КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1(13), 2021
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2021.13.8191
УДК 004.056:004.4

Лахно Валерій Анатолійович
д.т.н., професор, завідувач кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0001-9695-4543
valss21@ukr.net

Гусєв Борис Семенович
к.т.н., доцент, доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0003-1658-7822
gusevbs@nubip.edu.ua

Смолій Віктор Вікторович
к.т.н., доцент, доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0003-2834-6989
dr.v.smoliy@gmail.com

Блозва Андрій Ігорович
к.пед.н., доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

Касаткін Дмитро Юрійович
к.пед.н., доцент, доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-2642-8908
d.kasatkin@nubip.edu.ua

Осипова Тетяна Юріївна
к.пед.н., доцент кафедри комп'ютерних систем і мереж НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-9199-3436
t_osipova@nubip.edu.ua

WAF ЗАХИСТУ ВНУТРІШНІХ СЕРВІСІВ У СТРУКТУРІ ZERO TRUST

Анотація. Сучасний світ висуває високі вимоги до IT-інфраструктури та комп'ютерних мереж підприємств, що обумовлює складність їх структур. Чим складніша структура і кількість ланок, що входять до неї, тим вища імовірність появи вразливих місць. З бурхливим розвитком Інтернету широкого застосування набули веб–додатки. За їх допомогою відбувається взаємодія з клієнтами, надається доступ до важливої інформації. Відмовитися від веб-додатків дуже складно. Без них організація може втратити свою конкурентоспроможність або взагалі не зможе працювати. На фоні зростання популярності веб-додатків зростає і необхідність їх захисту від злому та несанкціонованого доступу, так як більше 75% атак хакерів спрямовані на вразливості веб-додатків та сайтів. Наслідки подібних зловмисних дій досить очевидні і не дуже приємні для компаній (в особливості їх клієнтів): втрата особистих даних, включаючи платіжну інформацію; можливість отримання доступу до комерційної таємниці та конфіденційних документів, крім того, вразливості веб-додатків можуть стати точкою входу зловмисників в корпоративну мережу. Традиційні методи мережевого захисту не запобігають атакам на веб-сервіси. Міжмережеві екрани орієнтовані на загрози мережевого і транспортного рівнів, в той час як веб-додатки працюють на прикладному рівні.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023

Брандмауер веб-додатків (Web Application Firewall) - тип брандмауеру, який застосовується для захисту веб-додатків. У той час, як прямий проксі-сервер захищає ідентифікацію клієнтського комп'ютера за допомогою посередника, WAF розгортається перед веб-додатками (в режимі зворотного проксі-серверу) і аналізує двонаправлений трафік HTTP/HTTPS, виявляючи шкідливий трафік та блокуючи його. WAF не є остаточним рішенням безпеки, скоріше вони призначені для використання в поєднанні з іншими рішеннями безпеки периметра мережі, такими як брандмауери нового покоління (NGFW) та системами запобігання вторгнень (IPS).

Ключові слова: безпека, брандмауери, OWASP, WAF.

ВСТУП

Сьогодні велика кількість людей користуються веб-додатками для пошуку потрібних продуктів і послуг. Клієнти надають свої імена, дані платіжних систем, що може стати золотою жилою для хакерів, які прагнуть заволодіти конфіденційною інформацією. При цьому захист веб-сайту також є питанням захисту фізичного обладнання. Хакери можуть не тільки вкрасти конфіденційну клієнтську інформацію, але й заразити сайт шкідливим ПО, що може вплинути на фізичне обладнання. Безпека веб-сайту має вирішальне значення для довговічності бізнесу, оскільки несанкціонований доступ досить сильно впливає на репутацію, призводить до простоїв і зниження продуктивності.

На сьогоднішній день питання безпеки веб-додатків дуже гостре, оскільки веб-додатки щільно інтегрувалися в сучасний світ. Визнаною світовою методологією оцінки вразливостей, що відображає сучасні тренди безпеки веб-додатків, є OWASP «Топ-10». У той час як глобальна політика безпеки веб-додатків повільно змінювалася в правильному напрямку за останні кілька років, 2020 рік і пандемія COVID-19 зупинили цей процес, а в деяких випадках, ситуація навіть погіршилася.

Постановка проблеми. Розглядається принцип побудови захисту веб-додатків у системі нульової довіри на базі брандмауера веб-додатків. Та його ефективність у захисті сервісів з використанням вільного ПО.

Основний матеріал статті.

Брандмауер веб-додатків (Web Application Firewall, WAF) – пристрій, який захищає веб-додатки від більшості існуючих на сьогоднішній день атак (в тому числі, від OWASP Top Ten) 10, 7.

WAF знаходиться між зовнішніми користувачами і веб-додатками, аналізує весь HTTP/HTTPS-трафік, виявляючи і блокуючи шкідливі запити до того, як вони зможуть вплинути на користувачів або на веб-додаток. В результаті WAF захищають критично важливі для бізнесу веб-додатки і веб-сервери від атак.

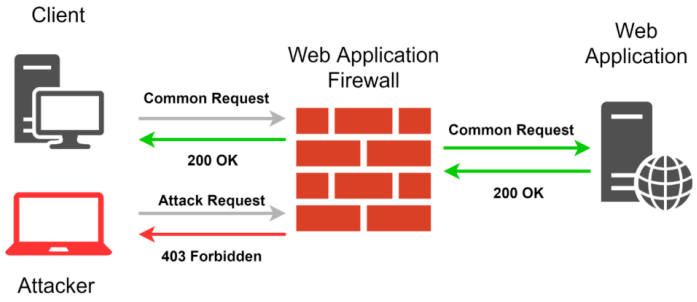

Рис.1. Схема роботи WAF

Традиційні мережеві брандмауери захищають локальну мережу від несанкціонованого доступу. Їх основна мета – відокремити захищену зону від менш безпечної і контролювати зв'язок між ними. Ключова технічна відмінність між брандмауерами рівня додатків і брандмауерами мережевого рівня – рівень, на якому вони працюють, що визначено моделлю взаємодії відкритих систем, яка характеризує і стандартизує функції зв'язку в телекомунікаційних і обчислювальних системах. WAF захищає від атак на 7 рівні моделі OSI–рівні додатків. Основними загрозами цього рівня є атаки на різного роду фреймворки, маніпуляція з файлами cookie, експлуатація SQL-ін'єкцій, атаки з використанням міжсайтових сценаріїв. Традиційні мережеві брандмауери працюють на рівнях 3 і 4 моделі OSI захищаючи мережевий трафік. З цієї причини, традиційний мережевий брандмауер сам по собі не захистить підприємства від атак на веб-сторінки 6.

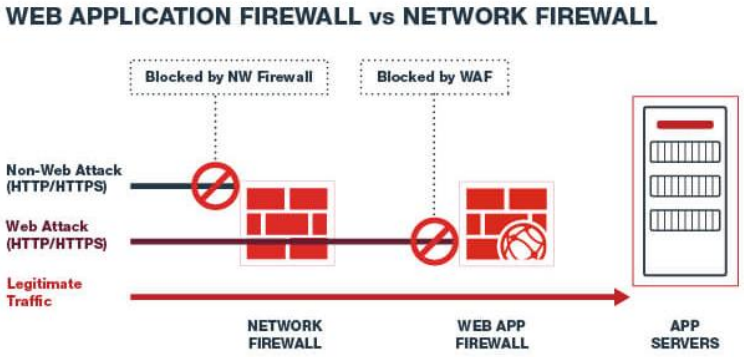

Рис.2. Порівняння традиційного брандмауеру з брандмауером веб-додатків в протидії веб-атакам

WAF працює на основі набору правил, що називаються політиками, які використовуються для фільтрації більшості відомих на сьогоднішній день атак. Багато служб WAF надають набір правил за замовчуванням, який періодично оновлюється.

WAF можуть працювати за моделлю негативної безпеки (чорний список), позитивної безпеки (білий список) або за гібридною моделлю. У моделі чорного списку використовуються попередньо встановлені сигнатури для блокування явно шкідливого веб-трафіку, а також сигнатури, призначенні для запобігання атакам, що використовують певні вразливості веб-сайтів і додатків. Наприклад, якщо кілька IP-адрес відправляють набагато більше пакетів, ніж типово, брандмауер, налаштований за чорним списком може запобігти DDOS-атаці.

Модель білого списку дозволяє веб-трафік, що відповідає спеціально налаштованим критеріям. Наприклад, брандмауер можна налаштувати так, щоб дозволяти запити HTTP GET тільки з певних IP-адрес. Брандмауери з моделлю білого списку найкраще підходять для веб-додатків у внутрішній мережі, які призначені для використання тільки обмеженою групою людей, наприклад співробітниками компанії 9.

WAF може бути реалізований одним з наступних способів, кожен з яких має свої переваги та недоліки:

- Мережевий WAF, як правило апаратний. Встановлюючись локально мінімізує затримку, але є більш дорогим варіантом;

- Хост-орієнтований WAF. Дешевше ніж мережевий WAF, пропонує більше можливостей для налаштування. Недоліком є споживання ресурсів локального серверу, складність реалізації та витрати на обслуговування;

- Хмарний WAF. Забезпечує найпростішу реалізацію, має мінімальну початкову вартість, пропонує рішення, яке постійно оновлюються для захисту від нових загроз без додаткові роботи або витрат з боку користувача. Недолік хмарного WAF полягає у віданні відповідальності третій стороні. Одним з найпопулярніших хмарних брандмауерів веб-додатків є Cloudflare WAF.

В даному проекті WAF реалізовується у хост-орієнтованому режимі на апаратній платформі Nano Pi R1 4.

Існує безліч безкоштовних WAF, які здатні захищати веб-додатки. Найбільша перевага WAF з відкритим вихідним кодом – вільна можливість змінювати код відповідно до вимог проектів. До найвідоміших WAF з відкритим вихідним кодом належать:

- ModSecurity. Оснащений безліччю функцій та пропонує повну свободу в розширенні можливостей. Серед основних можливостей даного брандмауера слід відмітити наступні: моніторинг безпеки додатків та контроль доступу в реальному часі, введення журналу HTTP-трафіку, постійна пасивна оцінка безпеки. Спільнота ModSecurity активно і постійно випускає оновлення.

- NAXSI. Абревіатура походить від Nginx Anti XSS & SQL Injection. Основне призначення даного брандмауера захист від SQL ін'єкцій та міжсайтовго скриптингу.

- WebKnight. Призначений для Microsoft IIS. Набір інструментів перевіряє всі запити і фільтрує їх у відповідності до політик, що встановлені адміністратором. Брандмауер направлений на запобігання атак переповнення буфера, SQL ін'єкцій, кодування символів 5.

WAF може інтегруватися в мережу наступними способами: режим мережевого моніторингу через SPAN порт, bridge mode, reverse proxy.

В режимі моніторингу пакети не проходять через брандмауер веб-додатків. Функція аналізатору комутованих портів (Switched Port Analyzer, SPAN) виконує пересилку копії трафіку, що надходить на якийсь порт, через інший порт цього ж комутатора. В такому режимі брандмауер виконує аналіз копії відстежуваного трафіку, а не пакетів, що пересилаються в дійсності. Перевага роботи в такому режимі в тому, що WAF не впливає на трафік, що дозволяє уникнути проблем з продуктивністю та затримками. Недоліком роботи в такому режимі є те, що WAF працює з копією трафіка і не може запобігати атакам на веб-додатки.

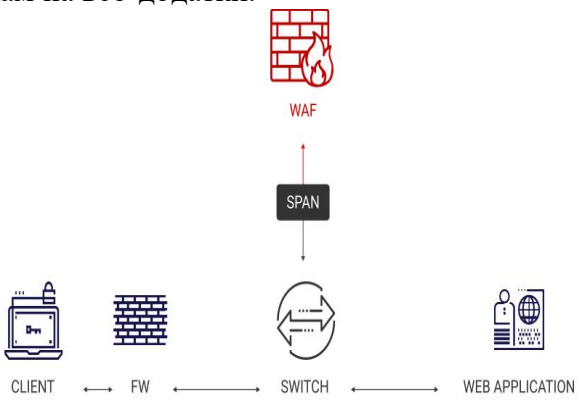

Рис.3. Приклад реалізації WAF в режимі моніторингу

ISSN 2663 - 4023

В режимі моста (bridge mode) WAF знаходиться на одній лінії між мережевим екраном і веб-серверами і діє як міст 2 рівня.

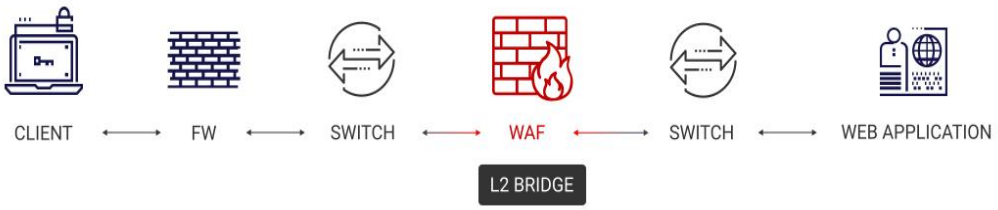

Рис. 4. Приклад реалізації WAF в режимі мосту

Зворотній проксі-сервер. Як правило, проксі-сервери виступають у ролі посередників при здійсненні онлайн-з'єднань. Проксі можуть ділитися на типи за різними критеріями. Тип проксі залежить від виду пристрою, який діє в якості проксі-серверу, рівня анонімності клієнта при використанні проксі, способу управління даними. Відповідно до ще одного критерію – розташування в структурі мережі, проксі-сервери діляться на зворотні і прямі.

Прямий проксі сервер – при використанні терміну «проксі», частіше за все мають на увазі саме прямий проксі сервер. Прямі проксі –типи проксі, які використовуються клієнтами для приховування своїх IP-адрес і збереження анонімності при роботі в Інтернеті. При використанні прямого проксі-серверу пристрій відправляє звичайний запит, ніби проксі-серверу і не існує, але всі запити до цільової системи будуть проходити через проксі-сервер. Проксі приймає запити і перенаправляє їх через свою IP-адресу, приховуючи справжню IP-адресу користувача. Найчастіше прямі проксі-сервери використовуються звичайними користувачами для обходу блокованих сервісів.

Зворотній проксі-сервер – приймає запити від імені веб-серверів. Зворотній проксі працює не для клієнтів, а для веб-серверів. Якщо прямий проксі-сервер призначений для забезпечення анонімності клієнтів, то зворотній проксі-сервер призначений для забезпечення анонімності веб-серверів. Вони приховують від клієнтів справжнє місцеположення серверів.

Зворотній проксі приймає запити з Інтернету і визначає, чи потрібно переадресовувати запит на реальний сервер 11.

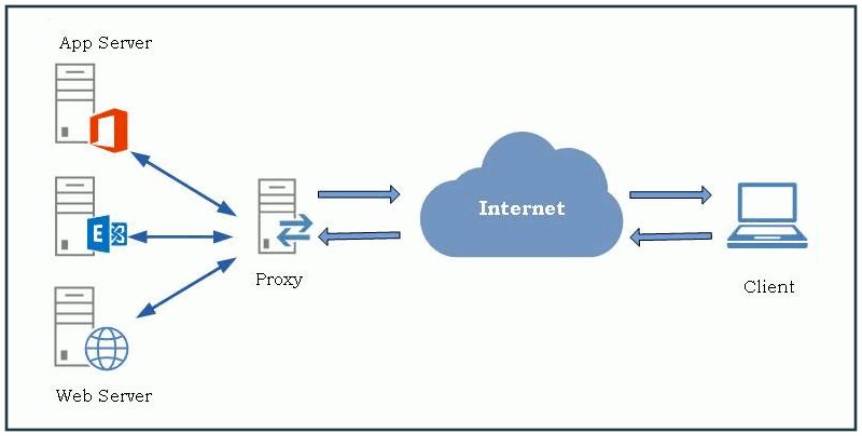

Рис.5. Приклад роботи зворотного проксі-серверу

ISSN 2663 - 4023

Зворотні проксі-сервери можуть використовуватися для:

- балансування навантаження. Зазвичай веб-сайти з великою кількістю щоденних користувачів не можуть обробляти весь трафік за допомогою одного вихідного серверу. Таким чином, зворотній проксі-сервер може рівномірно розподіляти навантаження між внутрішніми серверами;
- додаткова безпека внутрішніх серверів. Якщо веб-сервер використовує зворотній проксі, його адреса приховується, а користувачі можуть отримати доступ тільки до IP-адреси зворотного проксі. Це вводить додатковий елемент захисту. Наприклад, набагато складніше провести атаку типу «відмова в обслуговуванні»;
- кешування. Процес збереження копій файлів в кеші для більш швидкого повторного доступу. Кешування дозволяє веб-сайтам ефективно повторно використовувати раніше отримані дані. Це дозволяє веб-додаткам працювати більш ефективно;
- SSL-шифрування. Шифрування і дешифрування з'єднань для кожного користувача може виявитися неефективним для вихідного серверу. Зворотній проксі-сервер може виконувати цю роботу, шифруючи і дешифруючи всі запити 8.

Реалізація міжмережевого екрану в якості зворотного проксі-серверу є найбільш популярною та найбільш вживаною.

Рис.6. Реалізація WAF в якості зворотного проксі-серверу

Міжмережевий екран – пристрій, що забезпечує безпеку мереж шляхом моніторингу мережевого трафіку керуючись встановленими наборами правил безпеки. Брандмауер веб-додатків (Web Application Firewall, WAF) – пристрій, який захищає веб-додатки від більшості існуючих на сьогоднішній день атак (в тому числі, від OWASP Top Ten). WAF знаходиться між зовнішніми користувачами і веб-додатками і аналізує весь HTTP/HTTPS-трафік, виявляючи і блокуючи шкідливі запити до того, як вони зможуть вплинути на користувачів або на веб-додаток. Традиційні мережеві брандмауери працюють на рівнях 3 і 4 моделі OSI захищаючи мережевий трафік. З цієї причини, традиційний мережевий брандмауер сам по собі не захистить підприємства від атак на веб-сторінки. WAF захищає від атак на 7 рівні моделі OSI – рівні додатків. Основними загрозами цього рівня є атаки на різного роду фреймворки, маніпуляція з файлами cookie, експлуатація SQL-ін'єкцій, атаки з використанням міжсайтових сценаріїв. В результаті WAF захищають критично важливі для бізнесу веб-додатки і веб-сервери від атак. WAF працює на основі набору правил, що називаються політиками, які використовуються для фільтрації більшості відомих на сьогоднішній день атак. Багато служб WAF надають набір правил за замовчуванням, який періодично оновлюється. Найбільш часто застосовуваним методом реалізації WAF в мережі є реалізація в якості зворотного проксі-серверу.

ISSN 2663 - 4023

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Брандмауер веб-додатків (Web Application Firewall, WAF) – пристрій, який захищає веб-додатки від більшості існуючих на сьогоднішній день атак (в тому числі, від OWASP Top Ten). WAF знаходиться між зовнішніми користувачами і веб-додатками і аналізує весь HTTP/HTTPS-трафік виявляючи і блокуючи шкідливі запити до того, як вони зможуть вплинути на користувачів або на веб-додаток. В результаті WAF захищають критично важливі для бізнесу веб-додатки і веб-сервери від атак. WAF працює на основі набору правил, що називаються політиками, які використовуються для фільтрації більшості відомих на сьогоднішній день атак. Багато служб WAF надають набір правил за замовчуванням, який періодично оновлюється. Найбільш часто застосовуваним методом реалізації WAF в мережі є реалізація в якості зворотного проксі-серверу. Функції брандмауеру було покладено на програму ModSecurity. Для встановлення брандмауеру веб-додатків ModSecurity було виконано інсталяцію веб-серверу Apache та проведено його налаштування для подальшої роботи в режимі зворотного проксі-серверу. Для блокування атак на веб-сервер було завантажено найновішу на даний момент версію правил OWASP CRS завантажену з GitHub 3, 2, 1. Для захисту від атак типу «відмова в обслуговуванні», «розподілена відмова в обслуговуванні» (DoS, DdoS) та bruteforce атак було встановлено модуль mod_evasive. Основні налаштування даного модуля знаходяться в файлі /etc/apache2/mods-enabled/evasive.conf.

В якості тест-серверу було обрано WAMP-сервер зі встановленим Wordpress та налаштованою стандартною сторінкою. Для доступу використовується IP-адреса 192.168.1.44 без WAF, та 192.168.1.251 – через WAF.

1. OWASP ZAP

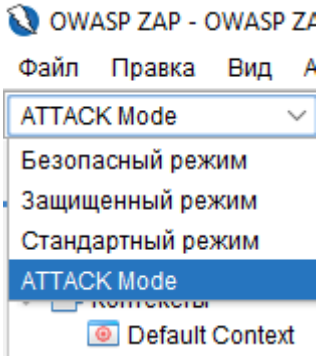

Рис.7. Вибір режиму сканування

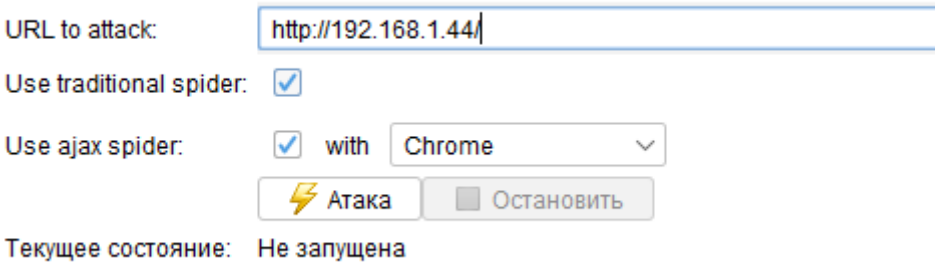

Рис.8. URL для сканування

ISSN 2663 - 4023

Після завершення сканування на вкладці «Сповіщення» можна переглянути результати. Оповіщення представлені 5 типами попереджень, серйозність яких відображається певним кольором прапорця.

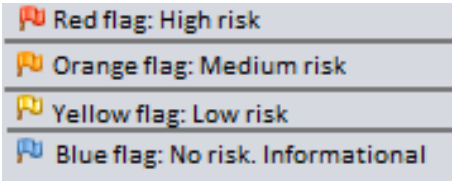

Рис.9. Серйозність оповіщень

Результати сканування веб-сторінки, яка не захищена WAF:

Рис.10. Тестування веб-сторінки, яка не захищена WAF

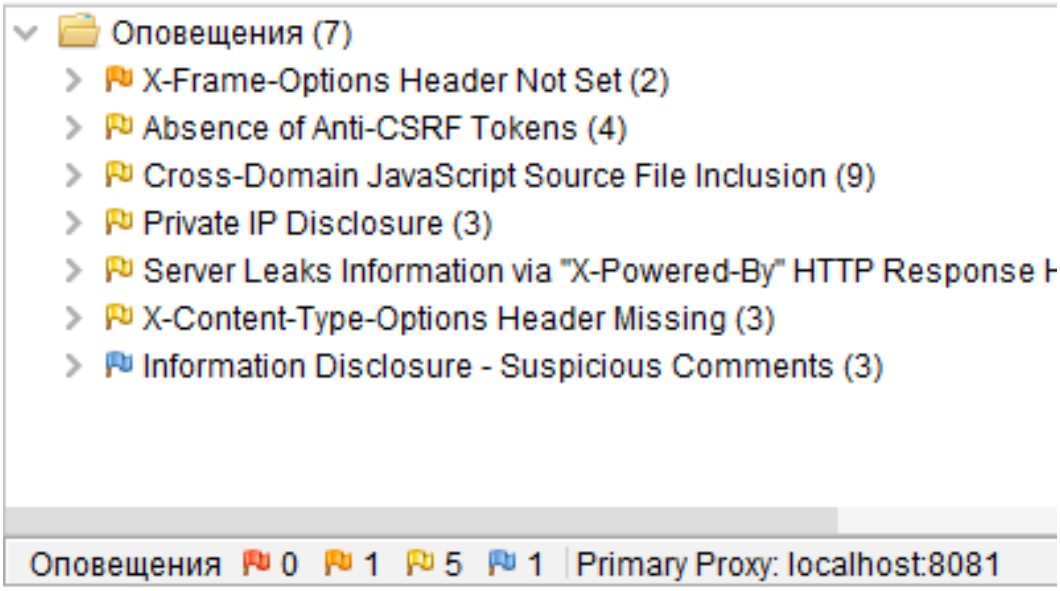

Рис. 11. Результат тестування сторінки, яка захищена WAF

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Тестування системи проводилося в два етапи: на першому етапі були використанні засоби автоматизації пошуку веб-вразливостей (сканери веб-вразливостей). При скануванні вразливого додатку через міжмережевий екран не було виявлено вразливостей високого рівня небезпеки. При цьому, спостерігається суттєве зменшення числа вразливостей середнього та низького рівнів небезпеки.

На другому етапі проводилося ручне тестування додатків на вразливості SQL-ін'єкції, міжсайтового скриптингу, атаки Path Traversal. При спробі провести атаку додатку, захищеного міжмережевим екраном - було отримано відповіді «403 Forbidden», що свідчить про неможливість проведення атак. Для фіксації атак на веб-севрер ModSecurity використовує два типи журналів: журнал помилок (error.log) та журнал аудиту modsec_audit.log. Журнал помилок створюється при виявленні помилки або при спробі провести атаку. Оскільки ModSecurity працює в парі з Apache всі журнали помилок (журнали помилок Apache+журнали помилок ModSecurity) створюються в одному файлі. Журнал аудиту починає заповнюватися після фіксації події в журналі помилок. В журналі аудиту записується більш детальна інформація про заблокавану атаку. Журнали аудиту ModSecurity створюються відповідно до унікальних ідентифікаторів журналу помилок.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 How to Secure Apache Web Server with ModEvasive on Ubuntu 16.04. https://www.alibabacloud.com/blog/how-to-secure-apache-web-server-with-modevasive-on-ubuntu-16-04_594051
2 How to Set Up ModSecurity with Apache on Debian/Ubuntu. https://www.linuxbabe.com/security/modsecurity-apache-debian-ubuntu
3 How To Use Apache as a Reverse Proxy with mod_proxy on Ubuntu 16.04. https://www.digitalocean.com/community/tutorials/how-to-use-apache-as-a-reverse-proxy-with-mod_proxy-on-ubuntu-16-04
4 NanoPI R1 – FriendlyARM Wiki. http://wiki.friendlyarm.com/wiki/index.php/NanoPi_R1
5 Open Source Web Application Firewall for Better Security. https://geekflare.com/open-source-web-application-firewall/
6 WAF vs. Firewall: Web Application & Network Firewalls. https://www.fortinet.com/resources/cyberglossary/waf-vs-firewall
7 Web Application Architecture: How the Web Works. https://www.altexsoft.com/blog/engineering/web-application-architecture-how-the-web-works/
8 What is a Reverse Proxy Server? https://oxylabs.io/blog/reverse-proxy
9 What is a web application firewalll (WAF)? https://cybersecurity.att.com/blogs/security-essentials/explain-how-a-web-application-firewall-works
10 What is Web Application Architecture? Components, Models, and Types. https://hackr.io/blog/web-application-architecture-definition-models-types-and-more.
11 Разница между обратным и прямым прокси. https://ip-calculator.ru/blog/ask/raznitsa-mezhdu-obratnym-i-pryamym-proksi/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023

Valerii A. Lakhno
Dr. Tech. Sc., Professor, Head of the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0001-9695-4543
valss21@ukr.net

Borys S. Husiev
Cand. Tech. Sc. (Ph.D), Docent, Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0003-1658-7822
gusevbs@nubip.edu.ua

Victor V. Smolii
Cand. Tech. Sc. (Ph.D), Docent, Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0003-2834-6989
dr.v.smoliy@gmail.com

Andrii I. Blozva
Cand. Pedag. Sc. (Ph.D.), Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

Dmytro Y. Kasatkin
Cand. Pedag. Sc. (Ph.D.), Docent, Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-2642-8908
d.kasatkin@nubip.edu.ua

Tetiana Y. Osypova
Cand. Pedag. Sc. (Ph.D), Associate Professor at the Department of Computer System and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-9199-3436
t_osipova@nubip.edu.ua

METHODS OF SYSTEM ANALYSIS IN THE FORMATION OF INFORMATION SECURITY POLICY ON TRANSPORT

Abstract. Approaches to the application of methods of system analysis to solve problems related to information security of enterprises in transport, which have a complex IT structure with a large number of components.

It is shown that the active expansion of the areas of informatization of the transport industry, especially in the segment of mobile, distributed and wireless technologies, is accompanied by the emergence of new threats to information security. It is shown that in order to build an effective information security system, the selection and implementation of adequate technical means of protection should be preceded by a stage of description, analysis and modeling of threats, vulnerabilities, followed by calculation of risks for IS and determining the optimal strategy for information security system. After evaluating the different NIB options according to several criteria, a decision is made: if the recommendations coincide, the optimal solution is chosen with greater confidence. If there is a contradiction of recommendations, the final decision is made taking into account its advantages and disadvantages, for example, the strategy of information security system development is chosen, which turned out to be optimal for at least two criteria. If different NIB development strategies are obtained for all three criteria, it is necessary to vary the values of pessimism-optimism in the Hurwitz criterion or change the data, for example, about possible threats to IP or automated enterprise management system.

An algorithm for modeling the decision-making process for selecting the optimal strategy for managing investment design components of the information security system for the transport business entity is proposed.

Keywords: informational security; methods of system analysis; criterion for evaluating the information security system.

REFERENCES

1 How to Secure Apache Web Server with ModEvasive on Ubuntu 16.04. https://www.alibabacloud.com/blog/how-to-secure-apache-web-server-with-modevasive-on-ubuntu-16-04_594051
2 How to Set Up ModSecurity with Apache on Debian/Ubuntu. https://www.linuxbabe.com/security/modsecurity-apache-debian-ubuntu
3 How To Use Apache as a Reverse Proxy with mod_proxy on Ubuntu 16.04. https://www.digitalocean.com/community/tutorials/how-to-use-apache-as-a-reverse-proxy-with-mod_proxy-on-ubuntu-16-04
4 NanoPI R1 – FriendlyARM Wiki. http://wiki.friendlyarm.com/wiki/index.php/NanoPi_R1
5 Open Source Web Application Firewall for Better Security. https://geekflare.com/open-source-web-application-firewall/
6 WAF vs. Firewall: Web Application & Network Firewalls. https://www.fortinet.com/resources/cyberglossary/waf-vs-firewall
7 Web Application Architecture: How the Web Works. https://www.altexsoft.com/blog/engineering/web-application-architecture-how-the-web-works/
8 What is a Reverse Proxy Server? https://oxylabs.io/blog/reverse-proxy
9 What is a web application firewalll (WAF)? https://cybersecurity.att.com/blogs/security-essentials/explain-how-a-web-application-firewall-works
10 What is Web Application Architecture? Components, Models, and Types. https://hackr.io/blog/web-application-architecture-definition-models-types-and-more.
11 Raznytsa mezhdu obratnым y priamым proksy. https://ip-calculator.ru/blog/ask/raznitsa-mezhdu-obratnym-i-pryamym-proksi/