УДК 004:42

РОЛЬ БРАНДМАУЕРІВ ВЕБ-ДОДАТКІВ У ЗАБЕЗПЕЧЕННІ РЕЗІЛЬЄНТНОСТІ МЕРЕЖІ.

Д.Ю. Лукашенко, науковий курівник, О. Є. Коваленко, професор, доктор технічних наук

Сучасний світ висуває високі вимоги до IT-інфраструктури та комп'ютерних мереж підприємств, що зумовлює їхню складність. Чим складніша структура й більша кількість елементів, що її формують, тим вищою стає ймовірність появи вразливих місць. Із бурхливим розвитком Інтернету все ширше застосовуються веб-додатки – саме через них здійснюється взаємодія з клієнтами, надається доступ до важливої інформації.

Відмова від використання веб-додатків є практично неможливою, адже в багатьох випадках це означало б втрату конкурентоспроможності або навіть функціональної спроможності організації. На фоні зростання популярності веб-сервісів зростає й кількість атак на них: понад 75% кіберзагроз спрямовані саме на вразливості веб-додатків [1, 2]. Наслідки таких атак можуть бути вкрай критичними – втрата особистих даних користувачів, зокрема платіжної інформації, витік конфіденційної або комерційної інформації, а також можливість використання веб-додатків як точки входу в корпоративну мережу.

Попри використання традиційних мережевих засобів захисту, таких як міжмережеві екрани нового покоління (Next Generation Firewall, NGFW) і системи запобігання вторгнень (Intrusion Prevention Systems, IPS), цих засобів недостатньо для захисту саме веб-додатків. Це зумовлено тим, що NGFW та IPS зосереджуються переважно на загрозах на мережевому та транспортному рівнях (L3-L4), тоді як веб-додатки працюють на прикладному рівні (L7).

Для підвищення резильєнтності мережі на прикладному рівні застосовується міжмережний екран веб-додатків (Web-Application Firewall, WAF) – спеціалізоване рішення, яке розгортається перед веб-додатками (зазвичай у режимі зворотного проксі) та аналізує двонаправлений HTTP/HTTPS-трафік. WAF здатний виявляти та блокувати спроби SQL-ін'єкцій, XSS-атак, «токсичні» cookie (cookie poisoning), обхідні шляхи (path traversal) тощо. Згідно з дослідженнями Gartner, WAF залишаються основним інструментом для захисту сучасних веб-додатків, і більшість великих організацій інтегрують його у свої архітектури.[2, 3].

WAF не є остаточним або самодостатнім рішенням безпеки. Його ефективність значно зростає в поєднанні з іншими засобами захисту, зокрема NGFW і IPS [1, 3]. Проте саме WAF забезпечує глибокий аналіз запитів на рівні HTTP/HTTPS, що є критично важливим для своєчасного реагування на загрози, які інші засоби можуть пропустити.

WAF-рішення поділяються на комерційні (Enterprise-level) та open-source. Серед комерційних рішень для захисту веб-додатків найпоширенішими є рішення від таких великих вендорів, як Imperva, Akamai, F5 та Fortinet. Вони пропонують повністю керовані рішення, які зазвичай включають у себе не тільки захист від типових веб-атак (SQL injection, XSS, CSRF), але й більш складні функції, зокрема: автоматичне оновлення правил та моніторинг безпеки в реальному часі, анаоіз трафіку за допомогою штучного інтелекту для виявлення нових вларзливостей, ітнеграція з іншими компонентами безпеки, такими, як системи запобігання вторгнень (IPS). Для прикладу, Imperva пропонує рішення, яке включає в себе як технології WAF, так і розширене захист від DDoS-атак, а також надає можливість використання кастомізованих правил для більш специфічних потреб [3]. У свою чергу, Akamai забезпечує місткісне масштабування та оптимізацію продуктивності, а також можливість використання різних рівнів захисту від атак — від базового фільтрування до глибокого аналізу за допомогою штучного інтелекту [2]. Недоліком таких рішень є висока вартість і необхідність в підготовці до

роботи з інтерфейсами складних корпоративних платформ. Водночас вони є чудовим вибором для великих компаній з високими вимогами до безпеки та стабільності роботи.

У той час як комерційні рішення забезпечують високу якість і підтримку, вони можуть бути дорогими для малих та середніх підприємств. Відкриті рішення, навпаки, є безкоштовними, а деякі з них забезпечують високий рівень кастомізації та масштабованості. Найбільш популярними open-source WAF є ModSecurity [4], open-appsec, Coraza та NAXSI.

Таблиця 1 – Порівняльна характеристика open-source WAF рішень:

Характеристика	ModSecurity	open-appsec	NAXSI	Coraza
Метод виявлення загроз	Сигнатурний (OWASP CRS)	Поведінковий аналіз (ШІ)	Whitlist + евристика	Сигнатурний (сумісний із ModSecurity)
Покриття загроз OWASP Top 10	Повне	Повне	Часткове	Повне
Ймовірність хибних спрацювань	Висока	Низька	Середня	Середня
Захист від атак нульового дня	Відсутній	Наявний	Відсутній	Відсутній
Можливість створення власних правил	Повна	Обмежена	Базова	Повна
Системи логування та моніторингу	Підтримується	Вбудоване логування	Базове логування	JSON-логування
Інтеграція з NGINX	Так	Так	Так	Так
Інтеграція з Apache/IIS	Так	Ні	Ні	Ні
Вплив на продуктивність	Середній/високий	Низький	Низький	Низький

Загалом, вибір WAF повинен ґрунтуватися не лише на технічних характеристиках, але й на контексті використання, розмірі компанії, технічному рівні персоналу та наявності ресурсів. В ідеалі, WAF слід розглядати як частину багаторівневої стратегії безпеки, що доповнює NGFW, IPS та інші засоби захисту, забезпечуючи стійкість мережі включно з прикладним рівнем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Why do I need a Web Application Firewall (WAF) to protect my website when I have a Next Generation Firewall (NGFW) already in place? [Електронний ресурс] – Режим доступу: https://www.linkedin.com/pulse/why-do-i-need-web-application-firewall-waf-protect-my-website - Дата звернення 06.04.2025

2. Gartner. Magic Quadrant for Web Application Firewalls [Електронний ресурс]. – 2023. – Режим доступу: https://www.gartner.com/en/documents/4004701 – Дата звернення: 06.04.2025.

3. Gartner. Magic Quadrant for Web Application Firewalls [Електронний ресурс]. – 2023. – Режим доступу: https://www.gartner.com/en/documents/3991674 – Дата звернення: 06.04.2025.

4. Trustwave. ModSecurity Reference Manual [Електронний ресурс]. – 2022. – Режим доступу: https://github.com/SpiderLabs/ModSecurity/wiki – Дата звернення: 06.04.2025.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ

ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
24 квітня 2025 року

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендєл

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.