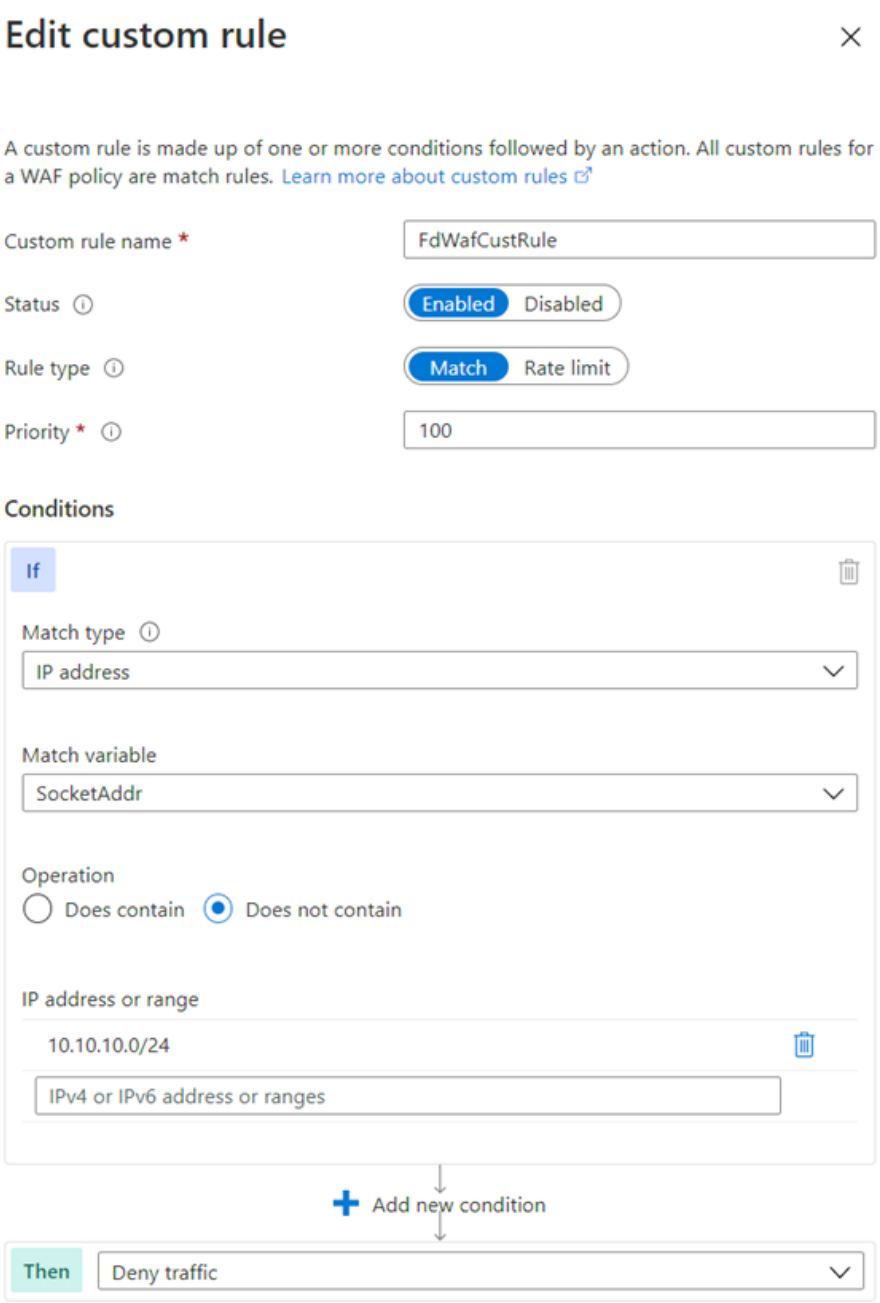

Рис. 3.10 – Створення політики WAF

Після завершення розгортання політики WAF перейдіть до імені зовнішнього вузла Azure Front Door. Ви повинні побачити налаштоване повідомлення про блокування.

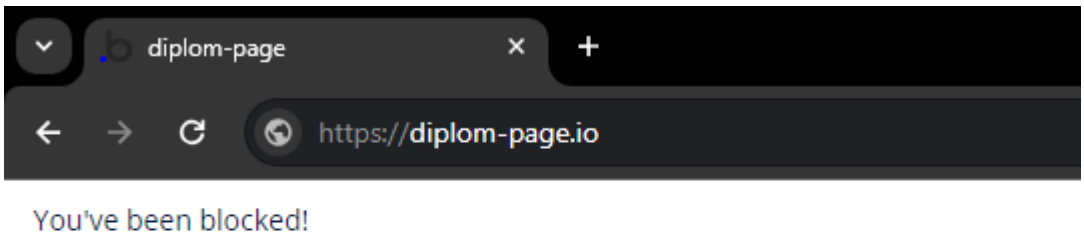

Рис. 3.11 – Налаштоване повідомлення про блокування

Зв'язування політики WAF із прослуховувачами дозволяє захистити декілька сайтів, що знаходяться за одним WAF, за допомогою різних політик. Наприклад, якщо у вас є п'ять сайтів за WAF, у вас може бути п'ять окремих політик WAF (по одній для кожного прослуховувача), щоб налаштувати винятки, настроювані правила та набори керованих правил для одного сайту, при цьому вони не будуть діяти для чотирьох, що залишилися. сайтів. Якщо потрібно застосувати одну політику до всіх сайтів, можна просто зв'язати її зі шлюзом додатків, а не з окремими прослуховувачами, тоді вона використовуватиметься глобально. Політики також можна застосувати до правил маршрутизації на основі шляху.

Можна створити будь-яку кількість політик. Щоб політика набула чинності після створення, її необхідно пов'язати зі шлюзом додатків, але можна пов'язати її з будь-яким поєднанням шлюзів додатків і прослуховувачів.

Якщо Шлюз додатків має пов'язану політику, а потім пов'язати іншу політику з прослуховувачем на цьому Шлюз додатків, політика прослуховувача набирає чинності, але тільки для прослуховувача, якому вони призначені. Політика Шлюза додатків, як і раніше, застосовуватиметься до всіх інших прослуховувачів, яким не призначена певна політика.

Створення політики

Спочатку створіть на порталі Azure базову політику WAF з керованим

набором стандартних правил (DRS). Угорі ліворуч на порталі виберіть Створити ресурс . Введіть WAF для пошуку, виберіть Брандмауер веб-застосунків і клацніть Створити. На сторінці “Створення політики WAF” на вкладці “Основні відомості” введіть наступні відомості та прийміть стандартні значення для інших параметрів:

Параметр	Значення
Об'єкт політики	Регіональний WAF (Шлюз додатків)
Відтік передплат	Виберіть ім'я передплати
Група ресурсів	Вибір групи ресурсів
Ім'я політики	Введіть унікальне ім'я для політики WAF.

Рис. 3.12 – Відомості для створення політики

Керовані правила

Правила OWASP, керовані Azure, включені за замовчуванням. Щоб вимкнути окреме правило групи правил, розгорніть правила в цій групі, встановіть прапорець перед номером потрібного правила і виберіть Вимкнути на вкладці вище.

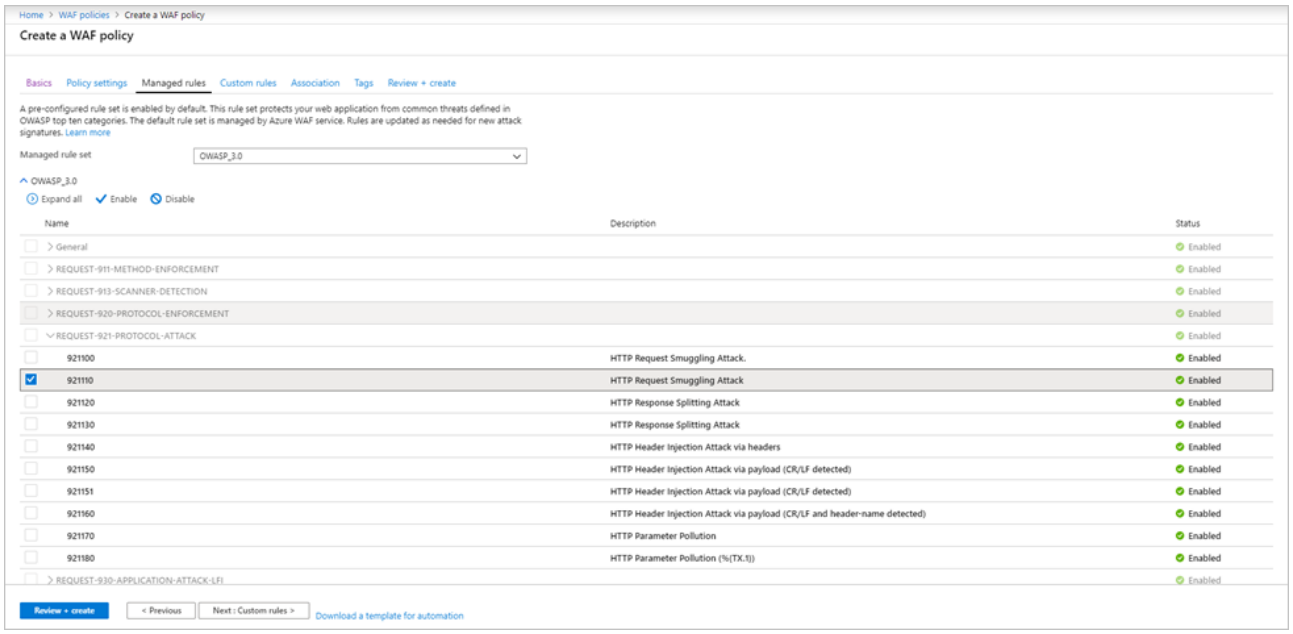

Рис. 3.13 – Вимкнути окреме правило групи правил

Налаштування правила

Щоб створити правило, що настроюється, виберіть Додати правило, що настроюється, на вкладці Налаштування правила . Відкриється сторінка налаштування правила. На Рис.у 3.14 показано приклад Налаштування правила блокування запиту, якщо рядок запиту містить текст blockme .

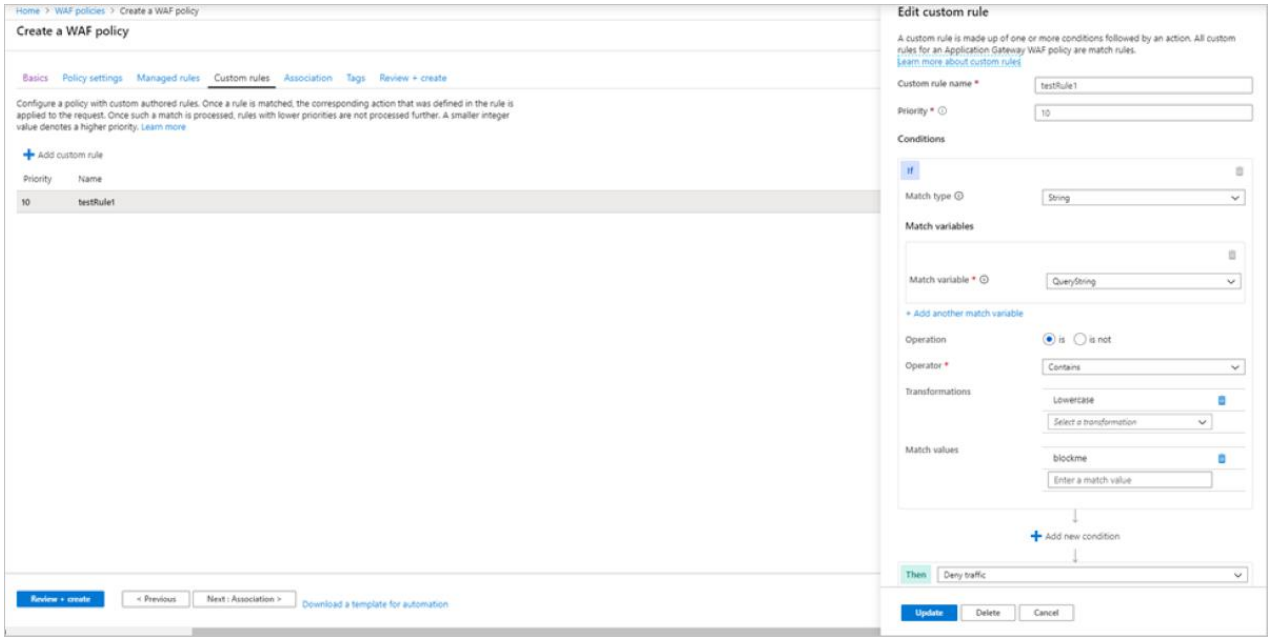

Рис. 3.14 – Налаштування правила блокування запиту, якщо рядок запиту містить текст blockme

Налаштування та керування політиками безпеки Azure WAF є критичними для забезпечення захисту веб-додатків від різноманітних кібератак та загроз. Завдяки Azure WAF організації можуть ефективно управляти правилами безпеки, адаптуючи їх до специфічних потреб своїх систем і додатків.

Процес створення, налаштування та застосування політик безпеки в Azure WAF охоплює кілька ключових етапів:

Створення політики: Визначення основних параметрів політики, таких як ім'я, тип та опис, забезпечує чітку структуру для подальших налаштувань.

Налаштування правил: Вибір та конфігурація правил безпеки дозволяють захистити веб-додатки від конкретних загроз, таких як SQL-ін'єкції, XSS-атаки та інші вразливості.

Застосування політики: Призначення політики до конкретного ресурсу

гарантує, що правила безпеки будуть застосовані на рівні, де вони найефективніші.

Моніторинг та керування: Регулярний моніторинг та оновлення політик забезпечують постійний захист від нових загроз, дозволяючи адміністраторам швидко реагувати на зміни в ландшафті загроз.

Використання Azure WAF та ретельне налаштування політик безпеки значно підвищують рівень захисту веб-додатків, мінімізують ризики витоків даних та забезпечують безперервність бізнес-процесів. Azure WAF надає потужні інструменти для проактивного захисту, що дозволяє організаціям бути на крок попереду потенційних загроз.

3.3. Розробка рекомендацій щодо захисту веб-сайтів на базі Azure WAF

Azure Web Application Firewall (WAF) є потужним інструментом для захисту веб-додатків від широкого спектру загроз безпеці. Для ефективного захисту веб-сайтів на базі Azure WAF необхідно врахувати кілька важливих аспектів. Нижче наведено детальний план розробки рекомендацій щодо захисту веб-сайтів за допомогою Azure WAF.

1. Оцінка поточних загроз та вимог безпеки

Перед впровадженням Azure WAF важливо провести ретельний аналіз поточних загроз, з якими може стикатися веб-сайт. Необхідно визначити вимоги безпеки, враховуючи специфіку бізнесу, тип веб-додатків та можливі сценарії атак.

Оцінка поточних загроз та вимог безпеки є важливим етапом у забезпеченні безпеки веб-сайтів. Першим кроком є ідентифікація критичних активів, таких як веб-сайти, бази даних та інфраструктура. Потім проводиться виявлення можливих загроз, серед яких загальні веб-атаки (SQL-ін'єкції, XSS, CSRF), DDoS-атаки, шкідливий код та фішинг.

Далі здійснюється оцінка ризиків, яка включає аналіз ймовірності реалізації загроз та їхнього впливу на бізнес. Важливо оцінити ефективність існуючих заходів безпеки. На основі цієї оцінки визначаються конкретні вимоги до безпеки, такі як

аутентифікація, шифрування даних, моніторинг, патчинг та навчання персоналу.

Усі результати оцінки документуються у звіті про оцінку ризиків, політиках безпеки та планах дій для подальшого використання. Регулярне оновлення оцінки допомагає підтримувати високий рівень безпеки в умовах постійно змінюваних загроз.

Рекомендації:

Провести аудит безпеки для виявлення поточних вразливостей.

Визначити критичні дані та ресурси, які потребують захисту.

Оцінити ризики та визначити пріоритетні загрози.

2. Вибір та налаштування Azure WAF

Azure Web Application Firewall (WAF) є хмарним рішенням, яке захищає веб-додатки від різних загроз безпеки, таких як SQL-ін'єкції та міжсайтовий скриптинг (XSS). Першим кроком у виборі Azure WAF є визначення потреб безпеки. Важливо оцінити типи загроз, від яких необхідно захистити ваші веб-додатки. Azure WAF підтримує стандарти OWASP, що забезпечує захист від найбільш поширених вразливостей.

Наступним етапом є розгляд можливостей інтеграції. Azure WAF легко інтегрується з іншими службами Azure, такими як Azure Front Door та Application Gateway. Це дозволяє обрати оптимальну конфігурацію для вашого середовища. Масштабованість є важливим фактором, оскільки Azure WAF підтримує автоматичне масштабування, забезпечуючи ефективну роботу під високими навантаженнями.

Процес налаштування Azure WAF починається зі створення політики WAF у порталі Azure. Ця політика визначає правила захисту та дії при виявленні загроз. Використання попередньо налаштованих правил OWASP допомагає захистити від найбільш поширених вразливостей, а кастомні правила дозволяють додати захист для специфічних потреб вашого додатка. Політику WAF потрібно прив'язати до Azure Front Door або Application Gateway, щоб забезпечити захист трафіку.

Моніторинг і логування є критично важливими для ефективної роботи Azure WAF. Налаштування моніторингу дозволяє відстежувати трафік та логувати

інциденти. Використання Azure Monitor та Application Insights допомагає аналізувати дані та оптимізувати політики. Перед увімкненням активного режиму блокування налаштування WAF слід тестувати в режимі спостереження, щоб упевнитися у відсутності хибних спрацьовувань. Ці кроки забезпечують ефективне налаштування та використання Azure WAF для захисту веб-додатків від різноманітних загроз.

Azure WAF пропонує два основних варіанти розгортання: на базі Azure Application Gateway та Azure Front Door. Вибір залежить від архітектури веб-додатків та вимог до продуктивності.

Рекомендації:

Для глобальних веб-додатків з низькою затримкою та високою доступністю використовуйте Azure Front Door.

Для додатків, які розташовані в одній або декількох регіонах, використовуйте Azure Application Gateway.

Налаштуйте основні параметри WAF, такі як рівень захисту (Prevention або Detection) та тип політик.

3. Створення та конфігурація політик безпеки

Створення та конфігурація політик безпеки в Azure WAF є ключовими етапами для забезпечення ефективного захисту веб-додатків. Першим кроком є доступ до порталу Azure, де необхідно вибрати службу Web Application Firewall. Вибравши службу, потрібно створити нову політику безпеки, яка буде захищати веб-додатки від відомих вразливостей.

Після створення політики, важливо визначити правила захисту. Azure WAF пропонує використання попередньо налаштованих правил OWASP, які забезпечують захист від найпоширеніших атак, таких як SQL-ін'єкції, міжсайтовий скриптинг (XSS) та інші загрози. Ці правила можуть бути включені або виключені залежно від конкретних потреб веб-додатка. Крім того, можна створювати кастомні правила для захисту від специфічних загроз, характерних для вашого додатка.

Наступним етапом є визначення дій, які WAF повинен виконувати при

виявленні загроз. Важливо налаштувати політику так, щоб вона спочатку працювала в режимі спостереження. Це дозволить моніторити трафік та виявляти потенційні загрози без блокування легітимного трафіку. Після тестування і налаштування політики можна перейти до режиму блокування, щоб автоматично блокувати шкідливий трафік.

Прив’язка політики WAF до служби, такої як Azure Front Door або Application Gateway, є наступним кроком. Це забезпечує, що всі вхідні та вихідні запити проходять через WAF, що дозволяє виявляти та блокувати загрози на ранніх етапах. Важливо регулярно переглядати та оновлювати правила політики, враховуючи нові загрози та рекомендації безпеки.

Моніторинг та логування є важливими аспектами для підтримки безпеки. Використання Azure Monitor та Application Insights дозволяє відстежувати активність WAF, аналізувати дані про загрози та оптимізувати налаштування політик. Регулярне переглядання логів допомагає виявляти нові вразливості та адаптувати політики для забезпечення максимальної безпеки.

Azure WAF дозволяє створювати користувацькі політики безпеки або використовувати вбудовані правила для захисту від загальних загроз.

Рекомендації:

Використовуйте вбудовані правила OWASP для захисту від найбільш поширених веб-атак, таких як SQL-ін'єкції, XSS-атаки та інші.

Налаштуйте користувацькі правила для специфічних загроз, характерних для вашого веб-додатка.

Встановіть обмеження на обсяг трафіку, перевірки IP-адрес та блокування підозрілої активності.

4. Активація функцій ведення журналу та моніторингу

Активація функцій ведення журналу та моніторингу є важливими етапами забезпечення безпеки та ефективного управління веб-додатками в Azure WAF. Спочатку необхідно перейти до порталу Azure та вибрати службу Web Application Firewall, де здійснюється налаштування політик безпеки. У меню налаштувань політики безпеки слід активувати функції ведення журналу та моніторингу.

Для активації журналювання необхідно налаштувати Azure Diagnostics. Це включає створення облікового запису Azure Storage, де будуть зберігатися журнали, або налаштування Log Analytics Workspace для зручного зберігання та аналізу даних. У налаштуваннях діагностики слід вибрати відповідні категорії журналів, такі як WAFLogs і ApplicationGatewayAccessLog, щоб зберігати записи про події безпеки та доступу.

Наступним кроком є налаштування Azure Monitor для забезпечення моніторингу активності WAF. Це включає налаштування метрик та оповіщень, які дозволяють відстежувати ключові показники ефективності та безпеки. Необхідно створити оповіщення для критичних подій, таких як виявлення атак, зниження продуктивності або інші підозрілі активності. Оповіщення можуть бути налаштовані для надсилання повідомлень електронною поштою, SMS або через інші засоби комунікації.

Для інтеграції з Azure Security Center слід активувати відповідні функції в налаштуваннях WAF. Azure Security Center забезпечує централізований огляд безпеки та допомагає виявляти вразливості, рекомендує дії для покращення захисту та надає аналітичні дані для ухвалення рішень. Це допомагає забезпечити проактивний підхід до управління безпекою та своєчасного реагування на інциденти.

Використання Application Insights дозволяє детально аналізувати трафік та поведінку користувачів. Це включає налаштування трекінгу запитів, затримок та інших параметрів для виявлення аномалій і підозрілої активності. Інтеграція з Application Insights також допомагає оптимізувати продуктивність веб-додатків та покращити досвід користувачів.

Нарешті, регулярний перегляд журналів та звітів є критично важливим для підтримання високого рівня безпеки. Ведення журналів дозволяє відстежувати історію подій, виявляти повторювані загрози та аналізувати поведінку атакуючих. Регулярний аналіз даних з журналів допомагає виявляти нові вразливості та адаптувати політики безпеки для протидії новим загрозам.

Регулярний моніторинг та аналіз журналів безпеки допомагають виявляти та

реагувати на потенційні загрози в режимі реального часу.

Рекомендації:

Активуйте ведення журналу для всіх політик WAF.

Використовуйте Azure Monitor та Azure Security Center для централізованого моніторингу та аналізу подій безпеки.

Налаштуйте сповіщення для критичних подій, таких як масові атаки або спроби проникнення.

5. Тестування та оптимізація налаштувань

Тестування та оптимізація налаштувань веб-додатків є важливим процесом для забезпечення їх ефективності та безпеки. Початковим етапом тестування є валідація конфігурацій. Це передбачає перевірку налаштувань на відповідність вимогам безпеки та функціональності. Веб-додаток повинен проходити комплексне тестування, включаючи тестування функціональних можливостей, безпеки, продуктивності та навантаження. Для цього використовують різні інструменти та методики, такі як автоматизовані тестові сценарії та ручне тестування.

Під час тестування безпеки важливо виявити потенційні вразливості, такі як SQL-ін'єкції, міжсайтовий скриптинг (XSS) та інші атаки. Використовуються спеціалізовані інструменти, такі як OWASP ZAP або Burp Suite, для проведення пенетраційного тестування. Це допомагає виявити слабкі місця у налаштуваннях і виправити їх до того, як вони будуть використані зловмисниками. Тестування продуктивності включає навантажувальні тести, які допомагають визначити, як веб-додаток поводиться під високим навантаженням. Інструменти на кшталт Apache JMeter або LoadRunner допомагають моделювати реальні умови роботи та виявляти вузькі місця в продуктивності.

Оптимізація налаштувань включає аналіз результатів тестування та внесення змін для покращення роботи веб-додатка. Важливо налаштувати кешування, мінімізувати використання ресурсів та оптимізувати бази даних. Наприклад, налаштування механізмів кешування, таких як Memcached або Redis, можуть значно покращити швидкість завантаження сторінок. Оптимізація запитів до баз

даних та індексація таблиць також сприяють підвищенню продуктивності.

Моніторинг є постійним процесом, який допомагає підтримувати налаштування на оптимальному рівні. Використання систем моніторингу, таких як Prometheus або Grafana, дозволяє відстежувати ключові показники продуктивності та швидко реагувати на будь-які зміни. Моніторинг безпеки допомагає виявляти підозрілу активність та реагувати на потенційні загрози в режимі реального часу. Це включає налаштування оповіщень та автоматичних дій у відповідь на інциденти безпеки.

Регулярний аудит конфігурацій допомагає забезпечити, що налаштування залишаються актуальними та ефективними. Під час аудиту перевіряються всі аспекти налаштувань, включаючи правила безпеки, політики доступу та продуктивність. Аудит дозволяє виявити застарілі або неефективні налаштування та оновити їх відповідно до сучасних стандартів.

Регулярне тестування налаштувань WAF дозволяє виявляти недоліки та оптимізувати захист веб-додатків.

Рекомендації:

Виконайте тестування за допомогою інструментів для виявлення вразливостей, таких як OWASP ZAP або Burp Suite.

Перевірте ефективність налаштувань WAF, проводячи пентестинг або інші форми етичного хакінгу.

Оптимізуйте правила та налаштування, виходячи з результатів тестування.

6. Навчання та підтримка користувачів

Навчання та підтримка користувачів є ключовими аспектами забезпечення ефективного використання веб-додатків і систем. Вони включають кілька важливих етапів, починаючи з початкового навчання користувачів, яке забезпечує їм необхідні знання для роботи з новими системами. Цей етап охоплює організацію навчальних сесій, підготовку навчальних матеріалів, таких як посібники користувача, відеоуроки та інтерактивні курси. Важливо, щоб ці матеріали були доступними та зрозумілими для користувачів різного рівня підготовки.

Після початкового навчання необхідно забезпечити постійну підтримку

користувачів. Це включає створення служби підтримки, яка надає допомогу через різні канали, такі як телефон, електронна пошта та чат. Служба підтримки повинна бути здатна швидко реагувати на запити користувачів та надавати кваліфіковану допомогу з вирішення технічних проблем. Крім того, важливо організувати систему внутрішніх форумів або баз знань, де користувачі можуть знаходити відповіді на часті питання та ділитися своїм досвідом.

Регулярне оновлення навчальних матеріалів та програм підтримки є необхідним для підтримки актуальності інформації. Це включає оновлення документації у відповідності з новими функціями та змінами в системах, а також проведення повторних навчальних сесій для користувачів. Крім того, важливо отримувати зворотний зв'язок від користувачів для виявлення проблем та вдосконалення процесів навчання та підтримки.

Важливо також враховувати різні рівні підготовки користувачів та їхні потреби. Для цього можна розробляти спеціалізовані навчальні програми для різних категорій користувачів, таких як новачки, середній рівень та просунуті користувачі. Це допоможе забезпечити більш ефективне навчання та підвищити задоволеність користувачів від роботи з системами.

Особливу увагу слід приділити безпеці. Навчання користувачів основам кібербезпеки, таким як розпізнавання фішингових атак, створення надійних паролів та безпечне використання інтернету, є критично важливим для захисту організації від загроз. Регулярні тренінги та оновлення знань користувачів у цій сфері допоможуть знизити ризики безпеки.

Підтримка користувачів також включає моніторинг та аналіз їхньої активності для виявлення проблемних зон та підвищення ефективності систем. Використання аналітичних інструментів дозволяє отримувати дані про взаємодію користувачів з системами, що допомагає виявляти проблеми та оптимізувати процеси навчання та підтримки.

Постійна підтримка та навчання користувачів є ключовими для забезпечення ефективного захисту веб-додатків.

Рекомендації:

Проведіть тренінги для IT-фахівців та адміністраторів з налаштування та використання Azure WAF.

Забезпечте регулярне оновлення знань про нові загрози та методи захисту.

Встановіть процедури для регулярного перегляду та оновлення політик безпеки.

ВИСНОВОК

У ході виконання дипломної роботи проведено комплексне дослідження щодо захисту веб-сайтів за допомогою веб-аплікаційного фаєрволу (WAF) Azure. Визначено актуальність проблеми безпеки веб-ресурсів у сучасному цифровому середовищі, де веб-сайти часто стають мішенню для різноманітних кібератак. Основною метою роботи було розробка рекомендацій для ефективного впровадження та використання Azure WAF, що дозволить підприємствам значно знизити ризики кібератак та забезпечити надійний захист своїх веб-додатків.

У процесі дослідження було проаналізовано існуючі методи та засоби захисту веб-сайтів, зокрема, можливості Azure WAF. Проведений аналіз показав, що використання Azure WAF забезпечує високий рівень захисту від різноманітних типів атак, таких як SQL-ін'єкції, XSS та DDoS-атаки. Значну увагу приділено питанням створення та конфігурації політик безпеки, що дозволяє налаштувати захист відповідно до конкретних потреб підприємства.

Розроблено рекомендації щодо вибору та налаштування Azure WAF, активації функцій ведення журналу та моніторингу, а також тестування та оптимізації налаштувань. Також підкреслено важливість навчання та підтримки користувачів для ефективного використання засобів захисту.

Практична значущість результатів роботи полягає в тому, що розроблені рекомендації можуть бути безпосередньо впроваджені фахівцями з кібербезпеки для захисту веб-ресурсів підприємств. Вони допоможуть мінімізувати ризики атак, забезпечити безперебійну роботу веб-додатків та підвищити загальний рівень безпеки інформаційних систем організацій.

Таким чином, проведене дослідження і розроблені на його основі рекомендації сприятимуть ефективному захисту веб-сайтів, що є критично важливим у умовах сучасного розвитку інформаційних технологій та зростаючих кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Azure Web Application Firewall Documentation. Microsoft Learn. https://learn.microsoft.com/en-us/azure/web-application-firewall/ (дата звернення: 10.05.2024).

2. Web Server and its Types of Attacks: https://www.greycampus.com/opencampus/ethicalhacking/web-server-and-its-types-of-attacks (дата звернення: 11.05.2024)

3. Brewer J. Web Server Vulnerabilities and a Defense in Depth Strategy Using the Squid Proxy/ Jim Brewer //1.4b. – 2004. (дата звернення: 10.05.2024)

4. Web Vulnerability Scanner v10 Product Manual: http://www.acunetix.com/resources/wvsmanual.pdf (дата звернення: 17.05.2024)

5. Acunetix Web Vulnerability Scanner: http://www.securitylab.ru/software/266415.php (дата звернення: 01.05.2024)

6. Дослідження вразливостей Web-сайтів та методів їх усунення: http://phone.kpi.ua/wpcontent/uploads/2014/06/4.pdf (дата звернення: 01.05.2024)

7. Жуков Ю.В. Основы веб-хакинга. Нападение и защита / Юрий Викторович Жуков, 2012. – 206 с (дата звернення: 01.05.2024)

8. Захист веб-додатків: http://www.ereading.club/bookreader.php/1012355/DJAndreysXeZa schita_veb-prilozheniy.html (дата звернення: 01.05.2024)

9. Бойчик І.М., Харів П.С., Хопчпн М.І., Піча Ю.В. Економіка підприємства —К.: "Каравела"; Львів: "Новий світ - 2000", 2001. - 298 с. (дата звернення: 12.05.2024)

10. М. А. Бєлов, Н. М. Євдокимова, В. Є. Москалюк та ін.;Планування діяльності підприємства: Навч.-метод. посібник для самост. вивч. дисц. — К.: КНЕУ, 2002. — 252 с. (дата звернення: 01.05.2024)

11. Blazquez D. Broken Authentication OWASP Top 10 / Daniel Blazquez. – 2019: https://hdivsecurity.com/owasp-broken-authentication (дата звернення: 01.05.2024)

12. Authentication Hacking: What are Authentication Hacking Attacks – 2014:

https://www.acunetix.com/websitesecurity/authentication/ (дата звернення: 11.05.2024)

13. Zeeshan N. 7 Ways To Stop Web Attacks Affecting Your Web Application / Nasrumminallah Zeeshan. – 2017: https://www.peerlyst.com/posts/7-ways-to-stop-web-attacksaffecting-your-web-application-nasrumminallah-zeeshan (дата звернення: 01.05.2024)

14. Common Vulnerability Scoring System v3.0: Specification Document: https://www.first.org/cvss/specification-document (дата звернення: 01.05.2024)

15. Створення політик Брандмауера веб-додатків для Шлюзу додатків: https://learn.microsoft.com/ru-ru/azure/web-application-firewall/ag/create-waf-policy-ag (дата звернення: 01.05.2024)

16. Azure Portal: https://portal.azure.com/ (дата звернення: 01.05.2024)

17. Налаштування правила обмеження IP-адрес за допомогою WAF для Azure Front Door: https://learn.microsoft.com/ru-ru/azure/web-application-firewall/afds/waf-front-door-configure-ip-restriction (дата звернення: 15.05.2024)

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)