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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту веб-додатків організації на базі рішення Akamai Kona Site Defender»

зі спеціальності *125 Кібербезпека та захист інформації*
(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

_____ Роман БЄЛИХ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
БЄЛИХ Роман
(прізвище, ім'я)

Керівник д.ф., доцент СОБЧУК Андрій
(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 Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
"___" жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

БЄЛИХ Романа Костянтиновича
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія захисту веб-додатків організації на базі рішення Akamai Kona Site Defender»

керівник кваліфікаційної роботи Собчук Андрій Валентинович, д.ф., доц.
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» жовтня 2024 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Akamai Kona Site Defender;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми забезпечення захисту веб-додатків організації.
2. Аналіз методів та засобів забезпечення захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.
3. Технологія забезпечення захисту веб-додатків організації.

4. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми забезпечення захисту веб-додатків організації.	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	12.10.2024 р.	
3.	Аналіз методів та засобів забезпечення захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.	27.10.2024 р.	
4.	Технологія забезпечення захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.	03.11.2024 р.	
5.	Розроблення рекомендацій щодо захисту веб-додатків організації.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Роман БЄЛИХ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Андрій СОБЧУК
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача БЄЛИХ Романа
на тему: «Технологія захисту веб-додатків організації на базі рішення Akamai Kona Site Defender»

Актуальність: Безпека веб-додатків відіграє ключову роль у сучасній епоху цифрових технологій. Веб-програми забезпечують широкий спектр функцій, необхідних для здійснення професійної діяльності, управління персональними даними та взаємодії в різних сферах життя. Вони стали основним інструментом для зберігання й обробки конфіденційної інформації, яка включає фінансові, особисті та інші критично важливі дані. Зважаючи на їхню значущість, забезпечення високого рівня безпеки є фундаментальним завданням, оскільки вразливості в системах можуть призводити до серйозних наслідків, включаючи витоки даних, фінансові втрати та підрив довіри. Надійний захист веб-додатків має враховувати новітні загрози та використовувати сучасні методи запобігання несанкціонованому доступу та експлуатації вразливостей. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу встановлено зміст проблеми забезпечення безпеки веб-додатків організації, визначено мету та завдання їх захисту, а також складові частини технології безпеки.
2. Досліджено методи та засоби захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.
3. Розглянуто основні компоненти технології захисту веб-додатків на базі Akamai Kona Site Defender, принципи її роботи та рекомендації щодо практичного впровадження для підвищення рівня безпеки.
4. Текст викладено грамотно та послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно, що забезпечує наочність та зрозумілість. Список науково-технічної літератури демонструє вміння працювати з джерелами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз умов застосування технологій захисту веб-додатків на базі рішення Akamai Kona Site Defender для забезпечення безпеки корпоративних ресурсів організації.
2. Запропонований порядок впровадження технології захисту веб-додатків на базі рішення Akamai Kona Site Defender бажано було б продемонструвати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **БЄЛИХ Роман** – присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент:

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

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач БЄЛИХ Роман до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія захисту веб-додатків організації на базі рішення Akamai Kona Site Defender».
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***БЄЛИХ Роман*** обрав тему роботи, метою якої було дослідити зміст технології захисту веб-додатків організації та розробити 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 ***БЄЛИХ Роман*** 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 ***БЄЛИХ Романа*** на оцінку **"добре"** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

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

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **БЄЛИХ Роман** допускається до захисту даної кваліфікаційної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 52 сторінки, 21 рисунків, 15 джерел.

Об'єкт дослідження – захист веб-додатків організації.

Предмет дослідження – технологія захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.

Мета роботи – розробити порядок застосування технології захисту веб-додатків організації та рекомендації щодо її впровадження.

Методи дослідження – аналіз наукової літератури, експлуатаційної документації, міжнародних стандартів у сфері кібербезпеки, а також їх порівняльний аналіз.

Рішення Akamai Kona Site Defender забезпечує комплексний захист веб-додатків шляхом використання сучасних технологій, таких як веб-аплікаційний брандмауер (WAF), захист від DDoS-атак, ідентифікація ботів і система глибокого аналізу трафіку для виявлення та блокування потенційних загроз. Це рішення дозволяє ефективно запобігати атакам, які спрямовані на вразливості веб-додатків, наприклад, SQL-ін'єкції, XSS-атаки або CSRF-атаки.

В роботі проведено аналіз проблеми захисту веб-додатків організації, сформульовано мету та завдання дослідження. Розглянуто сучасні методи й засоби захисту веб-додатків. Досліджено функціональні можливості, архітектуру та основні компоненти рішення Akamai Kona Site Defender, зокрема механізми інтеграції цього рішення в інфраструктуру організації.

На основі виконаних досліджень запропоновано порядок застосування технології Akamai Kona Site Defender для забезпечення надійного захисту веб-додатків. Розроблено рекомендації для спеціалістів з кібербезпеки щодо ефективного впровадження і налаштування рішення.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, ВЕБ-ДОДАТКИ, ЗАХИСТ, AKAMAI KONA SITE DEFENDER, КІБЕРБЕЗПЕКА, ТЕХНОЛОГІЇ ЗАХИСТУ ВЕБ-ДОДАТКІВ.

ABSTRACT

Text part of the qualification work: 52 pages, 21 figures, 15 sources.

Object of research – protection of an organization's web applications.

Subject of research – protecting an organization's web applications based on the Akamai Kona Site Defender solution.

The aim of research – to develop a methodology for applying the technology to protect an organization's web applications and provide recommendations for its implementation.

Research methods – study of the literature on this topic, analysis of operational documentation, international standards and their comparison.

The Akamai Kona Site Defender solution provides comprehensive protection for web applications using modern technologies such as a Web Application Firewall (WAF), DDoS attack mitigation, bot identification, and deep traffic inspection systems to detect and block potential threats. This solution effectively prevents attacks targeting web application vulnerabilities, including SQL injections, XSS attacks, and CSRF attacks.

The study analyzes the problem of protecting an organization's web applications, formulates the research aim and objectives, and reviews current methods and tools for web application protection. The functional capabilities, architecture, and core components of the Akamai Kona Site Defender solution are examined, including mechanisms for integrating the solution into an organization's infrastructure.

Based on the research conducted, a methodology for applying the Akamai Kona Site Defender technology to ensure reliable web application protection is proposed. Recommendations for cybersecurity professionals regarding the effective deployment and configuration of the solution have been developed.

Field of application – cybersecurity of information resources of the organization.

INFORMATION RESOURCES OF THE ORGANIZATION, WEB APPLICATIONS, PROTECTION, AKAMAI KONA SITE DEFENDER, CYBERSECURITY, WEB APPLICATION PROTECTION TECHNOLOGIES

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AKSD – Akamai Kona Site Defender

API – Application Programming Interface

CSP – Content Security Policy

CSRF – Cross-Site Request Forgery

DDoS – Distributed Denial of Service

DNS – Domain Name System

DOM – Document Object Model

LFI – Local File Inclusion

PII – Personally Identifiable Information

SQLi – SQL Injection

WAF – Web Application Firewall

XSS – Cross-Site Scripting

ZT – Zero Trust

ACL – Access Control List

CDN – Content Delivery Network

CORS – Cross-Origin Resource Sharing

CSR – Certificate Signing Request

CVSS – Common Vulnerability Scoring System

OWASP – Open Web Application Security Project

TLS – Transport Layer Security

TTPs – Tactics, Techniques, and Procedures

WASP – Web Application Security Protocol

ВСТУП

Безпека веб-додатків (також відома як Web AppSec) - це ідея створення веб-сайтів, які функціонують належним чином, навіть коли вони піддаються атакам. Концепція включає в себе набір засобів контролю безпеки, вбудованих у веб-додаток для захисту його активів від потенційно зловмисних агентів.

Захист веб-додатків організацій є одним із ключових завдань у сфері кібербезпеки, оскільки веб-додатки стали основним інструментом для взаємодії з клієнтами, партнерами та співробітниками. Їх використання охоплює широкий спектр завдань: від управління фінансовими операціями та зберігання конфіденційної інформації до підтримки комунікаційних платформ і автоматизації бізнес-процесів. Уразливості веб-додатків можуть призвести до значних фінансових втрат, репутаційних ризиків та витоку конфіденційної інформації, яка є цінним активом організації.

Злочинці активно експлуатують слабкі місця в архітектурі та захисті веб-додатків, використовуючи такі атаки, як SQL-ін’єкції, XSS-атаки, CSRF-атаки, атаки типу "відмова у обслуговуванні" (DDoS) та інші. Їхня мета може варіюватися від отримання доступу до баз даних та конфіденційної інформації до повного виведення додатків з ладу. Такі атаки можуть спричинити значні наслідки, зокрема припинення роботи критичних сервісів, викрадення персональних даних користувачів або втрату конкурентних переваг через компрометацію інтелектуальної власності.

Крім того, сучасні веб-додатки часто інтегруються з хмарними платформами, сторонніми API та іншими зовнішніми ресурсами, що створює додаткові потенційні точки входу для атак. Розширення меж корпоративної інфраструктури, використання технологій роботи з будь-якого місця (WFA) та зростання обсягів трафіку ускладнюють забезпечення комплексного захисту додатків. У цих умовах традиційні методи захисту, що зосереджуються лише на периметрі мережі, стають недостатньо ефективними.

Впровадження передових технологій, таких як Akamai Kona Site Defender, дозволяє забезпечити багаторівневий захист веб-додатків, використовуючи інтелектуальні алгоритми виявлення загроз, інтеграцію з глобальними мережами доставки контенту (CDN), захист від ботів та системи автоматичного блокування атак. Рішення Akamai Kona Site Defender здатне не лише виявляти відомі типи атак, але й адаптуватися до нових загроз, що постійно еволюціонують.

Враховуючи зростаючу складність загроз і обсяги атакуючого трафіку, дослідження, спрямоване на аналіз ефективності та впровадження таких рішень, є надзвичайно важливим. Вивчення функціональних можливостей, архітектури та механізмів інтеграції Akamai Kona Site Defender в інфраструктуру організації дозволяє не лише забезпечити належний рівень захисту, але й оптимізувати витрати на впровадження та експлуатацію системи кібербезпеки. Розробка рекомендацій для спеціалістів з кібербезпеки сприяє підвищенню стійкості організацій до кіберзагроз та гарантуванню безперервності їхніх бізнес-процесів.

Об'єкт дослідження – захист веб-додатків організації.

Предмет дослідження – технологія захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.

Мета роботи – розробити порядок застосування технології захисту веб-додатків організації та рекомендації щодо її впровадження.

Наукові завдання:

Дослідити сутність проблеми захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.

Проаналізувати підходи до захисту веб-додатків організації за допомогою Akamai Kona Site Defender.

Проаналізувати існуючі рішення із захисту веб-додатків організації на платформі Akamai Kona Site Defender.

Проаналізувати методи та засоби захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.

Розкрити порядок реалізації технології захисту веб-додатків організації за допомогою Akamai Kona Site Defender.

Методи дослідження – аналіз наукової літератури, експлуатаційної документації, міжнародних стандартів у сфері кібербезпеки, а також їх порівняльний аналіз.

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту веб-додатків організації на базі рішення Akamai Kona Site Defender, а також розроблено рекомендації фахівцям з кібербезпеки щодо її впровадження та налаштування для забезпечення належного рівня захисту.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми забезпечення безпеки веб-додатків організації

Безпека веб-додатків є важливим напрямом інформаційної безпеки, що зосереджується на захисті веб-сайтів, додатків і веб-сервісів. Вона включає методи та технології для запобігання загрозам як зовнішнього, так і внутрішнього характеру. Ці загрози можуть варіюватися від незначних перебоїв у роботі до серйозних витоків даних, що призводять до фінансових збитків і юридичних проблем. [1]

Основною метою забезпечення безпеки веб-додатків є ідентифікація та мінімізація вразливостей, які можуть бути використані зловмисниками. Такі вразливості можуть виникати на різних етапах життєвого циклу веб-додатка: від його розробки і тестування до впровадження і подальшого обслуговування. Вразливі місця можуть бути присутні як у самому програмному забезпеченні, так і в серверному чи мережевому середовищі.

Додатковим аспектом є захист даних організації та її користувачів від крадіжки або маніпуляцій, а також забезпечення стабільної та безперебійної роботи онлайн-сервісів. Захист веб-додатків гарантує, що чутливі дані, такі як фінансова інформація, особисті дані чи бізнес-секрети, залишаються конфіденційними та недоступними для несанкціонованого доступу.

Загрози безпеці веб-додатків стають дедалі більш актуальними, оскільки сучасне суспільство значною мірою покладається на онлайн-сервіси. Компрометація веб-додатка може мати серйозні наслідки для організацій: фінансові втрати, юридичні штрафи за недотримання вимог законодавства та втрату репутації. Наприклад, витік даних може завдати збитків як через прямі втрати коштів, так і через втрату довіри клієнтів та партнерів. [2]

Без заходів тестування безпеки протягом усього життєвого циклу розробки застосунків, команди розробників можуть піддавати їх кібератакам, через що вони залишаються вразливими.

- Аналітики часто розглядають безпеку як мережеву чи IT-проблему, що призводить до того, що лише кілька експертів з безпеки організації знають про загрози на рівні додатків.
- Команди, які формулюють вимоги до безпеки застосування у вигляді нечітких очікувань або негативних тверджень ускладнюють процес створення тестів.
- Тестування безпеки застосування на пізньому етапі життєвого циклу зазвичай обмежується перевіркою на предмет спроби злому.

Типові атаки на веб-додатки

Специфічні вразливості веб-додатків повинні визначати технології, які використовуються для їх захисту. На рисунку 1 показано чисельні точки в системі, які можуть потребувати захисту. Часто потрібно спочатку використовувати загальні концепції протидії, щоб переконатися, що було обрано технологію, яка найкраще відповідає потребам організації, а не ту, яка лише заявляє про протидію новітнім методам злому.

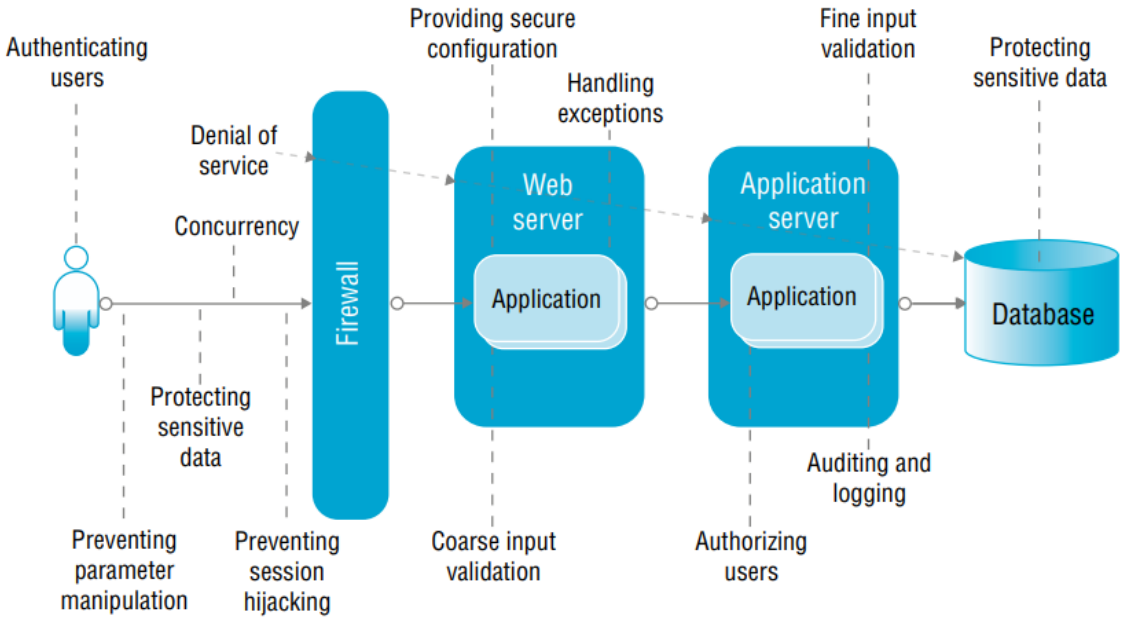


Рис. 1.1. Проблеми безпеки веб-додатків

Поширені атаки на веб-додатки:

Міжсайтовий скриптинг (XSS)

Атака міжсайтового скриптингу (XSS) – це поширена загроза для веб-додатків, коли зловмисник додає або впроваджує шкідливий код у вже існуючий авторизований додаток. Такі атаки можуть як безпосередньо зламати окремий сайт, так і скомпрометувати сторонній скрипт, щоб отримати доступ до всіх сайтів, на яких цей скрипт використовується. Під час цих атак шкідливий код може бути переданий іншим користувачам веб-сайту, а клієнти можуть заразитися шкідливим програмним забезпеченням, яке компрометує їхню конфіденційну інформацію. Найскладнішими для виявлення є DOM-орієнтовані XSS-атаки, оскільки їх вразливість знаходиться у клієнтському коді, а не на сервері, і сервер не має змоги зафіксувати атаку.

XSS-атаки зазвичай відбуваються, коли веб-додаток не проводить належної перевірки введених користувачем даних перед їх відображенням на сторінці. Наприклад, якщо секція коментарів або відгуків на сторінці продукту не виконує очистку введених коментарів, зловмисник може вставити шкідливий код у поле коментаря. Цей код буде доданий на сторінку та виконаний у браузері жертви. Такий тип атаки називають "збереженим" або "персистентним" XSS, тому що шкідливий код зберігається на сервері й передається всім майбутнім користувачам додатка. Звідти зловмисний сценарій з’явиться як вихідний код і виконуватиметься в наступних браузерах відвідувачів:

```
1   <br>
2   <strong>Comment:</strong>
3   <br>
4   <script src="http://192.160.0.106:4444/hook.js"></script>
5   <br>
6   <hr>
7   </span>
8   <h2 class="title-regular-2">Leave a Comment</h2>
```

Рис. 1.2. Вихідний код

Приклад: зловмисник знаходить веб-додаток, який не проводить очищення введення у секції коментарів, і додає шкідливий JavaScript-код. За допомогою цього

коду зловмисник може виконувати різні дії, наприклад: зчитувати локальне сховище, отримувати доступ до cookies, красти персональні дані (PII), проводити фішингові атаки або поширювати шкідливе ПЗ.

Запобігання XSS:

- Перевіряйте та очищуйте введення користувачів перед їхнім відображенням на сторінці.
- Використовуйте функції кодування спеціальних символів (наприклад, < і >), щоб браузер не інтерпретував їх як HTML.
- Налаштуйте заголовок Content-Security-Policy, щоб обмежити джерела завантаження вмісту на сторінку, зменшуючи можливість впровадження шкідливого коду з зовнішніх джерел.

Атаки впровадження SQL-коду (SQL Injection)

SQL-ін’єкція (SQLI) схожа на XSS-атаку, але її ціль – не клієнтський код, а серверна база даних. Зловмисник використовує уразливість у веб-додатку, щоб маніпулювати базою даних, отримувати доступ до конфіденційної інформації (наприклад, логіни чи фінансові дані) або виконувати несанкціоновані дії (додавати, змінювати чи видаляти записи). Функцію пошуку можна реалізувати за допомогою наступного SQL-запиту:

```
1   SELECT * FROM products WHERE name LIKE '%SEARCH_TERM%';
```

Рис. 1.3. Функція пошуку

Якщо веб-програма не перевірить пошуковий термін належним чином, зловмисник може ввести шкідливий код у поле введення, щоб маніпулювати базою даних. Наприклад, зловмисник може ввести такий пошуковий термін:

```
OR 1=1; --
```

Рис. 1.4. Пошуковий термін

Цей вхід змінить SQL-запит на наступне:

```
SELECT * FROM products WHERE name LIKE '%' OR 1=1; --%';
```

Рис. 1.5. Результат зміни пошукового терміну

Отриманий запит повертатиме всі рядки в таблиці продуктів, оскільки речення WHERE завжди матиме значення TRUE. -- наприкінці введення використовується для коментування решти оригінального запиту, щоб він не заважав шкідливому коду зловмисника.

SQL-ін’єкція відбувається, коли веб-додаток не перевіряє введені користувачем дані. Наприклад, якщо додаток дозволяє шукати продукти через поле введення, але не перевіряє це введення, зловмисник може вставити шкідливий код для маніпулювання базою даних.

Запобігання SQL:

Використовуйте підготовлені запити (prepared statements) та параметризовані запити. Вони дозволяють розробникам використовувати плейсхолдери для введення, запобігаючи прямому впровадженню даних у SQL-запит.

А також, варто проводити перевірку та очищення введених даних.

Атаки на обхід шляхів (Path Traversal)

Path traversal (або directory traversal) – це атака, яка передбачає доступ до файлів і директорій на веб-сервері за межами кореневої директорії. Зловмисники можуть використовувати цю уразливість для отримання доступу до конфігураційних файлів, журналів або виконання довільного коду на сервері.

Цей тип атак виникає, коли додаток не перевіряє введення, що використовується для вказівки шляху до файлу або директорії. Наприклад, якщо додаток дозволяє користувачам завантажувати файли, вказуючи їхню назву, зловмисник може вставити у шлях символи ../, щоб отримати доступ до файлів за межами дозволеної директорії.

Місцеве включення файлів (LFI): це варіант path traversal-атаки, під час якої зловмисник змушує додаток виконати або розкрити локальні файли на сервері, відкриваючи можливості для подальших атак.

Запобігання Path Traversal:

- Перевіряйте та обмежуйте введення користувачів, особливо символи, які можуть змінити шлях (../).
- Використовуйте абсолютні шляхи для доступу до файлів і встановлюйте обмеження на рівні серверної конфігурації.

Міжсайтові запити з підробкою (CSRF)

Атака CSRF змушує користувача виконати небажані дії у веб-додатку, на якому він вже авторизований. Мета зловмисника – виконати несанкціоновані дії (наприклад, переведення коштів або зміну пароля), відправивши шкідливий запит, який виглядає легітимним.

Приклад: якщо користувач авторизований у банківському додатку, який дозволяє переводити кошти через форму без унікального токена, зловмисник може створити шкідливий сайт із формою, що імітує банківську. Потім, через соціальну інженерію, змусити користувача заповнити цю форму.

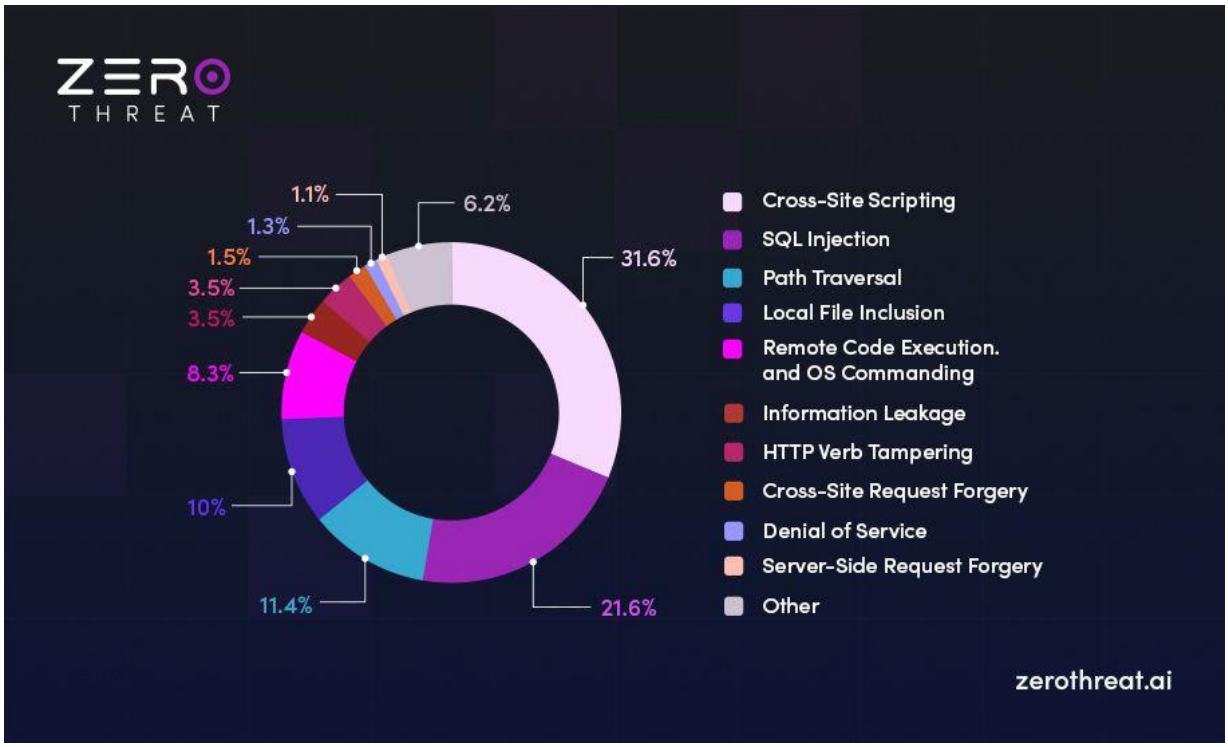


Рис. 1.6. Статистика застосованих атак [3]

Окрему загрозу становлять вразливості нульового дня, які ще не відомі розробникам і можуть бути використані зловмисниками до моменту створення виправлень. Вони є особливо небезпечними через ефект раптовості та складність виявлення. [4]

Відповідно до рекомендацій Міжнародної ради консультантів з електронної комерції (International Council of E-Commerce Consultants), веб-додатки мають забезпечувати обробку виключно довірених даних і ефективно запобігати проникненню шкідливих або недовірених даних, які можуть становити загрозу для бази даних, функціонування додатка чи конфіденційної інформації користувачів.

Для досягнення цього важливо забезпечити повний контроль і прозорість щодо виконуваного на веб-сайті коду, включно з власним і стороннім. Також необхідно здійснювати моніторинг і регулювання зібраних та переданих даних з метою запобігання витоку інформації.

Рекомендується проводити регулярні оцінки безпеки веб-додатків для виявлення та усунення вразливостей. Такі перевірки мають бути інтегровані на всіх етапах життєвого циклу розробки додатків. Окрім того, важливо уникати використання застарілих версій веб-серверів, операційних систем, систем управління контентом, бібліотек та іншого програмного забезпечення, оскільки це може створювати додаткові ризики. [5]

1.2. Аналіз вимог до безпеки веб-додатків

Оскільки цифровий світ продовжує розвиватися, ризик кіберзагроз зростає паралельно з ним. Хакери стають дедалі більш кваліфікованими, все частіше і точніше націлюючи свої атаки на веб-додатки. Наслідки успішної атаки можуть бути катастрофічними: від значних фінансових втрат і шкоди репутації до серйозних операційних збоїв.

Для бізнесу, особливо для тих, хто працює з чутливими даними, інвестування в надійні механізми безпеки є не просто запобіжним заходом, а необхідністю. Без

сильних заходів безпеки бізнес ризикує зазнати витоків даних, втрати довіри клієнтів та виявлень невідповідності, що може мати суттєвий вплив на загальний успіх компанії.

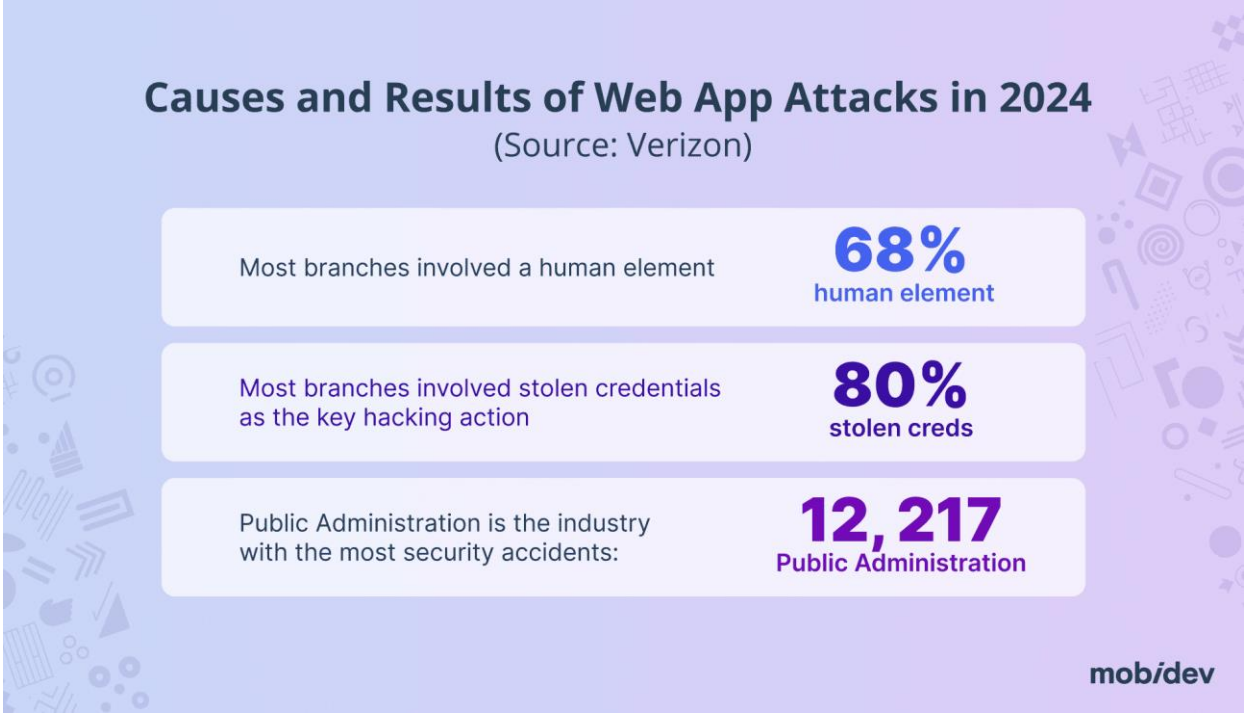


Рис. 1.7. Статистика веб-атак [6]

Вимоги до безпеки веб-додатків базуються на галузевих стандартах, законах або попередньому досвіді. Ці вимоги повинні визначати дії та нові або існуючі функції, які допоможуть захистити ваш додаток від атак.

Наприклад, це може бути PCI DSS (Стандарт безпеки даних індустрії платіжних карток) або HIPPA (Закон про переносимість і відповідальність за медичне страхування). Також це може бути стандарт ASVS (Application Security Verification Standard) від OWASP. Основною метою проекту OWASP Application Security Verification Standard (ASVS) є нормалізація діапазону охоплення і рівня суворості, доступних на ринку, коли мова йде про виконання перевірки безпеки веб-додатків за допомогою комерційно придатного відкритого стандарту. Стандарт забезпечує основу для тестування засобів контролю технічної безпеки додатків, а також будь-яких засобів контролю технічної безпеки в середовищі, на які покладаються для захисту від таких вразливостей, як міжсайтовий скриптинг (XSS)

і SQL-ін'єкції. Цей стандарт може бути використаний для встановлення рівня впевненості в безпеці веб-додатків. Вимоги були розроблені з урахуванням наступних цілей:

- Використання в якості метрики - надання розробникам і власникам додатків мірила, за допомогою якого можна оцінити ступінь довіри до їхніх веб-додатків,
- Використання в якості керівництва - Надання рекомендацій розробникам засобів контролю безпеки щодо того, що потрібно вбудовувати в засоби контролю безпеки, щоб задовольнити вимоги до безпеки додатків, а також
- Використовувати під час закупівель - Забезпечити основу для визначення вимог до перевірки безпеки додатків у контрактах. [7]

Розглянемо ASVS докладніше. Загалом, цей стандарт має дві основні цілі:

Допомогти організаціям розробляти і підтримувати безпечні веб-додатки та дозволити постачальникам послуг безпеки, постачальникам інструментів безпеки та споживачам узгодити власні вимоги та пропозиції.

В ASVS є три рівні безпеки веб-додатків. Перший рівень забезпечує низький рівень безпеки, а третій - найвищий.

Рівні безпеки у ASVS визначають різний рівень захисту. Дії першого рівня забезпечують базовий захист від більшості сучасних атак, включаючи OWASP Top 10, і є мінімально необхідним стандартом. Другий рівень вимагає більше зусиль, але забезпечує вищий рівень безпеки, зокрема захист від більшості сучасних програмних ризиків. Третій рівень призначений для критично важливих систем, таких як охорона здоров'я, військові застосунки та інші об'єкти критичної інфраструктури.

На другому рівні безпеки необхідно забезпечити інтеграцію питань безпеки на всіх етапах життєвого циклу розробки програмного забезпечення. Важливим є проведення моделювання загроз для кожної зміни дизайну, централізований контроль безпеки веб-додатків і використання автентифікованого підходу для всіх проміжних шарів програми. Також потрібно забезпечити єдиний формат і

стандартизований підхід до ведення журналів, що сприяє підвищенню якості аудиту безпеки.

Вимоги до паролів та захисту автентифікації

Вимоги до паролів та захисту автентифікації передбачають, що паролі мають бути довшими за 12 символів і коротшими за 128. Поле для введення пароля повинно відображати лічильник складності, щоб заохочувати користувачів створювати надійні комбінації.

Для захисту від перебору автентифікації необхідно впровадити механізми, такі як CAPTCHA, які дозволяють розрізняти користувачів і автоматизовані системи, а також обмеження кількості спроб автентифікації в заданий проміжок часу.

Тимчасові паролі повинні мати довжину не менше шести символів та обмежений термін дії, щоб зменшити ризики їх несанкціонованого використання. Найкращі практики забезпечення безпеки веб-додатків включають використання перевірених та оновлених фреймворків і бібліотек. Застосування лише перевірених компонентів з реєстром і регулярним оновленням дозволяє зменшити ризики використання вразливого коду.

Для захисту доступу до бази даних слід забезпечити шифрування з’єднання між додатком і базою, а також використовувати надійну автентифікацію чи складні паролі. Додатково важливо реалізувати кодування даних, щоб запобігти XSS-атакам. Це можна зробити шляхом перетворення спеціальних символів у безпечні форми за допомогою токенів CSRF, що дозволяє уникнути вставки шкідливого коду та захистити сесійні дані від викрадення.

Перевірка вхідних даних є важливим етапом, який запобігає збереженню некоректної інформації у системі. Для цього варто використовувати списки дозволених символів, зокрема для таких параметрів, як поштові індекси чи адреси. Впровадження цифрової ідентифікації із багатофакторною автентифікацією (MFA) або криптографічною автентифікацією (CBA) значно знижує ризики компрометації облікових записів.

Контроль доступу повинен базуватися на принципі «заборони за замовчуванням», що обмежує права доступу користувачів до мінімально необхідного рівня. Для збереження облікових даних доцільно використовувати спеціалізовані менеджери секретів, такі як AWS Secrets Manager або Hashicorp Vault. Захист конфіденційних даних, таких як номери кредитних карток, передбачає їхнє шифрування як під час передачі, так і в стані спокою. При цьому слід уникати надмірного шифрування, яке може уповільнювати роботу додатку.

Логування має бути централізованим, що забезпечує ефективне фільтрування даних та доступність лише для читання. Використання сервісів, таких як AWS CloudTrail, дозволяє відстежувати активність API, водночас виключаючи з логів конфіденційну інформацію.

Обробка помилок повинна бути організована таким чином, щоб не розкривати зайвих технічних деталей. Наприклад, повідомлення «невірний логін або пароль» є більш безпечним, ніж «неправильний пароль», оскільки зменшує можливості для атак перебором. Лаконічні повідомлення та коректна обробка винятків забезпечують стабільність і безпеку роботи додатків.

Використання найкращих практик та дотримання стандартів ASVS є важливими кроками для забезпечення безпеки веб-додатків. Впровадження цих рекомендацій дозволить мінімізувати ризики і захистити як сам додаток, так і дані користувачів.

1.3. Аналіз існуючих засобів для захисту веб-додатків організації

Безпека веб-додатків є критично важливою через часті інциденти, що призводять до витоку даних, зокрема паролів, електронної пошти та фінансової інформації, які спричиняють серйозні репутаційні та фінансові втрати для власників сайтів. Для ефективного захисту необхідно зосередитися на безпечній розробці веб-додатків, належній конфігурації серверів, політиці управління паролями та перевірці стороннього коду.

Вразливості часто виникають через людські помилки або недоліки зовнішніх бібліотек, що використовуються у веб-додатках. Безпека веб-додатків означає здатність додатка зберігати працездатність і конфіденційність даних навіть під час атак. Разом із надійними механізмами безпеки необхідно застосовувати додаткові інструменти для захисту від загроз і забезпечення доступності системи.

Незахищеність додатків від DoS і DDoS-атак може призвести до їхньої недоступності. Наприклад, у 2015 році GitHub зазнав DDoS-атаки з піковим трафіком 1,35 Тбіт/с, через що платформа не працювала 10 хвилин. Подібні атаки демонструють вразливість навіть великих компаній до кіберзагроз, незважаючи на їхню інфраструктуру та репутацію.

Сучасні веб-додатки мають численні вразливості, які можуть призвести до витоку конфіденційних даних, зокрема фінансової та медичної інформації. Наприклад, у 2013 році через витік даних Yahoo було скомпрометовано 3 мільярди акаунтів, завдано збитків у $120 млн, що негативно вплинуло на репутацію компанії.

Захист конфіденційної інформації, включаючи фінансові дані чи медичну таємницю, вимагає належного рівня безпеки, адже порушення таких даних може мати як юридичні, так і репутаційні наслідки. Еволюція загроз і складність атак вимагають впровадження чітких принципів і політик безпеки для зниження ризиків.

Найпоширеніші ризики для безпеки веб-додатків

Як вже згадувалось вище, веб-загрози постійно змінюються, тому дуже важливо бути в курсі їхніх змін. Однією з найбільш важливих і цінних статистичних даних для нас є топ-10 ризиків безпеки веб-додатків від OWASP.

Зібравши дані від більш ніж 40 відомих компаній, що займаються безпекою додатків, OWASP опублікував цей «топ-10» в Інтернеті. Десять найнебезпечніших вразливостей були визначені на основі інформації, зібраної з більш ніж 100 000 різних програм.

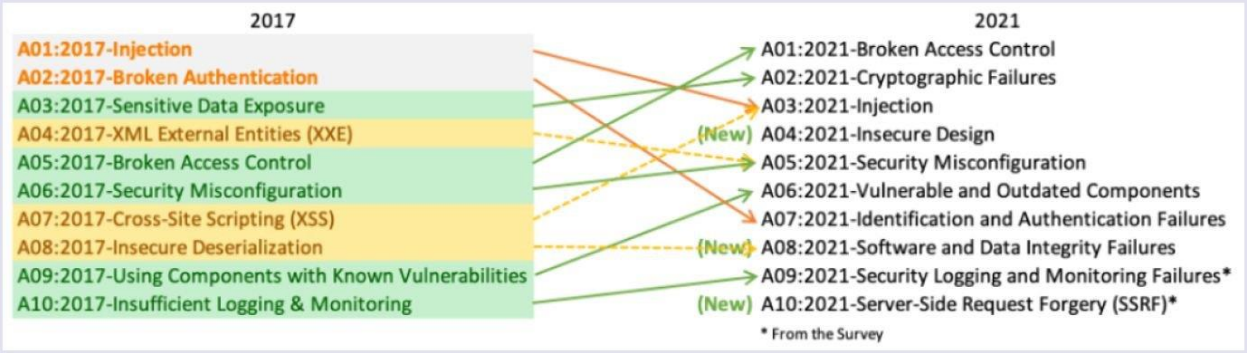


Рис. 1.8. Перелік найпоширеніших веб-загроз від OWASP та основні зміни переліку різних років

1. Порушення контролю доступу. Атаки можуть відбуватися, коли неправильно налаштовані дозволи аутентифікованого користувача. Тобто, користувач може мати більше дозволів, ніж потрібно. Зловмисники можуть скористатися цим і викрасти дані.

2. Криптографічні збої. Зазвичай це проблема з шифруванням під час передачі. Наприклад, під час використання HTTP замість HTTPS або застарілих алгоритмів хешування, таких як MD5 або SHA1, зловмисники можуть легко викрасти паролі, номери кредитних карток і все, що вводиться на сайті без шифрування, якщо дані користувача не зашифровані під час передачі.

3. Ін'єкції. Ін'єкції - одна з найпоширеніших технік веб-хакінгу. Ін'єкційні атаки дозволяють зловмисникам підробляти ідентифікаційні дані, втручатися в існуючі дані і навіть розкривати всі дані додатку організації. Отже, таке втручання може призвести до втрати даних або серйозних змін у структурі бази даних.

4. Незахищений дизайн. Атака може статися через широку категорію проблем, які можна виразити як «відсутній або неефективний дизайн управління». Прикладом цього є недотримання найкращих архітектурних практик.

5. Неправильна конфігурація безпеки. Атака може статися через паролі за замовчуванням, шкідливі бібліотеки або наявність непотрібних компонентів у програмі.

6. Уразливості програми та застарілі компоненти. Атаки можуть відбуватися, коли користувач не знає, в якому стані знаходиться поточне програмне

забезпечення. Наприклад, воно може бути застарілим, або бібліотеки не мають жорсткого кодування версій. У такому випадку варто звернути увагу, що якщо ви при оновленні цих компонентів, потрібно їх протестувати.

7. Помилки ідентифікації та автентифікації. Ці помилки пов'язані з керуванням сеансами. Наприклад, використання слабких паролів або недостатній захист сесій - це ймовірність того, що токени можуть бути використані пізніше. Таким чином, хакери можуть викрасти облікові дані для сеансу або зламати додаток.

8. Порушення цілісності програмного забезпечення та даних. Варто переконатися, що на кожному етапі розробки програмного забезпечення забезпечується цілісність додатку. Використовуйте лише надійні сховища. Крім того, переконайтеся, що код залишається інтегрованим під час потоку CI/CD (безперервна інтеграція/поставка). Конвеєр CI/CD - це абстрактна автоматизована серія кроків, які необхідно виконати для тестування, побудови та доставки додатку.

9. Ведення журналів безпеки та моніторинг збоїв. Часто практикується не приділяти належної уваги логуванню та моніторингу. Тим не менш, варто відстежувати активність API, сеанси і входи в систему за допомогою інструментів моніторингу. Таким чином, можна побачити, коли зловмисник входив в систему і які дії він виконував. Але варто не забувати, що логи не повинні містити облікових даних або будь-яких конфіденційних даних.

10. Підробка запитів на стороні сервера (SSRF). Це може бути викликано тим, що зловмисник може надати URL-адреси, які викличуть певні дії на сервері. Ці дії можуть бути будь-якими, від читання даних додатку до метаданих сервера.

Кажуть, що поінформований - значить озброєний. Знаючи різні ризики веб-безпеки, можна вжити заходів і запобігти їм. Для забезпечення високого рівня безпеки веб-продуктів важливо використовувати сучасні практики та інструменти. Один із ключових підходів — інтеграція з сервісами безпеки, такими як AWS WAF і AWS Shield, які забезпечують захист від загроз на рівні веб-додатків та мережі. Для централізованого моніторингу варто застосовувати AWS Security Hub, який збирає дані з різних сервісів безпеки, створюючи єдине інформаційне середовище.

Рекомендується впроваджувати багатофункціональні секрети для захисту облікових даних та інтегрувати сканери безпеки. Сканери зображень контейнерів дозволяють виявляти вразливості у додатках, які працюють у контейнерах, що забезпечує регулярний моніторинг і захист від атак.

Типи тестування безпеки веб-додатків

Для підвищення безпеки слід застосовувати різні підходи до тестування:

- Статичне тестування безпеки додатків (SAST). Використовується на етапі написання коду, дозволяючи аналізувати його на наявність уразливостей. Прикладами таких інструментів є Brakeman для Ruby або Bandit для Python.
- Динамічне тестування безпеки додатків (DAST). Виконується шляхом моделювання атак на веб-додатки ззовні. Для цього можна використовувати інструменти, такі як Abbey Scan, AppScan або AppSpider.
- Аналіз складу програмного забезпечення (SCA). Виконується для перевірки компонентів з відкритим вихідним кодом, які можуть містити вразливості. Це допомагає запобігти інцидентам, подібним до Log4Shell.

Цей комплексний підхід, що включає інтеграцію з сервісами безпеки, впровадження спеціалізованих інструментів і багаторівневе тестування, забезпечує надійний захист веб-продуктів та інфраструктури.

Рис. 1.9. Типи тестування безпеки додатків

Підхід та філософія DevSecOps

DevSecOps (розробка, безпека та експлуатація) визначає практики, які є майже необхідними в сучасній розробці програмного забезпечення. Однак ми виділимо лише найважливіші з них.

Ми всі знаємо, що операції з безпеки веб-додатків часто можуть сповільнювати процес розробки. Критично важливим тут є «зсув вліво» операцій з безпеки. Це означає зусилля DevOps, спрямовані на забезпечення безпеки на ранніх стадіях розробки веб-додатків.

Дійсно, ця практика внесе зміни у ваш конвеєр розробки. Наприклад, ви можете відмовити у розгортанні, якщо додаток має більше X вразливостей безпеки.

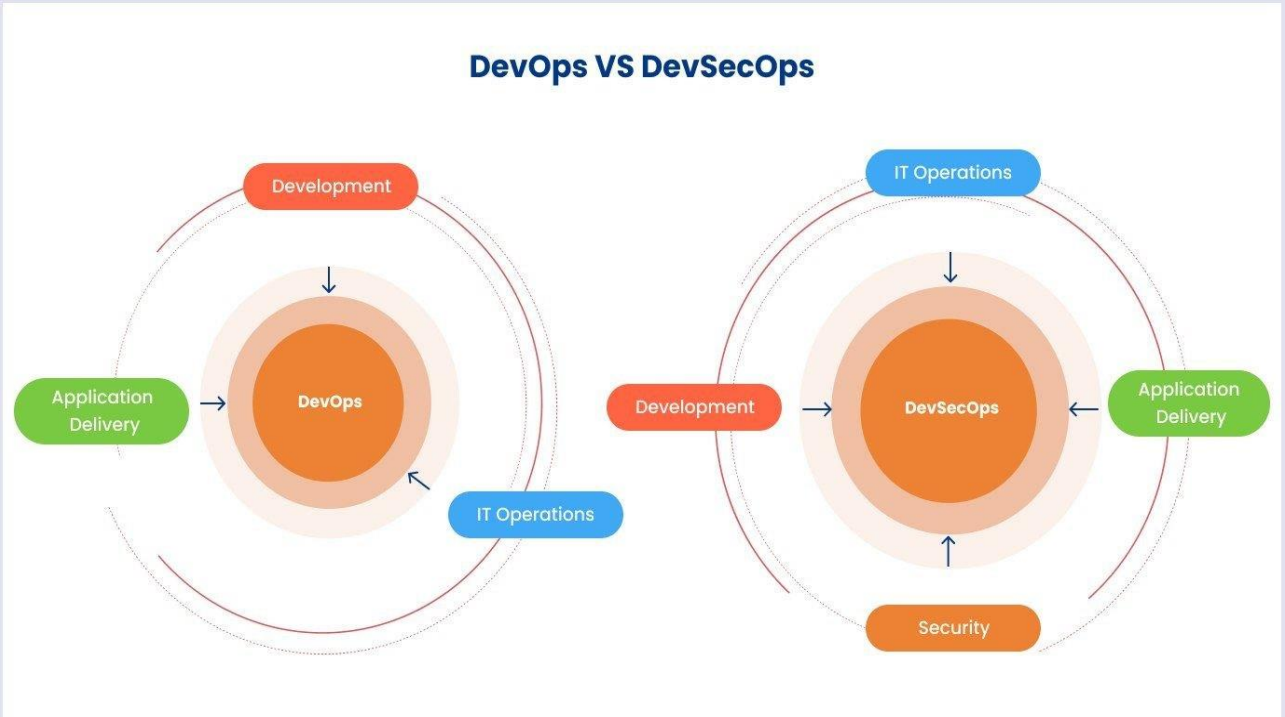


Рис. 1.10. Різниця між DevOps і DevSecOps

У процесі аналізу вразливостей додатків та інструментів для їх захисту було виявлено важливість застосування комплексного підходу до забезпечення безпеки. Серед найбільш ефективних засобів захисту варто зазначити використання служб безпеки AWS, інструментів моніторингу, а також багатофункціональних секретів. Кожен з цих інструментів відіграє ключову роль у зміцненні безпеки, проте для досягнення максимального ефекту необхідно забезпечити збалансованість між усіма складовими програми та інфраструктури.

Важливим аспектом є налаштування пріоритетів безпеки, що дозволяє своєчасно виявляти та знижувати ризики. Ідентифікація загроз для бізнесу та визначення пріоритетів для їх захисту допомагають сконцентрувати зусилля на найбільш критичних ділянках. Таким чином, комплексний підхід до безпеки, який включає використання сучасних інструментів та стратегій, дозволяє значно знизити рівень уразливостей і мінімізувати потенційні загрози для організації. [8]

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ AKAMAI KONA SITE DEFENDER

2.1. Порівняння існуючих рішень для захисту веб-додатків

Оскільки майже 45% кібератак спрямовані на веб-додатки, забезпечення їх безпеки є надзвичайно важливим. WAF (Firewall веб-додатків) є одним із найбільш рекомендованих інструментів для захисту таких додатків. Популярність використання WAF настільки зросла, що очікується, що глобальний ринок цих рішень досягне обсягу 8,06 мільярда доларів до 2026 року.

Хоча ринок WAF рясніє різноманітними рішеннями, не всі з них забезпечують належний рівень захисту для веб-додатків. Ми провели порівняння двох найбільш відомих інструментів WAF: Akamai та Cloudflare, щоб оцінити їх ефективність у реальних умовах.

Akamai є одним із лідерів на ринку рішень безпеки, і його WAF, Kona Site Defender, надає потужний захист для програм і API. Це рішення, що має високий рівень захисту (WAAP), включає функції, як динамічне та самоадаптивне реагування, виявлення API, а також надає практичну інформацію про безпеку, що дозволяє забезпечити найкращий захист у своєму класі.

З іншого боку, Cloudflare WAF пропонує керовані правила для запобігання загрозам нульового дня та найпоширенішим атакам з OWASP Top 10. Це рішення вимагає мінімальних налаштувань і забезпечує захист від таких загроз, як крадіжка облікових записів, SQL-ін’єкції та атаки XSS.

Незважаючи на обіцянки обох рішень, реальна ефективність дещо відрізняється. Під час тестування були виявленні випадки обходу захисту як у Cloudflare, так і в Akamai.

У випадку з Cloudflare вдалося обійти захист 392 рази, що є значною кількістю.

Щодо Akamai, хоча кількість випадків обходу була менша, вони все ж мали місце: 131 інцидент обходу. Ці результати чітко показали, що обидва рішення не є

настільки ефективними, як вони стверджують. Для детальнішої оцінки їхньої ефективності ми провели масштабне тестування за допомогою GoTestWAF.

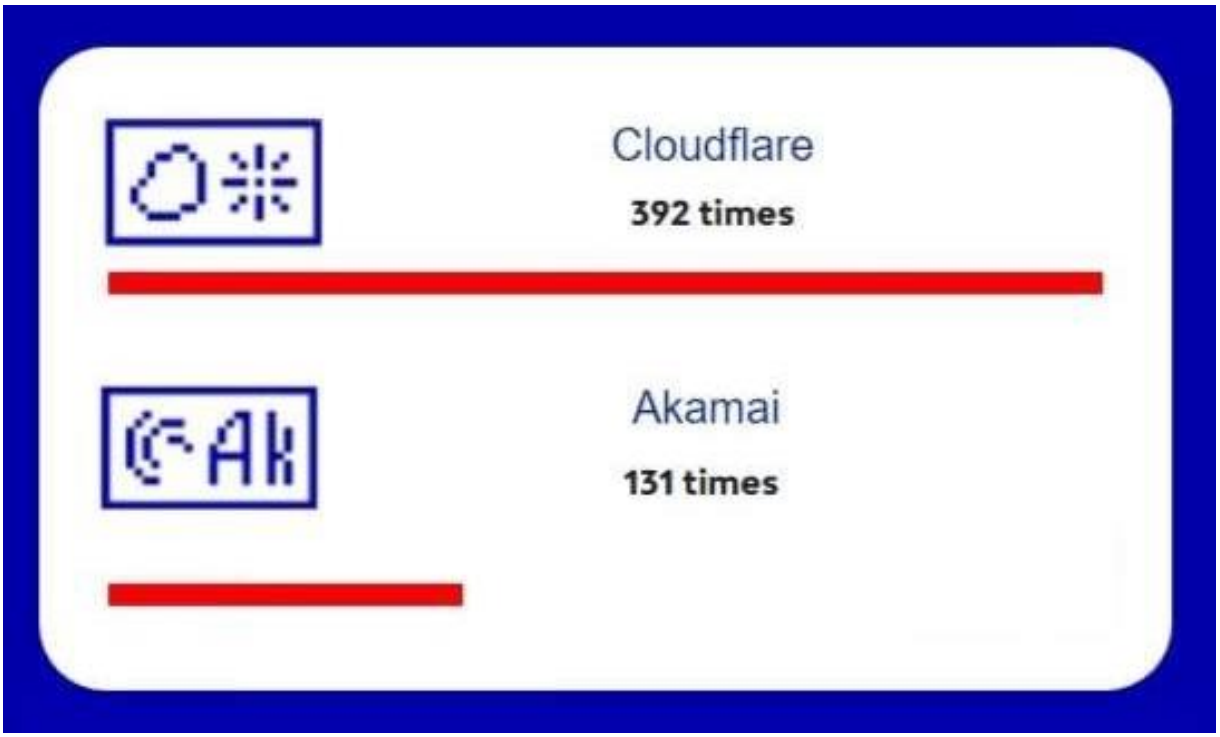


Рис. 2.1. Кількість обходів захисту порівнюваних рішень

Результати тестування цих двох WAF за допомогою GoTestWAF.

Результати тесту Akamai:

- Версія GoTestWAF: v0.3.1-286-g554f4d1
- Загальна оцінка: F
- Оцінка: 55,5/100
- Всього надіслано запитів: 1413
- Кількість заблокованих запитів: 788
- Кількість прийнятих запитів: 620

Akamai отримав оцінку A+ у тесті True-positive, оскільки заблокував 98,6% запитів. У безпеці додатків його оцінка B-.

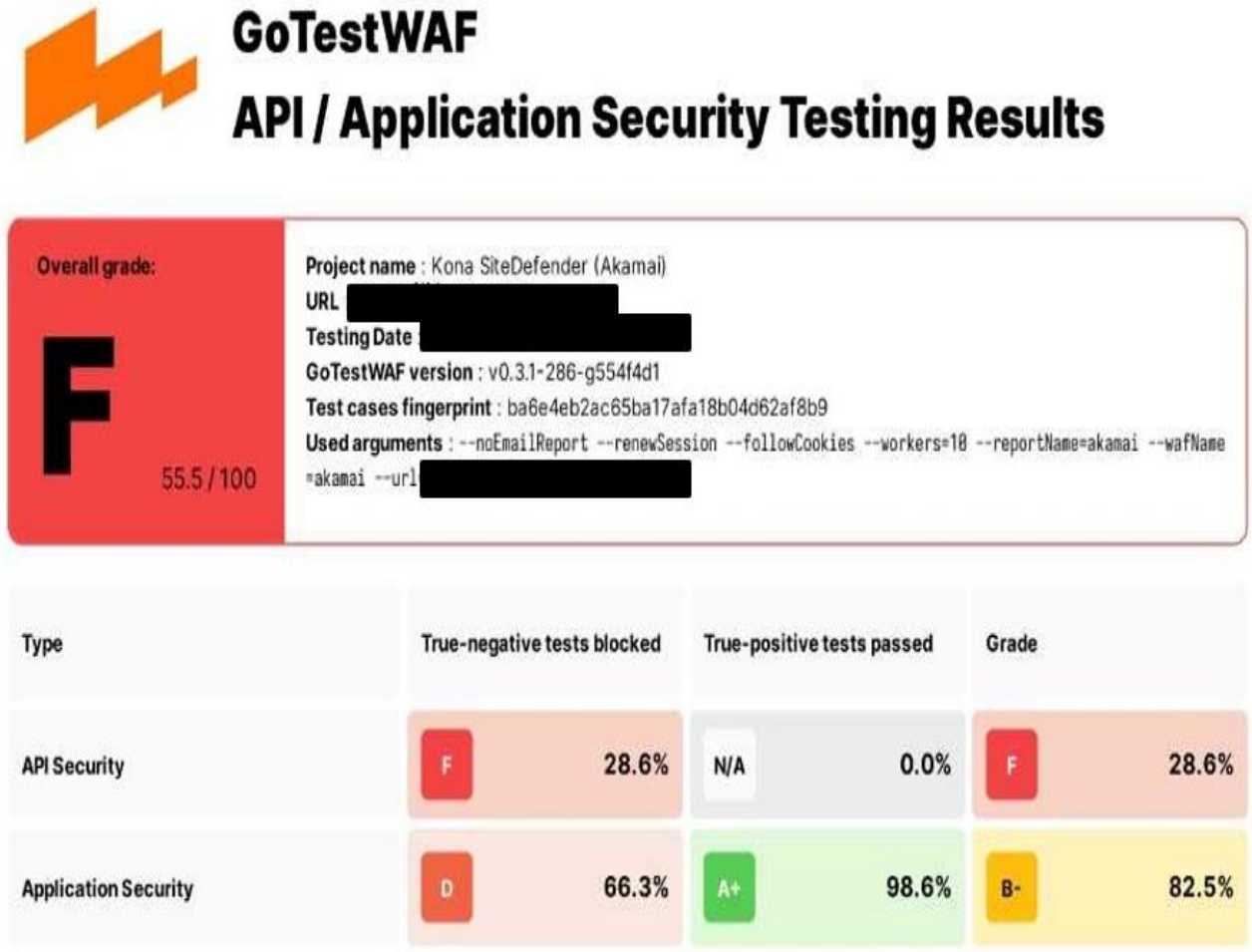


Рис. 2.2. Результати тестування Akamai

Тест безпеки API Akamai показав, що він блокує 100% запитів REST. Але лише 10% запитів GraphQL блокуються.

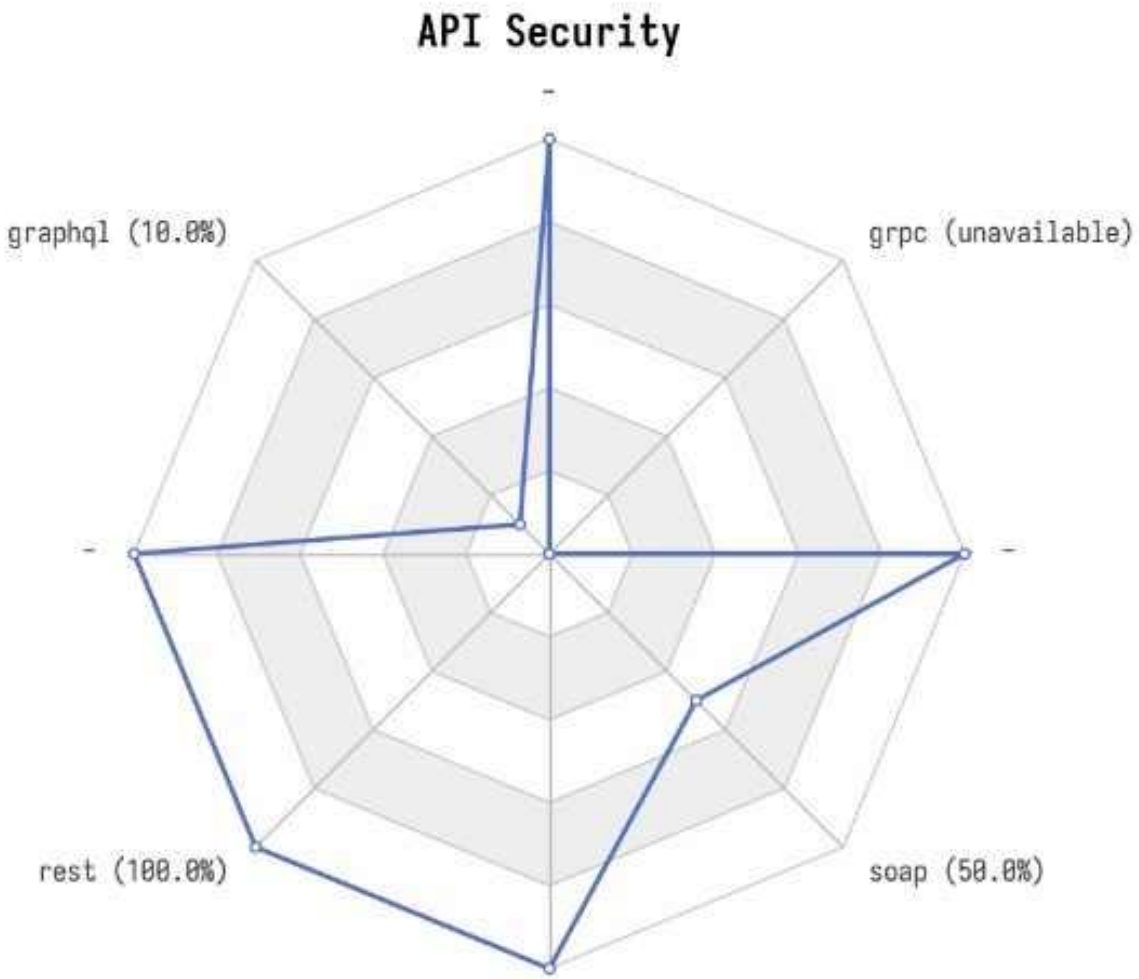


Рис. 2.3. Результати тестування API Akamai

Результат тесту Cloudflare

- Версія GoTestWAF: v0.3.1-286-g554f4d1
- Загальна оцінка: F
- Оцінка: 52,2 зі 100
- Всього надіслано запитів: 1413
- Кількість заблокованих запитів: 605
- Кількість прийнятих запитів: 788

Під час тестування Akamai за допомогою GoTestWAF було виявилено, що система не змогла ефективно заблокувати реальні негативні запити, як у контексті захисту API, так і в рамках захисту веб-додатків. Щодо справжньо позитивних

тестів, вдалося відслідкувати лише захист додатків, і результати виявилися відмінними, оскільки 100% запитів було успішно заблоковано.

Type	True-negative tests blocked	True-positive tests passed	Grade
API Security	F 28.6%	N/A 0.0%	F 28.6%
Application Security	F 51.6%	A+ 100.0%	C 75.8%

Рис. 2.4. Результати тестування веб-додатків

Безпека API Akamai була перевірена за допомогою GoTestWAF. Тестування API gRPC виявилося недоступним, однак були отримані результати для GraphQL, SOAP та REST. Результати наведені нижче.

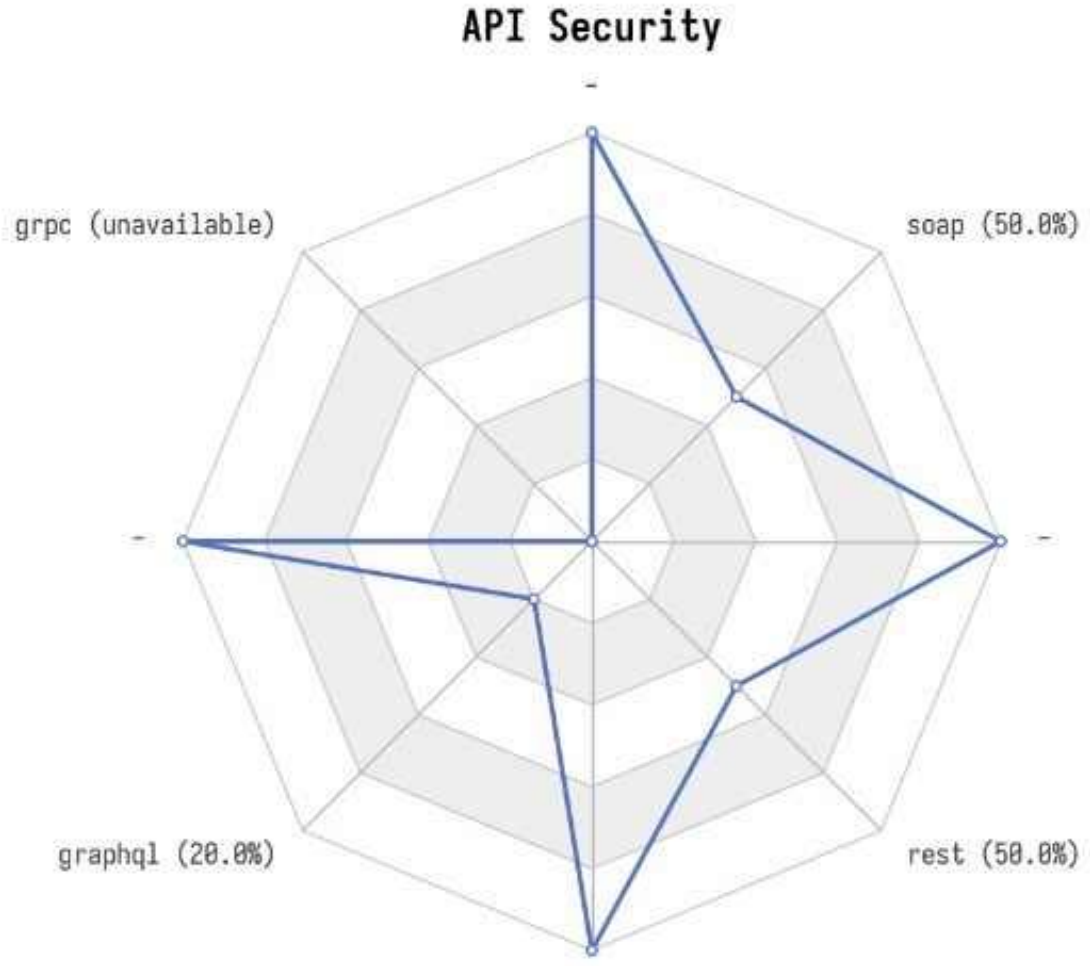


Рис. 2.5. Тестування для GraphQL, SOAP та REST

Під час тестування безпеки програми було виявлено, що Akamai блокує 100% запитів SQL-ін’єкції та XSS.

Аналіз результатів тестування показав, що обидва ці WAF не справили на нас враження. Також було проведено тестування Wallarm WAF, і його результати виявилися значно більш вражаючими.

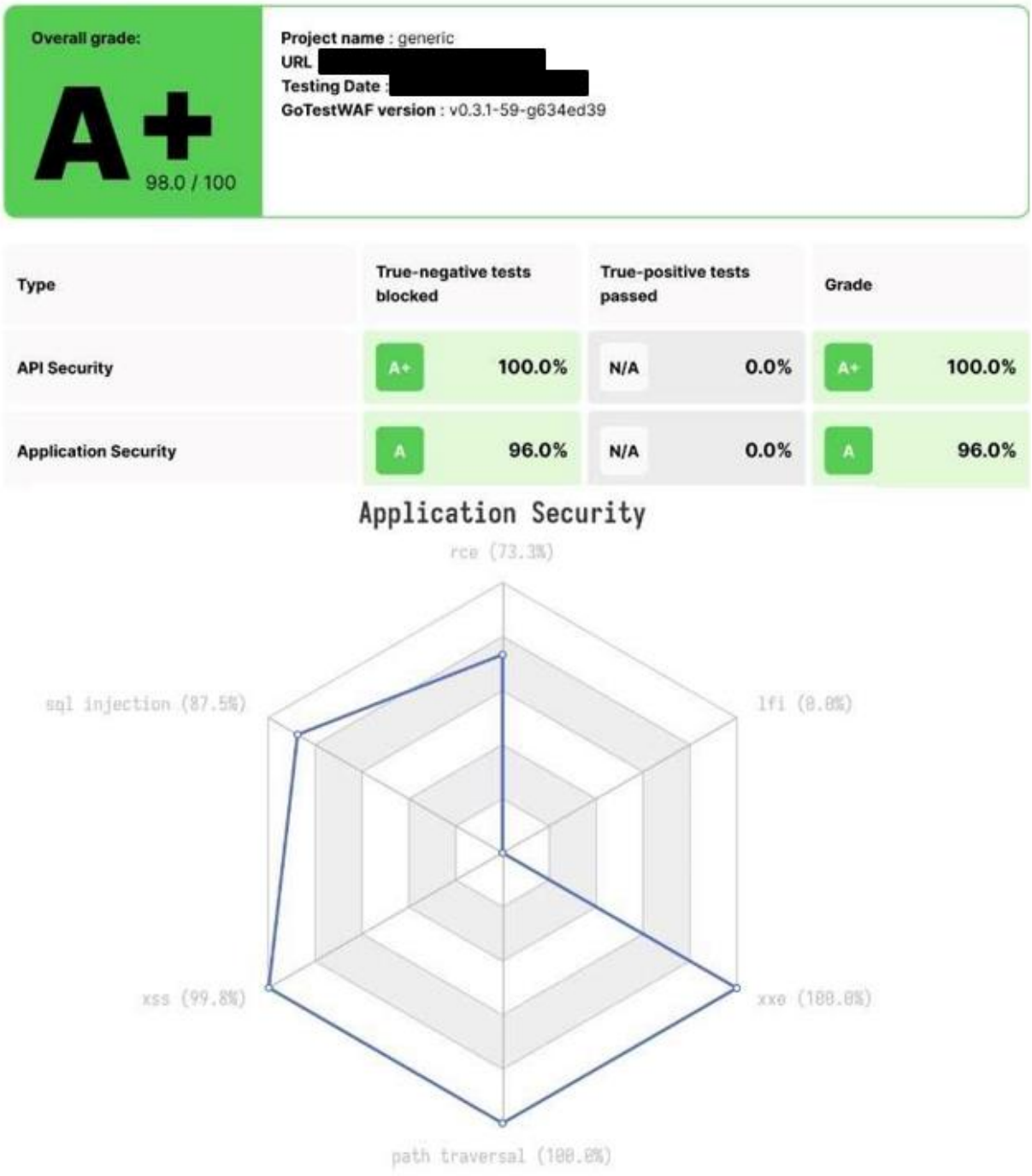


Рис. 2.6. Тестування Wallarm WAF

На основі порівняння Kona Site Defender від Akamai і Cloudflare WAF, можна зазначити, що обидва рішення демонструють сильні сторони, але Akamai має переваги в низці ключових аспектів. Akamai заблокував 98,6% істинно-позитивних запитів і досяг найвищого рівня захисту у випадках SQL-ін’єкцій та XSS-атак. Також його показники блокування REST-запитів значно перевищують результати Cloudflare, хоча в GraphQL-запитах результати були слабшими. [9]

2.2. Призначення та основні функції рішення Akamai Kona Site Defender

Akamai Technologies, Inc. (NASDAQ: AKAM), світовий лідер у сфері послуг мережі доставки контенту (CDN), сьогодні оприлюднила кілька важливих удосконалень у своєму флагманському рішенні Cloud Security Kona Site Defender. Оновлення, які стосуються таких областей, як правила брандмауера веб-застосунків (WAF), швидша реалізація правил, а також покращені звіти й аналітика, розроблені, щоб надати клієнтам знання, інструменти та технології, необхідні для забезпечення високої доступності їхніх веб-сайтів і додатків, водночас захист важливих даних і інформації про бізнес і клієнтів. [10]

Akamai Kona Site Defender є одним із найбільш ефективних рішень для захисту веб-додатків і інтернет-ресурсів від різноманітних кіберзагроз. Завдяки своїй гнучкості та багаторівневому підходу до безпеки, система забезпечує високий рівень захисту веб-додатків від таких загроз, як DDoS-атаки, ін’єкції коду, атаки на рівні веб-додатків та зловмисні запити. Оскільки веб-додатки є основними точками взаємодії користувачів та організацій, їх захист є критично важливим для забезпечення конфіденційності, цілісності та доступності даних. Akamai Kona Site Defender пропонує передові методи для досягнення цієї мети, застосовуючи хмарні технології для оперативного захисту.

Kona Site Defender — це хмарне рішення для захисту веб-додатків, яке пропонує широкий спектр можливостей для забезпечення безпеки на рівні додатків та інфраструктури. Цей продукт інтегрує різноманітні інструменти для боротьби з основними типами кіберзагроз, зокрема атаками типу DDoS, веб-вразливостями та

іншими атаками, що використовують шкідливі запити до серверів. Kona Site Defender допомагає організаціям захищатися від кібератак, забезпечуючи ефективну фільтрацію трафіку та аналізуючи взаємодію між користувачами та веб-сайтами.

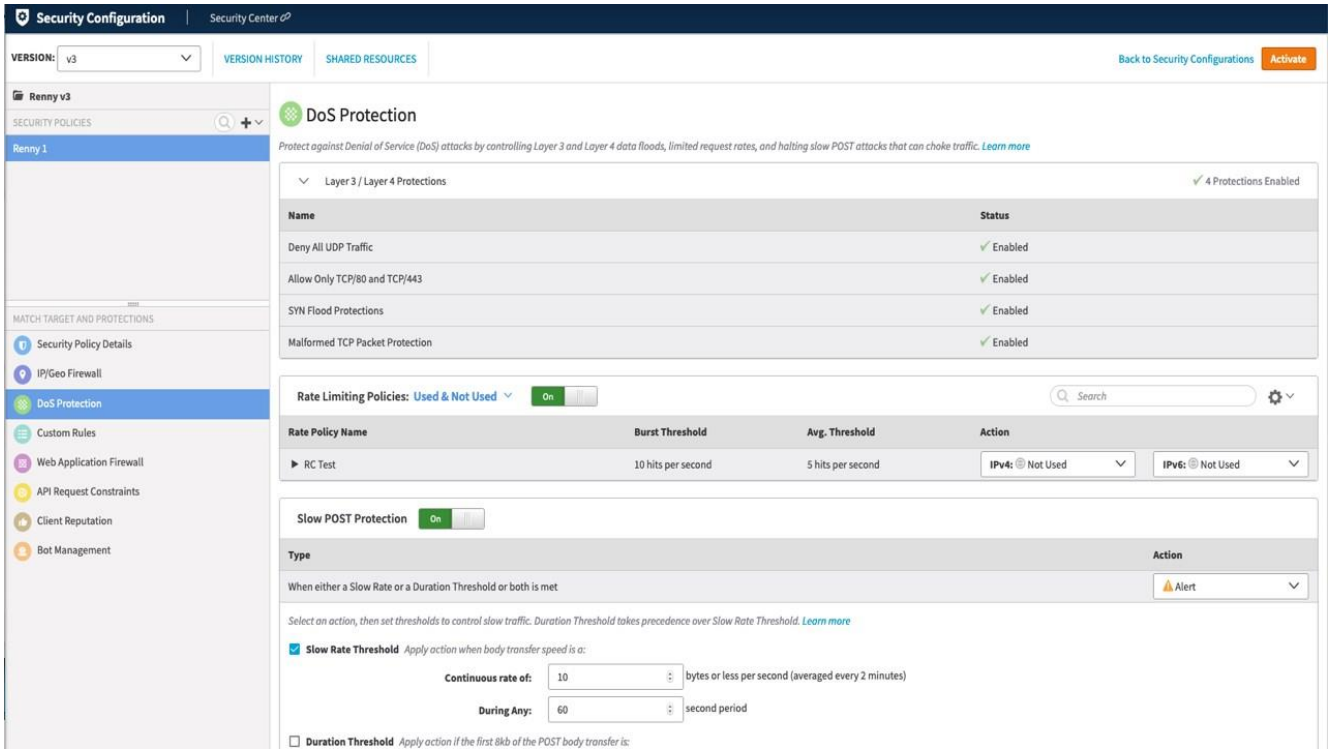


Рис. 2.7. Інтерфейс Akamai Kona Site Defender

Однією з ключових особливостей Akamai Kona Site Defender є його здатність забезпечувати захист від атак на всіх рівнях веб-інфраструктури. Це включає не лише механізми для захисту від DDoS-атак, але й інтеграцію з Web Application Firewall (WAF), який здатний захищати веб-додатки від ін’єкцій, XSS, CSRF та інших вразливостей, що можуть бути використані для компрометації веб-додатків.

- Захист від DDoS-атак

Однією з найбільш серйозних загроз для веб-додатків є атаки відмови в обслуговуванні (DDoS), які спрямовані на перевантаження серверів або інфраструктури великою кількістю запитів, що в свою чергу призводить до втрати доступності веб-ресурсу. Akamai Kona Site Defender використовує потужну хмарну

інфраструктуру для ефективного виявлення та запобігання DDoS-атакам, забезпечуючи:

Аналіз трафіку в реальному часі: система здатна здійснювати безперервний моніторинг і аналіз трафіку, виявляючи аномалії та вживаючи заходів для блокування шкідливих запитів, що надходять на сайт.

Розподілене блокування атак: завдяки глобальній інфраструктурі Akamai, система здатна здійснювати фільтрацію трафіку на рівні локальних точок присутності, що дозволяє значно знизити навантаження на сервери і підвищити ефективність захисту.

Інтелектуальна фільтрація трафіку: Kona Site Defender використовує передові алгоритми для виявлення та блокування підозрілих запитів, що дозволяє запобігти атакам в реальному часі, навіть якщо вони мають великі масштаби.

- Захист від вразливостей веб-додатків

Akamai Kona Site Defender має потужний набір інструментів для захисту веб-додатків від типових вразливостей, що можуть бути використані зловмисниками для виконання атак. Інтеграція з Web Application Firewall (WAF) дає можливість ефективно захищатися від таких атак, як:

SQL ін’єкції - це тип атаки, коли зловмисник намагається вставити шкідливий SQL-код через форму вводу або URL. Kona Site Defender здатний заблокувати такі запити до того, як вони досягнуть сервера.

Міжсайтове скриптування (XSS): атака XSS дозволяє зловмисникам вставляти шкідливі скрипти, які виконуються на стороні клієнта. Захист від цієї вразливості є важливим для забезпечення безпеки користувачів і їх даних.

Міжсайтове підроблення запитів (CSRF): атакуючи сайт через CSRF, зловмисники можуть здійснити небажані дії від імені користувача. KSD захищає від таких атак, перевіряючи запити і виявляючи спроби використання автентифікаційних даних користувача для виконання зловмисних дій.

Аналіз та профілювання трафіку дозволяють Kona Site Defender адаптувати правила безпеки до характеру трафіку, постійно оновлюючи захист і реагуючи на нові загрози. За допомогою цього підходу система автоматично застосовує

коригування в налаштуваннях безпеки в залежності від динаміки взаємодії з користувачами і атакуючими.

- Захист від бот-мереж

Веб-додатки часто стають жертвами автоматизованих ботів, які можуть використовуватися для спроб несанкціонованого доступу до ресурсу, збору даних або здійснення атак на систему. Kona Site Defender активно використовує інтелектуальні методи для виявлення ботів, включаючи такі заходи:

Виявлення аномалій в поведінці трафіку: за допомогою аналізу моделей поведінки трафіку система може відрізняти реальних користувачів від ботів.

Рішення CAPTCHA та аналіз цифрових відбитків пристроїв дозволяють додатково перевіряти користувачів, що мінімізує можливості використання автоматизованих систем для злому.

Kona Site Defender має хмарну архітектуру, що дозволяє масштабувати захист відповідно до потреб конкретного ресурсу. Система здатна обробляти високі обсяги трафіку, що робить її ідеальним рішенням для організацій будь-якого розміру.

Ще однією перевагою є те, що завдяки використанню глобальної інфраструктури Akamai, система забезпечує високу швидкість обробки запитів і знижує час відгуку, що є критичним для високонавантажених веб-додатків.

Автоматичне оновлення правил безпеки: Akamai Kona Site Defender автоматично оновлює свої правила безпеки, що дозволяє швидко реагувати на нові загрози та атаки, знижуючи ймовірність компрометації системи.

Також перевагою є низька затримка і висока доступність. Оскільки рішення реалізовано в хмарі, воно забезпечує високу доступність і зменшує навантаження на власну інфраструктуру компанії, що дозволяє зберігати стабільну роботу веб-додатків навіть в умовах високого трафіку.

Хоча Akamai Kona Site Defender є потужним і ефективним рішенням для захисту веб-додатків, воно має і деякі обмеження:

- для малих і середніх підприємств вартість цього рішення може бути відносно високою. Ціна залежить від кількості запитів та обсягу трафіку, тому для організацій з обмеженим бюджетом це може стати суттєвим фактором.
- хоча хмарна архітектура забезпечує високу гнучкість і масштабованість, вона також створює залежність від доступності Інтернету та може мати проблеми в разі великих технічних збоїв або атак на саму інфраструктуру Akamai.

Akamai Kona Site Defender є надійним та потужним рішенням для захисту веб-додатків, яке комбінує в собі передові технології для забезпечення захисту від атак на рівні веб-додатків та інфраструктури. Завдяки інтеграції з WAF, а також потужним методам виявлення та запобігання DDoS-атакам, цей продукт є ефективним інструментом для організацій, які прагнуть забезпечити високу безпеку власних веб-ресурсів. Однак вартість та залежність від хмарної інфраструктури можуть бути певними обмеженнями для малих підприємств або тих, хто шукає рішення для специфічних технічних умов. [11]

2.3. Переваги та особливості використання рішення Akamai Kona Site Defender

Kona Site Defender забезпечує захист веб-сайтів і API від широкого спектра атак, включаючи складні DDoS-атаки, атаки на веб-додатки та прямі атаки на сервери. Для цього використовується багатошарова система захисту, яка працює безперервно. Рішення інтегровано в Akamai Intelligent Platform™, що складається з понад 200 000 серверів, розташованих у 3500 локаціях по всьому світу в 131 країні на 1600 мережах. Така архітектура дає можливість здійснювати блокування атак на ранніх етапах, на рівні краю мережі Akamai, і значно знижує навантаження на вебсервери і додатки.

Однією з основних функцій Kona Site Defender є постійний захист від DDoS-атак. Веб-брандмауер додатків поглинає атаки на рівні додатків і автентифікує валідний трафік на краю мережі. Для кожної атаки система автоматично реагує за

кілька секунд, застосовуючи вбудовані механізми захисту. У разі складних або нових атак, що потребують індивідуального підходу, експерти з безпеки можуть створювати спеціалізовані правила на основі підписів загроз. Крім того, архітектура Akamai Intelligent Platform™ передбачає використання зворотного проксі-сервера, який приймає трафік лише через порти 80 і 443 і автоматично блокує всі атаки на мережевому рівні. Це дозволяє ефективно поглинати найбільші мережеві атаки, що досягають швидкості до 61 Tbps, не порушуючи нормальну роботу системи. Захист від DDoS-атак на DNS-інфраструктуру може бути доповнений за допомогою рішення Fast DNS.

Kona Site Defender включає великий набір попередньо визначених правил брандмауера для рівня додатків, що дозволяє забезпечити гнучкий захист від атак на додатки. Команда Akamai Threat Research Team регулярно оновлює ці правила на основі внутрішніх даних розвідки, отриманих від моніторингу 15-30% глобального веб-трафіку. Такі оновлення значно підвищують точність виявлення загроз і знижують кількість хибних спрацьовувань. Крім того, налаштування правил дозволяють швидко вжити заходів проти нових уразливостей вебсайтів до того, як будуть впроваджені зміни в програмному забезпеченні.

Для захисту API від шкідливих запитів Kona Site Defender застосовує позитивні та негативні моделі безпеки. Користувачі можуть визначати, які запити та виклики є дозволеними. Kona Site Defender перевіряє параметри RESTful API на відповідність списку дозволених значень, а також проводить аналіз JSON-т bodies та параметрів шляху на наявність небезпечного вмісту. Для запобігання DDoS-атакам через API використовуються механізми обмеження частоти запитів. Крім того, система надає можливість аналітики та звітності на рівні API, що дає змогу здійснювати моніторинг безпеки та своєчасно реагувати на загрози.

У контексті широкого впровадження хмарних технологій, автоматизації та практик DevOps, організації повинні інтегрувати безпеку в свої гнучкі процеси розробки. Kona Site Defender забезпечує можливість програмного оновлення правил безпеки та інтеграції цих оновлень у процеси розробки. За допомогою наданих API для управління, розробники та адміністратори можуть автоматизувати

завдання налаштування безпеки в рамках процесів CI/CD, що дозволяє забезпечити постійну відповідність політик безпеки до змін у розроблених системах.

Akamai Technologies, Inc., лідер у галузі доставки контенту та забезпечення кібербезпеки, представила оновлену версію свого рішення Kona Site Defender, яка забезпечує вдосконалений захист веб-додатків і сайтів. Ці покращення охоплюють адаптацію правил веб-додаткового брандмауера (WAF) до нових типів атак, оптимізацію швидкості впровадження правил і розширення можливостей аналітики. Метою таких змін є гарантування стабільності роботи веб-ресурсів та ефективний захист даних клієнтів і організацій.

Kona Site Defender поєднує автоматизовані механізми захисту від атак DDoS та потужний веб-додатковий брандмауер, забезпечуючи багаторівневий захист від найпоширеніших загроз. Серед них атаки DDoS на прикладному та мережевому рівнях, SQL-ін’єкції та XSS-атаки. Ця технологія, успішно інтегрована у майже 900 клієнтських ресурсів, дозволяє підтримувати високу продуктивність систем навіть за умов атак, не впливаючи на якість користувацького досвіду.

До складу останніх оновлень входять нові правила WAF, створені для протидії специфічним загрозам, як-от вразливості HTTP.sys та ін’єкції шаблонів серверної сторони (Server Side Template Injection). Глобальна платформа Akamai надає можливість спостерігати за світовими тенденціями трафіку, дозволяючи оперативно оновлювати захисні правила та усувати прогалини в безпеці. Впровадження нових правил тепер здійснюється за менш ніж хвилину, що забезпечує миттєву реакцію на виявлені загрози та знижує ризики простою веб-ресурсів.

Оновлення також включають вдосконалені інструменти аналітики та звітності. Новий модуль аналізу загроз надає користувачам доступ до даних про атаки за останні 72 години, що дозволяє не лише реагувати на актуальні загрози, але й прогнозувати майбутні ризики. Функція "Header Visibility" забезпечує детальний огляд запитів, які активували тригери безпеки, дозволяючи з’ясувати природу загроз і оптимізувати механізми захисту.

Крім цього, клієнти можуть скористатися послугами експертів команди Global Security Services, яка проводить аудит безпеки, надає рекомендації щодо вдосконалення конфігурацій та допомагає з реалізацією змін. Це забезпечує додатковий рівень захисту для організацій, які використовують Akamai Cloud Security Solutions.

Akamai постійно вдосконалює свої рішення, інтегруючи найсучасніші технології захисту, що дозволяє ефективно протидіяти новим типам кіберзагроз і забезпечувати надійну безпеку веб-додатків та інфраструктури клієнтів.[12]

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ

3.1. Технологія застосування рішення Akamai Kona Site Defender

Створення інноваційних цифрових досвідів часто включає використання безсерверних технологій на межі мережі, архітектур на основі мікросервісів, середовищ IaaS, функціональності на стороні клієнта та API. Ці сучасні методи розробки, хоча й спрямовані на створення високоперсоналізованих, швидких та постійно доступних користувацьких досвідів, водночас вводять нові вразливості та ризики. IT та безпекові команди стикаються з проблемами підтримки бізнесу через високий темп випуску коду та неможливість встигати за змінами в додатках та API. Кіберзлочинці можуть швидко здійснити атаку на основі крадених облікових даних, придбати викрадені дані та орендувати ботнет. Для вирішення цих проблем часто потрібно використовувати кілька продуктів безпеки від різних постачальників, що, у разі їх неінтегрованості та складності використання, може призвести до зниження ситуаційної усвідомленості, збільшення витрат та виникнення внутрішньоорганізаційних тертя.

Конвергенція технологічних рішень

Використання кількох продуктів призводить до високих витрат, підвищеної складності та потреби в кваліфікованих кадрах, що є непосильним для багатьох організацій. Захист веб-додатків та API в умовах глобального бізнесу сьогодні вимагає цілісного та розширюваного захисту, який можна ефективно використовувати. У компанії Akamai поставлено завдання максимальної вартості завдяки універсальному і потужному захисту додатків і API, що автоматизований і простий у використанні.

Протягом кількох років глобальні аналітичні компанії та клієнти визнають компанію Akamai лідером у сфері безпеки додатків та API. Як лідер, компанія Akamai презентує нове рішення для захисту веб-додатків та API (WAAP), яке поєднує основні технології, такі як веб-фаєрвол додатків, боротьба з ботами, безпека API та захист від DDoS-атак в одному продукті.

Kona Site Defender використовує новий адаптивний механізм безпеки Akamai, що забезпечує сучасний підхід до захисту всіх веб-додатків та API.

Kona Site Defender надає потужний набір засобів захисту, спрямованих на досягнення максимальних результатів у забезпеченні безпеки. На відміну від рішень, які пропонують "достатній" захист, простота Kona Site Defender приховує в собі деякі з найсучасніших технологій. Більше 92% клієнтів Akamai використовують інструменти безпеки додатків і API в режимі блокування.

Виявлення атак у два рази швидше з п'ятикратним зниженням хибних спрацьовувань — нові багатовимірні адаптивні виявлення атак комбінують інтелект платформ Akamai з даними та метаданими кожного запиту веб-додатка чи API. Ці дані використовуються з логікою прийняття рішень, що дозволяє ідентифікувати і зупиняти атаки з високою точністю. Адаптивне виявлення дозволяє виявити вчетверо більше атак за SQLi, XSS, RFI та CMDi з п'ятикратним зниженням хибних спрацьовувань без впливу на користувачів.

Зменшення ризику API завдяки автоматичному виявленню та захисту — автоматичний і безперервний аналіз трафіку дозволяє виявляти відомі, невідомі та змінювані API, їх кінцеві точки, визначення та характеристики, після чого застосовуються прості робочі процеси для захисту API від атак DDoS, ін'єкцій і крадіжки облікових даних. Кожен запит API автоматично перевіряється на наявність шкідливого коду, незалежно від того, чи застосовуються позитивні контрольні механізми безпеки.

Перегляд і зупинка зловмисних ботів — виявлення та зниження негативного впливу ботів забезпечується можливостями виявлення і боротьби з бот-трафіком, інтегрованими в Kona Site Defender. Технології виявлення ботів Akamai автоматично масштабуються в міру зростання бот-трафіку, забезпечуючи захист бізнесу. За допомогою цих технологій забезпечується видимість впливу ботів на цифрові активи і блокування поганих ботів у разі потреби.

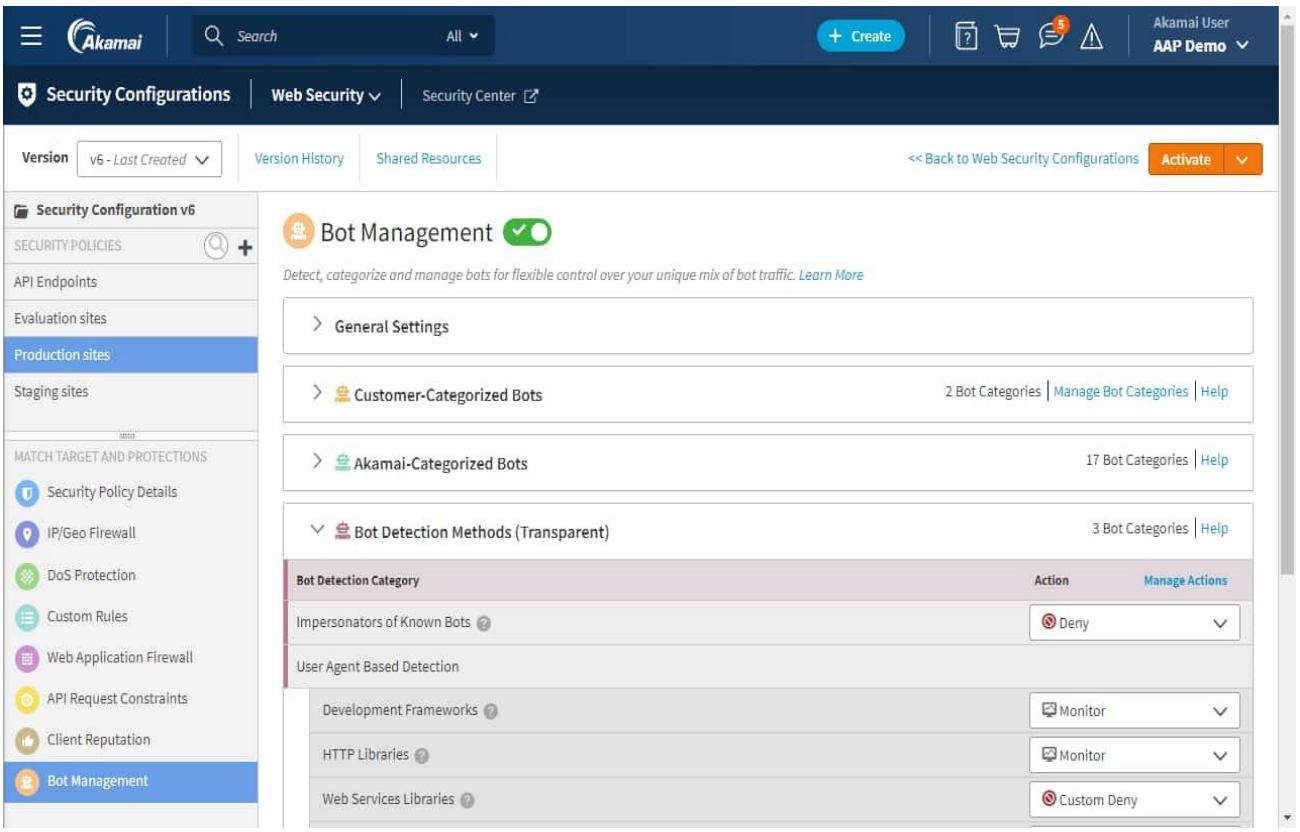


Рис. 3.1.Вбудовані можливості видимості ботів та мінімізації ризиків за допомогою Kona Site Defender

Продукти, що важко використовувати, призводять до ризиків та операційних витрат. Саме тому Kona Site Defender спроектовано з максимальною автоматизацією для спрощення щоденних завдань і дозволяє залишити складніші завдання для людського аналізу. Автоматизація продовжує удосконалюватися і розвиватися завдяки постійному оновленню технологій компанії Akamai.

Самоінтелектуальне налаштування для зниження навантаження на команду — усі тригери безпеки, включаючи справжні атаки та помилково ідентифіковані як атаки, автоматично та безперервно аналізуються за допомогою машинного навчання, з рекомендаціями для налаштування політик. Можливість отримувати сповіщення про нові рекомендації і приймати їх через інтерфейс користувача або автоматизувати за допомогою API або CLI.

Автоматичне оновлення захисту від дослідників Akamai — застосування повністю автоматизованого підходу до безпеки додатків і API з адаптивними захистами, що керуються компанією Akamai. Дослідники безпеки використовують

передові методи машинного навчання для безперервного аналізу даних атак і автоматичного оновлення захистів від нових загроз.

Інтеграція з DevOps для швидкої адаптації до бізнес-змін — інтеграція з API Akamai через CLI, Terraform або сценарії у CI/CD автоматизаційному процесі дозволяє швидко впроваджувати додатки, створювати єдині політики безпеки для великих портфелів додатків і API, централізувати виконання політик безпеки в гібридних і мультихмарних інфраструктурах, а також покращити співпрацю між командами DevOps та безпеки.

```
terraform {
  required_providers {
    akamai = {
      source = "akamai/akamai"
      version = "1.6.1"
    }
  }
}

provider "akamai" {
  edgerc = "~/.edgerc"
}

data "akamai_appsec_configuration" "configuration" {
  name = "AAP security configuration"
}

resource "akamai_appsec_selected_hostnames" "akamai_appsec_selected_hostname" {
   config_id = data.akamai_appsec_configuration.configuration.config_id
   mode = "REPLACE"
   hostnames = [
               "www.securitydemo.com",
               "qa.securitydemo.com"
               ]
}

resource "akamai_appsec_activations" "activation" {
   config_id = data.akamai_appsec_configuration.configuration.config_id
   network = "STAGING"
   notes  = "Activate initial security configuration"
   notification_emails = [ "john@securitydemo.com" ]
}
```

Рис. 3.2. Приклад HCL-коду для керування іменами хостів, захищеними Kona Site Defender, за допомогою Terraform

Організації мають переосмислити, що рішення WAAP не тільки забезпечують сильніший захист, але й додають цінність завдяки зручності використання. Цей спрощений робочий процес допомагає знизити ризики та забезпечує глибший контекст для розуміння кіберзагроз. Kona Site Defender спроектовано з принципом "простота передусім", щоб допомогти керівникам приймати обґрунтовані ризикові рішення у реальному часі і виконувати критичні завдання без операційного паралічу. [13]

3.2. Рекомендації щодо захисту веб-додатків організації на базі рішення Akamai Kona Site Defender

Для досягнення успіху в сучасному гіперзв’язаному світі підприємствам необхідно постійно працювати над інноваціями та забезпечувати належний рівень безпеки. Однією з основних перешкод для інновацій є загроза веб-атак. Для ефективного захисту важливо регулярно налаштовувати системи безпеки, щоб протистояти новітнім загрозам. У деяких випадках для забезпечення належного захисту необхідний цілодобовий моніторинг інфраструктури та швидке реагування на атаки. Ключовим аспектом побудови стійкої стратегії веб-захисту є вибір правильної технології, готовність до атак, проактивний моніторинг, періодичне налаштування систем безпеки та звітування, що дозволяє бути на крок попереду нападників і завжди готовими до можливих загроз.

Керована послуга Kona Site Defender орієнтована на компанії, які бажають делегувати моніторинг безпеки, нейтралізацію загроз і управління рішеннями Akamai Cloud Security. Для побудови надійного захисту ця послуга зосереджується на трьох основних напрямах: готовність до атак, моніторинг безпеки та підтримка під час атак, а також звітування з питань безпеки.

Оцінка загроз та готовності до атак передбачає регулярний аналіз веб-трафіку. У межах такого огляду проводиться ґрунтовний аналіз характеру трафіку відповідно до обраної політики захисту, що дозволяє оптимізувати захист і

блокувати шкідливий трафік, мінімізуючи кількість помилкових блокувань легітимних користувачів.

Конфігурація рішень для веб-захисту потребує періодичного налаштування, щоб залишатися актуальною та ефективною в умовах нових загроз. Керована послуга Kona Site Defender надає доступ до фахівців із безпеки, які допомагають налаштувати конфігурації відповідно до поточного ландшафту загроз.

Забезпечення готовності до атак передбачає відпрацювання комунікаційних процесів, шляхів ескалації та оперативної гнучкості через проведення навчальних "настільних вправ".

Цілодобовий моніторинг забезпечує своєчасне виявлення атак, що є критично важливим для їх нейтралізації. Послуга здійснює проактивний аналіз подій, зафіксованих у Kona Site Defender, що дозволяє виявляти загрози на ранніх етапах.

Підтримка під час атак включає надання допомоги експертами Akamai для розробки та впровадження тактичних заходів щодо нейтралізації загроз, а також забезпечення цілодобової підтримки для реагування на ситуацію.

Звітування з питань безпеки включає щомісячні звіти, що містять інформацію про зловмисну активність, інциденти безпеки та оновлення конфігурацій, а також підсумкові звіти після атак, що включають детальний аналіз події, вжиті заходи та рекомендації для запобігання подібним загрозам у майбутньому.

Для забезпечення високого рівня взаємодії з клієнтами надається персональний експерт із безпеки, який допомагає розвивати довгострокову стратегію захисту веб-додатків.

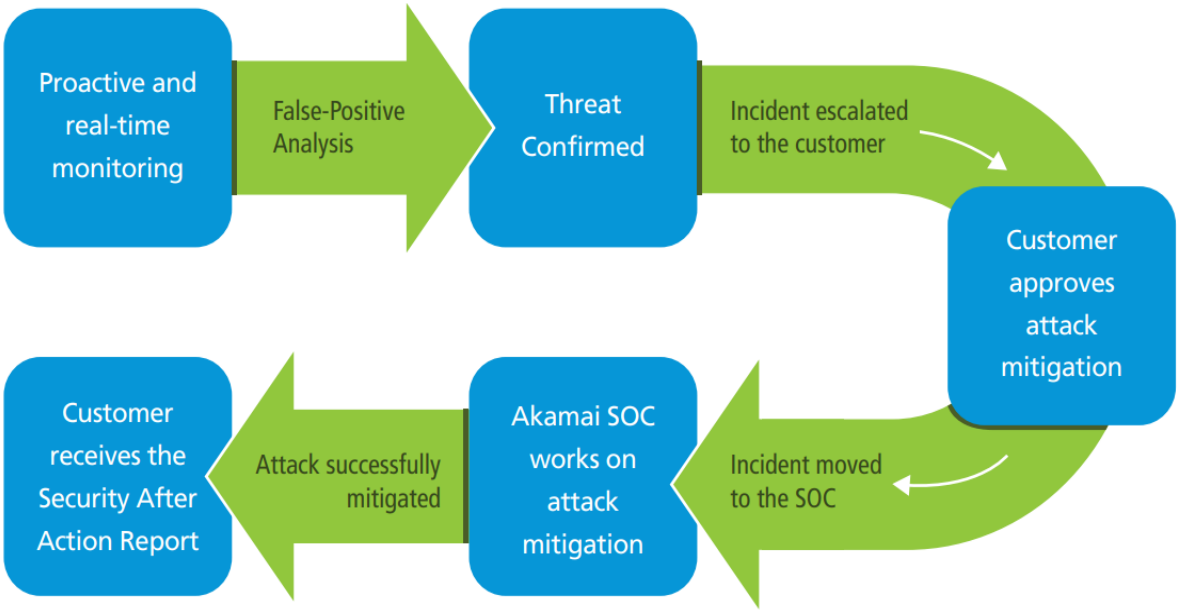


Рис. 3.3. Стратегія захисту веб-додатків від Akamai [14]

Послуга Managed Kona Site Defender надає доступ до експертизи Akamai та цілодобових операційних центрів безпеки для моніторингу, регулярного аналізу та оптимізації захисту веб-сайтів організацій. Це сприяє створенню надійної системи веб-захисту, здатної оперативно реагувати на хмарні атаки та підвищувати загальну стійкість інфраструктури.

Екосистема Akamai забезпечує високу швидкість, надійність і безпеку в Інтернеті. Рішення Akamai базуються на розподіленій платформі Akamai Intelligent Platform™ та керуються через настроюваний центр Luna Control Center, що дозволяє ефективно управляти безпекою та оптимізувати інфраструктуру для досягнення найкращих результатів у захисті веб-ресурсів.

3.3. Рекомендації щодо захисту веб-додатків організації

Забезпечення безпеки веб-додатків є критично важливим аспектом в умовах сучасного цифрового середовища. Веб-додатки стали невід’ємною частиною як особистого, так і професійного життя. Вони активно використовуються у

повсякденних взаємодіях між користувачами та цифровими сервісами, що підвищує значення їх безпеки. Однією з основних проблем для користувачів та організацій є безпечне зберігання та обробка чутливої інформації, що передається через ці додатки. Мова йде про фінансові дані, особисті дані та іншу конфіденційну інформацію, яку користувачі очікують зберігати в безпеці.

З метою забезпечення належного рівня захисту, веб-додатки повинні бути вільними від вразливостей, які можуть бути використані зловмисниками. Дотримуючись вказаних найкращих практик та здійснюючи проактивний підхід до забезпечення безпеки, можна гарантувати збереження даних користувачів та цілісність веб-додатків.

Забезпечення безпеки веб-додатків є важливою складовою розробки та експлуатації сучасних інформаційних систем. Веб-додатки повинні бути захищені від різноманітних кіберзагроз, що постійно еволюціонують. Для цього існують перевірені практики, які знижують ризики атак і підвищують рівень безпеки системи. Нижче наведено основні методи забезпечення безпеки веб-додатків.

1. Валідація введених даних. Один з основних аспектів безпеки веб-додатків — це валідація введених даних. Вразливості, такі як SQL-ін'єкції та міжсайтовий скриптинг (XSS), можуть виникати через неправильне оброблення користувацького вводу. Якщо введені дані не перевіряються належним чином, зловмисники можуть вводити шкідливі запити або скрипти, що призводить до витоку або втрати даних.

Для запобігання таким атакам необхідно здійснювати перевірку даних на клієнтській та серверній стороні. Серверна валідація повинна бути головним етапом перевірки, оскільки користувацькі дані можуть бути змінені на стороні клієнта. Для захисту від SQL-ін'єкцій слід використовувати параметризовані запити, а для боротьби з XSS — очищати введені дані від небезпечних символів і тегів.

2. Аутентифікація та контроль доступу. Аутентифікація та контроль доступу — важливі елементи захисту від несанкціонованого доступу. Всі

користувачі повинні проходити ідентифікацію, а доступ до функціоналу та даних має бути обмежений відповідно до їх ролей.

Для захисту паролів необхідно використовувати криптографічні хеш-функції, такі як bcrypt або Argon2, а також впроваджувати багатофакторну аутентифікацію (MFA), що підвищує рівень безпеки. Крім того, доцільно обмежити кількість спроб входу, щоб запобігти атакам методом підбору паролів.

3. Використання HTTPS та TLS шифрування. Веб-додатки повинні використовувати HTTPS для забезпечення зашифрованого з'єднання між клієнтом і сервером. Шифрування в HTTPS гарантує конфіденційність і цілісність даних, що передаються, та запобігає їх перехопленню і зміні під час передачі.

Протокол HTTPS використовує технологію TLS (Transport Layer Security) для забезпечення безпечного обміну даними. Важливо правильно налаштувати TLS, використовуючи сучасні алгоритми шифрування та регулярно оновлюючи сертифікати безпеки.

4. Обмін ресурсами між різними доменами (CORS). Політика CORS дозволяє обмежити доступ до ресурсів веб-додатка лише з довірених доменів. Використання правильних заголовків CORS допомагає запобігти атакам типу Cross-Site Request Forgery (CSRF) та XSS.

```
@Configuration
public class WebConfig implements WebMvcConfigurer {
   @Override
   public void addCorsMappings(CorsRegistry registry) {
       registry.addMapping("/**")
               .allowedOrigins("https://example.com")
               .allowedMethods("GET", "POST", "PUT", "DELETE", "OPTIONS")
               .allowedHeaders("*")
               .allowCredentials(true)
               .maxAge(3600);
   }
}
```

Рис. 3.4. Налаштування заголовків CORS

Заголовки CORS необхідно налаштовувати таким чином, щоб доступ до ресурсів мали тільки надійні домени. Це знижує ймовірність міжсайтових атак.

5. Пенетраційне тестування. Пенетраційне тестування є важливим методом перевірки безпеки веб-додатка шляхом симулювання атаки. Тестування дозволяє виявити вразливості та потенційні точки входу для зловмисників.

Пенетраційне тестування може бути виконане як за допомогою автоматизованих інструментів, так і вручну. Основною метою є перевірка на наявність уразливих місць, таких як SQL-ін'єкції, XSS та інші загрози.

6. Впровадження DevSecOps DevSecOps передбачає інтеграцію безпеки на всіх етапах життєвого циклу розробки програмного забезпечення. Це включає автоматизацію перевірок безпеки в процесах CI/CD, що дозволяє виявляти та виправляти вразливості ще на етапі створення коду.

DevSecOps також використовує превентивні заходи для захисту від ін'єкцій, XSS та витоків чутливих даних, що допомагає зменшити ризики.

7. Налаштування та розгортання Коректне налаштування середовища для розгортання веб-додатка є важливим етапом у забезпеченні його безпеки. Це включає налаштування веб-сервера, бази даних та використання безпечних методів кодування.

Також важливо забезпечити правильну конфігурацію серверів і баз даних. Сервери повинні бути захищені від несанкціонованого доступу, а бази даних — захищені від витоку чутливих даних.

8. Чек-лист безпеки веб-додатків від OWASP. OWASP (Open Web Application Security Project) надає набір рекомендацій для забезпечення безпеки веб-додатків. Виконання цього чек-листа допомагає запобігти типові загрози, такі як ін'єкції, проблеми з аутентифікацією та конфіденційністю даних.

9. Правильна практика ведення журналів. Моніторинг і ведення журналів є важливими для своєчасного виявлення загроз. Журнали повинні містити інформацію про всі критичні події та зміни, що дозволяє відслідковувати дії зловмисників і швидко реагувати на інциденти.

При веденні журналів необхідно переконатися, що чутливі дані, як-от паролі або номери карток, не потрапляють у журнали без маскування.

10. Веб-фаєрвол (WAF). Веб-фаєрвол (WAF) допомагає захистити веб-додаток від типових атак, таких як SQL-ін'єкції, XSS та DoS-атаки. WAF аналізує вхідний трафік і блокує шкідливі запити, що дозволяє знизити ймовірність атак на додаток.

Незважаючи на те, що WAF не є універсальним засобом захисту від усіх типів атак, його правильна конфігурація є першою лінією оборони для веб-додатка. [15]

Безпека веб-додатків є критично важливим аспектом захисту конфіденційних даних і забезпечення загальної функціональності програми. Зі збільшенням кількості кіберзагроз важливо впроваджувати найкращі практики безпеки веб-додатків, щоб запобігти несанкціонованому доступу та витоку даних.

ВИСНОВКИ

Ефективний захист веб-додатків є ключовим елементом для забезпечення безпеки організаційних ресурсів. Аналіз основних загроз для веб-додатків, таких як DDoS-атаки, ін'єкції SQL, XSS, а також методи їх запобігання, дозволив виявити важливість комплексного підходу до забезпечення безпеки.

Одним із важливих елементів є правильна конфігурація та впровадження заходів безпеки на різних етапах розробки та експлуатації веб-додатків. Це включає використання механізмів автентифікації та авторизації, шифрування даних, регулярний моніторинг безпеки та своєчасне оновлення програмного забезпечення.

Особливу увагу було приділено використанню спеціалізованих рішень, таких як WAF, а також інтеграції з хмарними сервісами для забезпечення додаткового рівня захисту. Усі ці заходи, застосовані в комплексі, забезпечують стійкість до різноманітних загроз і дозволяють зменшити ймовірність успішного вторгнення.

Враховуючи швидкий розвиток технологій та появу нових загроз, постійний моніторинг та оновлення засобів захисту веб-додатків є необхідними для забезпечення належного рівня безпеки. Застосування сучасних технологій, наявність навчання персоналу та створення ефективних процедур реагування на інциденти допомагають організаціям мінімізувати ризики і забезпечити безперебійну роботу веб-ресурсів.

Akamai Kona Site Defender забезпечує не лише високий рівень захисту від зовнішніх атак, але й допомагає забезпечити стабільну роботу веб-додатків навіть у випадках великих навантажень. Завдяки впровадженню технології автоматичного реагування на загрози та постійного моніторингу трафіку, організація отримує можливість оперативно виявляти та усувати потенційні вразливості.

Основними перевагами рішення є високий рівень автоматизації процесів захисту, простота інтеграції в існуючу інфраструктуру та масштабованість. Крім того, Akamai Kona Site Defender дозволяє здійснювати централізоване управління безпекою та моніторинг трафіку, що значно полегшує адміністративну роботу. Завдяки багатошаровій системі захисту, високій доступності і швидкості

реагування на загрози, він забезпечує організаціям ефективний захист від DDoS-атак, веб-атак та атак на API, дозволяючи знижувати ризики простоїв і крадіжки даних. Система також пропонує можливості для інтеграції безпеки в процеси DevOps, що дозволяє підтримувати високий рівень безпеки при швидкому розвитку і оновленні веб-додатків.

Рішення Akamai Kona Site Defender є ефективним інструментом для організацій, які прагнуть забезпечити високий рівень безпеки власних веб-додатків, зокрема, в умовах постійно зростаючих кіберзагроз. Впровадження цієї технології дозволяє мінімізувати ризики втрати даних, забезпечити надійний захист від атак і підтримувати стабільну роботу веб-ресурсів на всіх етапах їх експлуатації.

ПЕРЕЛІК ПОСИЛАНЬ

1. What Is Web Application Security and How Does It Work? | Black Duck. Application Security Software (AppSec) | Black Duck. URL: https://www.blackduck.com/glossary/what-is-web-application-security.html (дата звернення: 10.10.2024).

2. Web Application Security: Risks, Technologies & Best Practices | CyCognito. CyCognito. URL: https://www.cycognito.com/learn/application-security/web-application-security.php (дата звернення: 10.10.2024).

3. Top 10 Web Application Security Practices You Need to Know. ZeroThreat. URL: https://zerothreat.ai/blog/best-practices-for-secure-web-app-development (дата звернення: 16.10.2024).

4. Web Application Security: Threats and 6 Defensive Methods. Bright Security. URL: https://brightsec.com/blog/web-application-security/ (дата звернення: 16.10.2024).

5. What is a Web Application Attack, and How Can You Prevent it?. CHEQ | The Go-to-Market Security Platform. URL: https://cheq.ai/blog/what-is-web-application-attack/ (дата звернення: 24.10.2024).

6. Lohvynenko A. 8 Web Application Security Best Practices: Fortifying Your Product. MobiDev. URL: https://mobidev.biz/blog/best-practices-to-secure-web-applications-from-vulnerabilities (дата звернення: 31.10.2024).

7. OWASP Application Security Verification Standard (ASVS) | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-application-security-verification-standard/ (дата звернення: 02.11.2024).

8. Web Application Security: Risks, Tools & 9 Best Practices. Software Development Company | Codica. URL: https://www.codica.com/blog/web-application-security/ (дата звернення: 01.11.2024).

9. Comparison of “Kona Site Defender” By Akamai and Cloudflare WAF In Practice – Web application firewalls bypasses collection and testing tools. Web

application firewalls bypasses collection and testing tools – How to test, evaluate, compare, and bypass web application and API security solutions like WAF, NGWAF, RASP, and WAAP. URL: https://waf-bypass.com/comparison-of-kona-site-defender-by-akamai-and-cloudflare-waf-in-practice/ (дата звернення: 06.11.2024).

10. KONA SITE DEFENDER PROTECT YOUR WEBSITES AND WEB APPLICATIONS FROM DOWNTIME AND DATA THEFT. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWBnqk (дата звернення: 07.11.2024).

11. Akamai Advances Kona Site Defender to Meet the Challenges Posed by Constantly Evolving Web Application and DDoS Threat Landscape. URL: https://www.akamai.com/newsroom/press-release/kona-site-defender-for-evolving-web-application-and-ddos-threat-landscape (дата звернення: 09.11.2024).

12. Akamai App & API Protector: Maximize Security Through Simplicity. URL: https://www.akamai.com/blog/news/akamai-app-and-api-protector-maximize-security-through-simplicity (дата звернення: 09.11.2024).

13. Managed Kona Site Defender Service. URL: https://catalogartifact.azureedge.net/publicartifacts/akamai-technologies.managedksd-95f3427e-fa00-4507-affb-06b02a98c297/Artifacts/Documents/Managed_Kona_Site_Defender_Product_Brief.pdf (дата звернення: 22.11.2024).

14. StackHawk. Secure Your Web App: 10 Key Improvements. StackHawk. URL: https://www.stackhawk.com/blog/web-application-security-checklist-10-improvements/ (дата звернення: 26.11.2024).

15. Imaginovation. 10 Web Application Security Best Practices You Need to Know. Medium. URL: https://medium.com/@Imaginovation/10-web-application-security-best-practices-you-need-to-know-30a6e2fed1a2 (дата звернення: 01.12.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО -КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО -НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

Кваліфікаційна робота
на тему:

«Технологія захисту веб-додатків організації на базі рішення Akamai Kona Site Defender»

Виконав: БЄЛИХ Роман, БСДМ-63
Керівник: СОБЧУК Андрій, д.ф., доцент

Об'єкт дослідження – захист веб-додатків організації

Предмет дослідження – технологія захисту веб-додатків організації на базі рішення Akamai Kona Site Defender

Мета роботи – розробити порядок застосування технології захисту веб-додатків організації та рекомендації щодо її впровадження

Методи дослідження – аналіз наукової літератури, експлуатаційної документації, міжнародних стандартів у сфері кібербезпеки, а також їх порівняльний аналіз

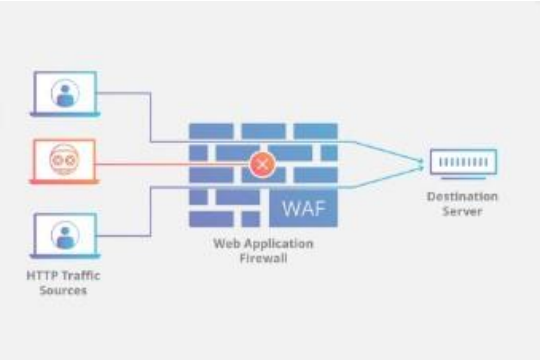
Наукові завдання:

- Дослідити сутність проблеми захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.
- Проаналізувати підходи до захисту веб-додатків організації за допомогою Akamai Kona Site Defender.
- Проаналізувати існуючі рішення із захисту веб-додатків організації на платформі Akamai Kona Site Defender.
- Проаналізувати методи та засоби захисту веб-додатків організації на базі рішення Akamai Kona Site Defender.
- Розкрити порядок реалізації технології захисту веб-додатків організації за допомогою Akamai Kona Site Defender.

Дослідження проблеми забезпечення захисту веб-додатків 3

Веб-додатки сьогодні є основними інструментами для взаємодії з клієнтами, партнерами та співробітниками. Однак вони також є ціллю для численних атак, таких як SQL-ін'єкції, XSS-атаки, DDoS-атаки тощо.
Компрометація веб-додатків може призводити до фінансових втрат, витоку конфіденційної інформації та зупинки бізнес-процесів. Вразливості часто виникають через недоліки в розробці або недостатній контроль безпеки.
Особливу увагу слід приділяти захисту даних та забезпеченню стабільної роботи додатків навіть у випадках активних атак.

Аналіз методів та засобів захисту веб-додатків організації 4



Сучасні методи захисту веб-додатків включають:
•WAF, які блокують SQL-ін'єкції, XSS-атаки та інші загрози.
•Захист від DDoS-атак, що забезпечує стабільність роботи веб-додатків навіть при перевантаженні мережі.
•Використання Content Security Policy (CSP) для обмеження джерел завантаження контенту.

Akamai Kona Site Defender поєднує всі ці функції, забезпечуючи комплексний підхід до кібербезпеки веб-додатків.

Призначення та основні функції рішення Akamai Kona Site Defender

5

Akamai Kona Site Defender є потужним інструментом для забезпечення безпеки веб-додатків. Його основне призначення — це захист від поширених кібератак, які спрямовані на порушення роботи веб-додатків або компрометацію конфіденційної інформації.
Система виконує функції WAF, блокуючи такі загрози, як SQL-ін'єкції, XSS та CSRF. Крім того, рішення інтегрується з мережею доставки контенту (CDN), що дозволяє ефективно відбивати DDoS-атаки, зберігаючи продуктивність веб-додатків навіть під час масових атак.

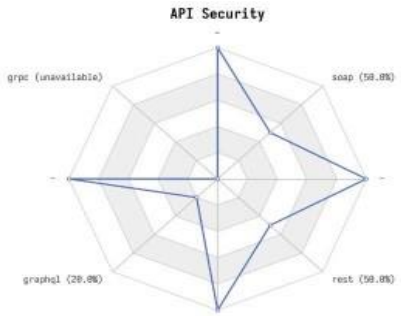
Також важливим компонентом є аналіз трафіку для виявлення ботів та автоматизованих загроз. Завдяки використанню сучасних алгоритмів система постійно оновлюється, забезпечуючи актуальність захисту перед новими типами атак.

Порівняння рішень Akamai Kona Site Defenderта Cloudflare WAF

6

Для оцінки ефективності рішення Akamai Kona Site Defender було проведено його порівняння з альтернативою — Cloudflare WAF.
Akamai Kona Site Defender продемонстрував високу ефективність у блокуванні складних атак, зокрема SQL-ін'єкцій і XSS, показавши результат 55,5/100 за тестовими метриками. Cloudflare WAF у цьому аспекті досяг оцінки 52,2/100.
Крім того, рішення Akamai виявилося надійнішим у захисті API.

Для REST API захист Kona Site Defender становив 100%, тоді як Cloudflare зазнав труднощів із обходами правил безпеки, що робить його менш придатним для сценаріїв, пов'язаних із високою динамікою API-запитів.
Важливо зазначити, що Akamai пропонує більше можливостей для інтеграції з корпоративними системами та хмарними сервісами завдяки гнучкій архітектурі та тісному зв'язку з CDN.



Type	True-negative tests blocked		True-positive tests passed		Grade
API Security	F	28.6%	N/A	0.0%	F	28.6%
Application Security	F	51.6%	A+	100.0%	C	75.8%

Технологія застосування рішення Akamai Kona Site Defender

7

Інтеграція Akamai Kona Site Defender у корпоративну інфраструктуру потребує кількох важливих етапів. Перш за все, необхідно встановити WAF, налаштувавши правила для моніторингу та блокування загроз.

Далі слід забезпечити інтеграцію з мережею доставки контенту, що дозволить ефективно розподіляти трафік і зменшувати ризик перевантаження серверів. Важливим аспектом є регулярне оновлення правил безпеки, адже нові загрози з'являються постійно, і лише адаптивна система може забезпечити їх блокування.

Рис. Стратегія захисту веб-додатків від Akamai

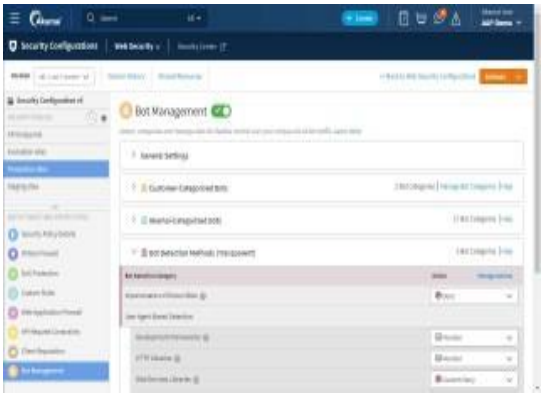
Останнім, але не менш важливим кроком є навчання персоналу. Спеціалісти з кібербезпеки повинні вміти працювати з системою, проводити аналіз трафіку та своєчасно реагувати на виявлені загрози.

Архітектура захисту з Akamai Kona Site Defender

8

Akamai Kona Site Defender побудований на багаторівневій архітектурі, яка забезпечує ефективний захист веб-додатків від різноманітних загроз. Одним із ключових елементів цієї архітектури є інтеграція з мережею доставки контенту (CDN). Це дозволяє розподіляти вхідний трафік між різними серверами, що зменшує ризик перевантаження системи навіть під час масштабних DDoS-атак.

На рівні додатків працює WAF, який аналізує всі вхідні запити, виявляє та блокує потенційно небезпечні дії. Система також включає модулі аналізу ботів, що дозволяє виявляти автоматизовані загрози та запобігати їх негативному впливу.



Ця багаторівнева архітектура забезпечує не лише високу ефективність захисту, але й адаптацію до нових типів атак, що постійно з'являються в кіберпросторі. Завдяки такій структурі, Akamai Kona Site Defender надає надійний захист, дозволяючи веб-додаткам функціонувати безперебійно навіть у складних умовах.

Рекомендації щодо захисту веб-додатків організації 9

Для забезпечення ефективного захисту веб-додатків рекомендується впроваджувати багаторівневий підхід до безпеки, який включає як технологічні рішення, так і організаційні заходи.
В першу чергу, варто використовувати сучасні інструменти, такі як WAF, для моніторингу трафіку, виявлення та блокування підозрілих запитів. Важливо забезпечити захист API, адже вони часто є точкою входу для зловмисників.
Щодо рішення Akamai Kona Site Defender, його інтеграція дозволяє знизити ризики атак. Для ефективного використання цього рішення слід налаштувати правила захисту з урахуванням специфіки веб-додатків організації, забезпечити інтеграцію з мережею доставки контенту для оптимального розподілу навантаження, а також регулярно оновлювати політики безпеки для адаптації до нових загроз.
Навчання персоналу також є ключовим елементом. Співробітники повинні мати навички роботи з системами моніторингута реагування на інциденти, щоб забезпечити швидке усунення потенційних загроз.

ВИСНОВКИ 10

Ефективний захист веб-додатків є ключовим елементом для забезпечення безпеки організаційних ресурсів. Аналіз основних загроз для веб-додатків, таких як DDoS-атаки, ін'єкції SQL, XSS, а також методи їх запобігання, дозволив виявити важливість комплексного підходу до забезпечення безпеки.
Одним із важливих елементів є правильна конфігурація та впровадження заходів безпеки на різних етапах розробки та експлуатації веб-додатків. Це включає використання механізмів автентифікації та авторизації, шифрування даних, регулярний моніторинг безпеки та своєчасне оновлення програмного забезпечення.
Особливу увагу було приділено використанню спеціалізованих рішень, таких як WAF, а також інтеграції з хмарними сервісами для забезпечення додаткового рівня захисту. Враховуючи швидкий розвиток технологій та появу нових загроз, постійний моніторинг та оновлення засобів захисту веб-додатків є необхідними для забезпечення належного рівня безпеки.
Akamai Kona Site Defender зарекомендував себе як потужне рішення для комплексного захисту веб-додатків. Його використання дозволяє не лише блокувати поширені атаки, але й забезпечувати стабільну роботу додатків навіть під час активних DDoS-атак. Порівняно з альтернативами, такими як Cloudflare WAF, Akamai демонструє вищу ефективність у захисті API та глибокий аналіз трафіку.
Застосування сучасних технологій, наявність навчання персоналу та створення ефективних процедур реагування на інциденти допомагають організаціям мінімізувати ризики і забезпечити безперебійну роботу веб-ресурсів.