ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ WEB-РЕСУРСІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Бойко А.О.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

РЕФЕРАТ

Текстова частина магістерської роботи: 62 сторінки, 11 рисунків, 1 таблиця, 15 джерел.

Об'єкт дослідження – процес забезпечення захисту Web-ресурсів інформаційної системи.

Предмет дослідження – технологія захисту Web-ресурсів інформаційної системи.

Мета роботи – розробити варіант системи захисту Web-ресурсів інформаційної системи та рекомендації щодо застосування технології в організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту Web-ресурсів інформаційної системи.

В роботі проведено аналіз проблеми забезпечення безпеки Web-ресурсів інформаційної системи та проаналізовано основні вразливості. Було проведено аналіз існуючих технологій забезпечення безпеки Web-ресурсів інформаційної системи.

Досліджено методи за засоби захисту Web-додатків на прикладі рішень Qualys Web Application Firewall та Qualys Web Application Scanning. Визначено основні характеристики, функції, можливості та принцип роботи Qualys WAF та Qualys WAS.

На основі проведених досліджень в роботі представлено варіант системи захисту Web-додатків інформаційної системи.

Галузь використання – кібербезпека корпоративної інформаційної системи.

ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, WEB-РЕСУРСИ, WEB-ДОДАТОК, WEB APPLICATION FIREWALL, SCANNING

ABSTRACT

Master’s thesis: 62 pages, 11 figures, 1 table, 15 sources.

The object of research is the process of ensuring the protection of Web resources of the information system.

The subject of research is the technology of protection of Web-resources of the information system.

The purpose of the work is to develop a variant of the system for the protection of Web-resources of the information system and recommendations for the use of technology in the organization.

Research methods – study of the literature on this topic, analysis of operating documentation, international standards and their comparison, modeling of the process of protecting Web resources of the information system.

The paper analyzes the problem of ensuring the security of Web resources of the information system and analyzes the main vulnerabilities. An analysis of existing technologies for ensuring the security of Web resources of the information system was carried out.

The methods for the protection of Web applications were studied using the Qualys Web Application Firewall and Qualys Web Application Scanning solutions as an example. The main characteristics, functions, capabilities and principle of operation of Qualys WAF and Qualys WAS are defined.

On the basis of the conducted research, the work presents a version of the protection system for Web-applications of the information system.

The field of use is cyber security of the corporate information system.

INFORMATION SYSTEM, CYBER SECURITY, WEB RESOURCES, WEB APPLICATION, WEB APPLICATION FIREWALL, SCANNING

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 5
ВСТУП 6
1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-СЕРВІСІВ 8
1.1 Основні характеристики, функції та архітектура web-сервісів 8
1.2 Аналіз проблеми захисту web-додатків 17
1.3 Аналіз основних загроз Web-додатків відповідно до OWASP Top-10 18
1.4 Аналіз існуючих технологій для забезпечення безпеки Web-додатків 26
2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВЕБ-ДОДАТКІВ НА БАЗІ РІШЕННЬ QUALYS 31
2.1 Аналіз основних функцій WAF 31
2.2 Призначення та властивості рішень щодо захисту веб-додатків від Qualys 33
2.3 Аналіз основних функцій та характеристика WAS від Qualys 35
2.4 Аналіз основних функцій та характеристик WAF від Qualys 37
2.5 Особливості роботи з Qualys Cloud Platform 40
3 ТЕХНОЛОГІЯ ЗАХИСТУ WEB-РЕСУРСІВ В КОРПОРАТИВНІЙ ІС НА БАЗІ QUALYS 43
3.1. Розроблення рекомендацій щодо застування технології WAF для захисту веб-ресурсів 43
3.2. Застування технології WAS для захисту веб-ресурсів 54
3.3. Рекомендації щодо захисту веб-додатків в інформаційній системі 63
ВИСНОВКИ 66
ПЕРЕЛІК ПОСИЛАНЬ 68
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 70

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

WAF — Web application firewall

WAS — Web Application Scanning

ІС — інформаційна система

HTTP — Hypertext Transfer Protocol

OWASP — The Open Web Application Security Project

ШПЗ — шкідливе програмне забезпечення

XSS — Cross-site scripting

PCI DSS — Payment Card Industry Data Security Standard

GDPR — General Data Protection Regulation

SOAP — Simple Object Access Protocol

REST — Representational state transfer

SQL — Structured Query Language

ВСТУП

Актуальність дослідження. Безпека веб-додатків відноситься до різноманітних процесів, технологій або методів захисту веб-серверів, веб-додатків і веб-служб, таких як API, від атак з боку Інтернет-загроз. Безпека веб-додатків має вирішальне значення для захисту даних, клієнтів і організацій від крадіжки даних, перерв у безперервності бізнесу чи інших шкідливих наслідків кіберзлочинності.

За більшістю оцінок, понад три чверті всіх кіберзлочинів спрямовані на програми та їх вразливі місця. Продукти та політики безпеки веб-програм спрямовані на захист програм за допомогою таких заходів, як брандмауери веб-програм (WAF), багатофакторна автентифікація (MFA) для користувачів, використання, захист і перевірка файлів cookie для підтримки стану користувача та статусу конфіденційності та різноманітні методи перевірки користувацьких даних, щоб переконатися, що вони не є зловмисними, перш ніж ці дані обробить програма.

Сучасний світ працює на додатках, від онлайн-банкінгу та програм для віддаленої роботи до доставки особистих розваг та електронної комерції. Не дивно, що програми є основною мішенню для зловмисників, які використовують такі вразливості, як недоліки в дизайні, а також слабкі місця в API, коді з відкритим кодом, віджетах сторонніх розробників і контролі доступу.

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження щодо технології захисту Web-ресурсів на прикладі Qualys WAF та WAS.

Об'єкт дослідження – процес забезпечення захисту Web-ресурсів інформаційної системи.

Предмет дослідження – технологія захисту Web-ресурсів інформаційної системи.

Мета роботи – розробити варіант системи захисту Web-ресурсів інформаційної системи та рекомендації щодо застосування технології в організації.

Наукові завдання:

дослідити сутність проблеми забезпечення захисту Web-ресурсів;

встановити сутність завдань захисту Web-ресурсів;

проаналізувати існуючі технології захисту Web-ресурсів;

проаналізувати методи та засоби забезпечення безпеки Web-ресурсів;

проаналізувати основні функції та принципи реалізації захисту Web-ресурсів.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту Web-ресурсів інформаційної системи.

Практичне значення одержаних результатів полягає в розробці варіанта захисту Web-ресурсів на базі рішення Qualys Web Application Firewall Qualys та Web Application Scanning, а також у розробці рекомендацій щодо застосування технології захисту Web-ресурсів в інформаційній системі.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-СЕРВІСІВ

1.1 Основні характеристики, функції та архітектура web-сервісів

Популярність Інтернет-ресурсів значно зросла за останні роки. Програми, засновані на веб-технологіях, стали потрібні у вирішенні завдань з різних галузей і поступово почали витісняти програми, засновані на інших технологіях.

Це призвело до ускладнення веб-додатків у плані структури, архітектури та реалізації, до того ж у веб-додатках почала використовуватися розподілена архітектура.

Таке ускладнення висунуло нові вимоги щодо безпеки веб-додатків. Відомо, що безпека — це ключовий момент розробки веб-додатку і розробники повинні приділяти достатньо уваги цьому питанню.

Якщо заходи безпеки будуть закладені в додаток на ранньому етапі розробки, це значно заощадить час і кошти, порівняно з варіантом, коли безпека буде додаватися в готовий або практично готовий додаток.

Питання безпеки та надійності є актуальними на всіх етапах розробки. І хоча з цього приводу було написано багато документів та статей, але мало що змінилося — програмісти продовжують писати програми, враховуючи питання безпеки не повною мірою.

Інтернет тепер є частиною життя кожної людини, а також основним засобом доступу до багатьох корисних послуг із суворими вимогами безпеки.

Внаслідок чого вразливість на веб-просторі може призвести до різних атак з катастрофічними наслідками: від економічних втрат, наприклад, у разі нападів на платіжні системи, такі як PayPal, і закінчуючи порушеннями конфіденційності, наприклад, у разі розкриття та підроблення електронних записів.

Через зростаючий споживчий попит розробка веб-додатків стає дедалі складнішою. Багато мов програмування поряд зі складною багаторівневою

архітектурою, що зазвичай бере участь у розробці веб-додатків, сприяють ймовірності помилок програмування.

Такі помилки можуть спричинити серйозні вразливості безпеки, які можуть бути використані зловмисниками.

Захист онлайн-сервісів - це досить трудомісткий процес з огляду на внутрішню складність Інтернету. Веб-екосистема є різнорідною і включає велику кількість різних компонентів і технологій, тому шляхи атаки на веб-додатки неймовірно великі, наприклад, до них можна віднести:

– недоліки безпеки у веб-браузері можуть розкривати дані автентифікації та конфіденційні дані, що зберігаються на сторінках;

– уразливості веб-протоколів можуть порушити захищеність та цілісність сеансу зв'язку;

– помилки в коді веб-програми можуть призвести до вбудовування шкідливого вмісту на веб-сторінки.

Навіть досвідченим веб-розробникам та фахівцям з безпеки важко стежити за всіма недоліками, що призводить до поширення порушень безпеки.

В останні кілька років багато дослідників безпеки запропонували наділити веб-платформу суворішими основами, що дозволяє точно міркувати про проблеми веб-безпеки.

Однак, враховуючи складність Інтернету, дослідницькі зусилля в даній сфері розкидані з різних тем і поки що досить важко зрозуміти суть офіційних методів веб-безпеки [1].

Веб-додаток - це клієнт-серверна програма, яка виконується на веб-платформі. Вона є невід'ємною частиною сучасної веб-екосистеми, що забезпечує динамічне надання інформації та послуг.

Як показано на рис. 1.1., веб-додаток складається з коду виконуваного як на стороні сервера, так і на стороні клієнта.

На стороні сервера, веб-додаток приймає вхідні дані від користувача через HTTP-запити та взаємодіє з локальною файловою системою, базою даних або іншими компонентами для доступу до даних та пошуку інформації.

Після цього сервер повертає вихідні дані (тобто згенеровані HTML-сторінки), які надсилаються клієнту через HTTP-відповіді. На стороні клієнта відображаються HTML-сторінки, а клієнтський код (тобто JavaScript), вбудований у відповіді HTTP, виконується веб-браузером.

Клієнтський код також може взаємодіяти з серверним кодом асинхронно, не заважаючи відображенню існуючої HTML-сторінки через AJAX та динамічно оновлювати сторінку. В даний час з метою сприяння швидкій розробці програм розробляються деякі бібліотеки та платформи програмування (наприклад, Ruby on Rails і Django). Наприклад, більшість платформ веб-розробки надають функції керування сеансами, які розробники можуть безпосередньо використовувати для керування веб-сеансами.

Модель виконання веб-додатків кардинально відрізняється від традиційних програм. Розробка веб-застосунків також стикається з труднощами, з якими не доводиться стикатися при розробці традиційних додатків.

По-перше, у відкритому веб-середовищі дані, що вводяться користувачем, потенційно небезпечні і ніколи не можна їм довіряти. Перевірка даних, що вводяться, є важливою частиною веб-програми для виявлення та очищення ненадійних даних, що вводяться користувачем. Хоча перевірка вхідних даних є важливою функцією, необхідною для всіх типів програм, її реалізація у веб-додатках є набагато складнішою через унікальні особливості технологій веб-розробки.

По-друге, зв'язок між клієнтом і веб-додатком здійснюється за допомогою протоколу HTTP. В результаті кілька вхідних даних від одного і того ж користувача будуть сприйматися як різні, незалежні користувачі веб-програми. Для корекції таких дій веб-програма має використовувати керування сеансами для зіставлення веб-запитів від одного користувача до веб-сеансу.

Оскільки результати обчислень клієнта ніколи не можуть бути довіреними, потрібна додаткова перевірка цих результатів на стороні сервера.

Ці унікальні можливості суттєво ускладнюють логічну реалізацію веб-програми, яка повинна забезпечувати керування потоком програми між клієнтом та сервером та між різними модулями.

Архітектура веб-програми описує розташування всіх компонентів веб-програми, а також акцентує взаємодію між різними компонентами програми, системами проміжного програмного забезпечення сторонніх виробників, веб-службами та базами даних. Так забезпечується моментальний знімок взаємодії між кількома програмами, що працюють разом для надання послуг кінцевим користувачам.

Різниця між архітектурою ПЗ та дизайном ПЗ

Архітектура програмного забезпечення включає всі високо рівневі компоненти системи та взаємодію всередині них.

Дизайн програмного забезпечення – це проектування на рівні коду, спрямоване на розподіл бізнес-логіки додатку за різними модулями зі своїми специфічними цілями. Він допомагає в побудові бізнес-логіки додатку та управлінні нею.

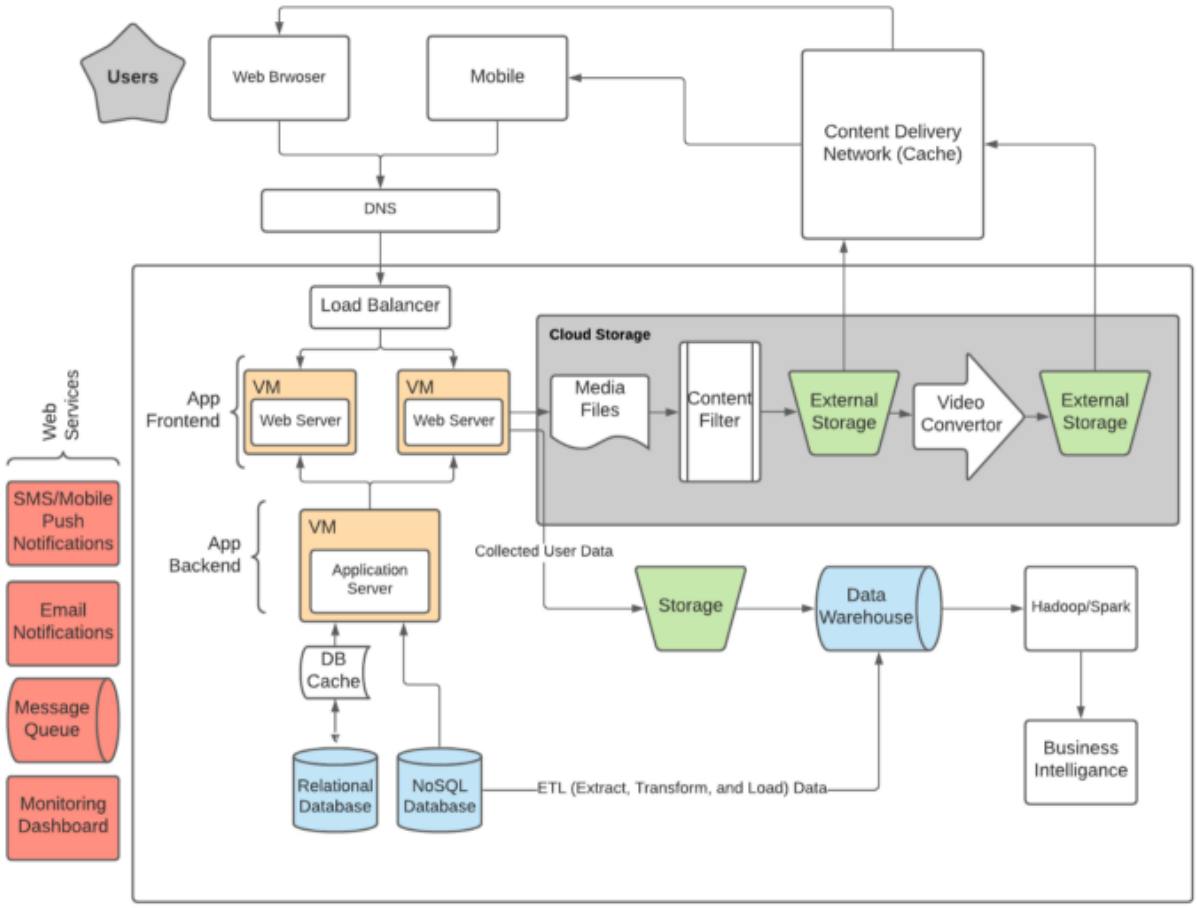

Рис. 1.1. Схема архітектури веб-додатку

Розглянемо основні поняття у цій схемі.

Користувач-агенти

Агенти користувача (користувач-агенти) - це в першу чергу інструменти, які допомагають користувачам взаємодіяти з сервером. Користувач переважно взаємодіє з сервером через веб-браузери - Google Chrome, Firefox, Microsoft Edge, Safari - або мобільні програми на платформах Android та IOS. Агент відправляє запит на сервер і отримує відповідь, яка потім показується користувачеві.

DNS

Сервери доменних імен – це щось на зразок адресної книги для веб-сайтів. Щоразу, коли користувач надсилає запит на веб-адресу за допомогою браузера, браузер використовує DNS, щоб знайти реальну адресу веб-сервера (IP-адреса). Браузеру необхідно з'ясувати, на якому сервері знаходиться веб-сайт, щоб він міг відправляти запити HTTP туди, куди потрібно.

Балансувальник навантаження

Балансувальник навантаження насамперед займається горизонтальним масштабуванням. Він надсилає вхідні запити на один із декількох серверів, а потім надсилає користувачеві відповідь, яку отримує від цих серверів. Зазвичай сервери веб-додатків існують у вигляді кількох копій, що дзеркально відображають один одного, щоб забезпечити узгодженість та доступність. Балансувальник навантаження розподіляє завдання між ними. Він добре працює у тандемі з автоматичним масштабуванням серверів.

Віртуальна машина

В обчислювальній техніці віртуальна машина (VM) – це віртуалізація/емуляція комп'ютерної системи. Віртуальні машини засновані на комп'ютерних архітектурах та забезпечують функціональність, аналогічну фізичному комп'ютеру. Їх реалізація може містити спеціалізоване апаратне забезпечення, програмне забезпечення або їх комбінацію.

Веб-сервер

Веб-сервер обробляє запит користувача і надсилає відповідь, що містить дані (HTML, JSON, XML і т.д.) у браузер. Веб-сервери, розміщені на віртуальній машині, використовують обчислювальні потужності, що надаються віртуальними машинами для виконання своїх завдань. Веб-сервер зазвичай відноситься до внутрішніх інфраструктур, таких як база даних, сервер кешу, черга завдань та інші.

Бази даних

База даних надає інструменти для організації, додавання, пошуку, оновлення, видалення та виконання обчислень з даними. Як правило, існують реляційні бази даних - MySQL, PostgreSQL, Microsoft SQL Server, Oracle Database, Microsoft Access і т.д., а також нереляційні бази даних - MongoDB, Dynamo DB та інші.

Служба кешування

Служба кешування забезпечує збереження даних, що дозволяє зберігати та шукати дані. Кешування дозволяє посилатися на попередній результат, щоб значно прискорити обчислення. Кеші застосовуються на різних технологічних рівнях,

включаючи операційні системи, та в мережах, включаючи мережі доставки контенту (Content Delivery Network, CDN) та DNS, веб-додатки та бази даних.

На стороні клієнта - Заголовки HTTP-кешу, браузери; DNS - DNS-сервери;

Web – заголовки HTTP-кешу, CDN, зворотні проксі, веб-прискорювачі, сховища ключів/значень;

Програми - сховища ключів / значень, локальні кеші;

Бази даних - кеш бази даних, буфери, сховища даних ключів / значень.

Мережа доставки контенту

Мережа доставки контенту, або мережа поширення контенту (CDN), є географічно розподіленою мережею проксі-серверів і пов'язаних з ними центрів обробки даних. Мета полягає в тому, щоб забезпечити високу доступність та продуктивність за рахунок просторового розподілу сервісу щодо кінцевих користувачів. CDN обслуговують більшу частину інтернет-контенту, включаючи веб-об'єкти (текст, графіку та скрипти), завантажувані об'єкти (медіафайли, програмне забезпечення, документи), додатки (електронна комерція, портали), потокові медіа у прямому ефірі, потокові медіа за запитом та сайти соціальних мереж.

Зовнішнє сховище

Зовнішні сховища використовуються для зберігання ресурсів, включаючи зображення, відео, документи та інші великі файли. У багатьох випадках із цими файлами також виконуються операції. Приклад — Youtube автоматично конвертує відео, завантажені користувачами, у кількох роздільних розширеннях. Facebook перетворює зображення та відео користувачів у формат, зручний для мобільних пристроїв. Оскільки зберігання цих даних на локальному диску віртуальної машини є дорогим і споживає великі обчислювальні ресурси, вони зазвичай зберігаються в зовнішньому сховищі. Хмарне сховище – один із найпопулярніших варіантів.

Хмарне сховище — це модель хмарних обчислень, яка зберігає дані в Інтернеті через постачальника хмарних обчислень, який керує сховищем даних як послугою. Сховище поставляється на вимогу з максимальною пропускною

спроможністю та витратами, а також унеможливлює купівлю власної інфраструктури зберігання даних та управління нею.

Веб-служби

Веб-служби надають загальну платформу, яка дозволяє кільком додаткам, побудованим різними мовами програмування, мати можливість взаємодіяти один з одним.

Веб-служби використовують SOAP (Simple Object Access Protocol, Протокол простого доступу до об'єктів) для надсилання даних XML між додатками. Дані надсилаються за запитом HTTP. Дані, які надсилаються з веб-служби до програми, називаються SOAP-повідомленням. Повідомлення SOAP - це не що інше, як XML-документ. Оскільки документ написаний мовою XML, клієнтська програма, що викликає веб-службу, може бути написана будь-якою мовою програмування.

Існує два основних типи веб-сервісів:

1. Простий протокол доступу до об'єктів або веб-служби SOAP.
2. Надсилання репрезентативного стану або веб-служби REST.

Сховище даних

Сховище даних - це система, що використовується для складання звітів та аналізу даних, і вважається основним компонентом бізнес-аналітики. Кожен сучасний додаток збирає, зберігає та аналізує дані. Сховища даних — це центральні сховища інтегрованих даних із одного або кількох розрізнених джерел. Вони зберігають поточні та історичні дані в одному місці, яке використовується для виконання бізнес-аналітики та створення звітів для підприємства.

Два основні підходи до побудови системи сховища даних – це вилучення, перетворення, завантаження (ETL - Extract, Transform, Load) та вилучення, завантаження, перетворення (ELT).

ETL - Extract, Transform, Load:

Вилучення - вилучення даних із кількох джерел.

Перетворення - перетворення даних, включаючи очищення, поділ та категоризацію.

Завантаження - завантаження даних у сховище.

Моделі компонентів веб-застосунків

Існує лише три моделі компонентів веб-програми. Це тісно пов'язане з кількістю служб і баз даних, які використовуються для веб-застосунків.

Один веб-сервер, одна база даних;

Декілька веб-серверів, одна база даних;

Декілька веб-серверів, кілька баз даних;

Сервіси програм.

Три так звані монолітні моделі такі завдяки жорсткій та стабільній природі їхнього сервера. Навпаки, сервіси додатків (мікросервіси та безсерверні), як правило, гнучкі, оскільки вони спрощують оновлення та масштабування. Застосування цієї моделі дозволяє розділити веб-сервери на дрібніші частини: сервіси в мікросервісах та функції безсерверних. Таким чином, стає простіше незалежно змінювати та масштабувати будь-яку з цих складових.

Найкращі практики в галузі архітектури веб-додатків

Основні критерії побудови надійної архітектури програми:

- Ефективність;
- Гнучкість;
- багаторазовість;
- Легкість у тестуванні;
- Послідовність та успішність у вирішенні завдань;
- Добре структурований та зрозумілий код;
- Масштабованість у процесі розробки;
- Швидкий час відгуку;
- відсутність падінь;
- Немає єдиної точки відмови;
- Простота;
- Опора на випробувані стандарти безпеки [2].

1.2 Аналіз проблеми захисту web-додатків

Безпека веб-додатків — це процес захисту веб-сайтів та онлайн-сервісів від різних загроз безпеці, що використовують вразливість у коді програми. Найпоширенішими цілями для атак на веб-додатки є системи керування контентом (наприклад, WordPress), інструменти адміністрування баз даних (наприклад, phpMyAdmin) та програми SaaS.

Злочинці вважають веб-додатки високо пріоритетними цілями через:

– Притаманну їх вихідному коду складність, яка збільшує ймовірність некерованих уразливостей та шкідливих маніпуляцій із кодом.

– Висока винагорода, зокрема конфіденційні особисті дані, зібрані в результаті успішних маніпуляцій з вихідним кодом.

– Простота виконання, оскільки більшість атак можна легко автоматизувати та запускати без розбору проти тисяч, а то й десятків чи сотень тисяч цілей одночасно.

Організації, не здатні захистити свої веб-додатки, ризикують зазнати атаки. Серед інших наслідків це може призвести до крадіжки інформації, порушення відносин з клієнтами, відкликання ліцензій та судових розглядів [3].

Веб-програми повинні вільно пропускати трафік через різні порти і зазвичай вимагають автентифікації; це означає, що їм також потрібний комплексний сканер уразливостей веб-застосунків. Оскільки веб-сайти повинні дозволяти вхідний і вихідний трафік в мережі, хакери часто атакують порти, що найчастіше використовуються. Це включає:

Порт 80 (HTTP): для незахищеного веб-сайту.

Порт 443 (HTTPS): для захищеного веб-сайту.

Порт 21 (FTP): протокол передачі файлів для передачі файлів на ваші сервери та з них.

Порти 25 (SMTP) для простого протоколу передачі пошти та порт 110 (POP3), незашифрований порт за замовчуванням: протоколи електронної пошти, які часто використовуються організаціями для надсилання та отримання електронної пошти.

Враховуючи широту доступних портів, не дивно, що хакери мають безліч можливостей зламати мережі, використовуючи відкритість, яку повинні мати веб-сайти для взаємодії зі своїми користувачами [4].

1.3 Аналіз основних загроз Web-додатків відповідно до OWASP Top-10

Вразливості веб-застосунків, як правило, є результатом відсутності обробки вводу/виводу, яка часто використовується або для маніпулювання вихідним кодом, або для отримання несанкціонованого доступу.

Open Web Application Security Project (OWASP) – це некомерційна організація, яка займається підвищенням безпеки програмного забезпечення. Вона працює за моделлю «відкритої спільноти», що означає, що будь-хто може брати участь і робити свій внесок в онлайн-чати, проекти та багато іншого, пов'язані з OWASP. Для всього, від онлайн-інструментів та відео до форумів та заходів, OWASP гарантує, що пропозиції залишаються безкоштовними та легко доступними через веб-сайт.

OWASP Top-10 містить ранжування та рекомендації щодо усунення 10 найбільш важливих загроз безпеці веб-додатків. Використовуючи великі знання та досвід учасників відкритої спільноти OWASP, звіт заснований на консенсусі серед експертів з безпеки з усього світу. Ризики ранжуються відповідно до частоти виявлених дефектів безпеки, серйозності виявлених вразливостей та величини їх потенційного впливу. Мета звіту – запропонувати розробникам та фахівцям з безпеки веб-додатків інформацію про найбільш поширені загрози безпеці, щоб вони могли використовувати висновки та рекомендації звіту у своїх власних методах забезпечення безпеки, зводячи до мінімуму наявність відомих ризиків у своїх додатках [5].

Останній список 10 основних вразливостей та загроз безпеки веб-застосунків OWASP

Оновлений OWASP Топ 10 список вийшов 24 вересня 2021 на 20-річчя OWASP.

OWASP Топ-10 вразливостей

1. Зламаний контроль доступу
2. Криптографічні збої
3. Ін'єкції
4. Небезпечний дизайн
5. Неправильна конфігурація безпеки
6. Вразливі та застарілі компоненти
7. Помилки ідентифікації та аутентифікації
8. Збої цілісності програмного забезпечення та даних
9. Реєстрація безпеки та моніторинг збоїв
10. Підробка запитів на стороні сервера

1. Порушений контроль доступу

Елементи управління безпекою доступу до веб-сайту повинні обмежувати доступ відвідувачів лише до тих сторінок або розділів, які потрібні даному типу користувачів. Наприклад, адміністратори сайту електронної комерції повинні мати можливість додавати нові посилання чи рекламні акції. Ці функції не повинні бути доступними для інших типів відвідувачів.

Розробників слід заохочувати до впровадження дисципліни «безпека насамперед», щоб уникнути пасток, таких як системи управління контентом (CMS), які за замовчуванням генерують дозвіл на повний доступ (аж до доступу на рівні адміністратора). Порушений контроль доступу може дати відвідувачам веб-сайту доступ до панелей адміністратора, серверів, баз даних та інших критично важливих для бізнесу програм. Фактично, ця загроза OWASP Top 10 навіть може використовуватися для перенаправлення браузерів на інші цільові URL-адреси.

Вразливість порушеного контролю доступу може бути усунена кількома способами:

Використовуйте найменш привілейований підхід, щоб кожній ролі було надано найнижчий рівень доступу, необхідний виконання її задач.

Видаліть облікові записи, які більше не потрібні або активні.

Аудит активності на серверах та веб-сайтах, щоб знати, хто що робить (і коли).

Якщо точок доступу кілька, вимкніть непотрібні на даний момент.

Забезпечте економічність серверів, вимкнувши непотрібні служби.

2. Криптографічні помилки

Дані в дорозі та стані спокою, такі як паролі, номери кредитних карток, медичні записи, особиста інформація та комерційна таємниця, вимагають додаткового захисту через можливість криптографічних збоїв (розкриття конфіденційних даних). Це особливо важливо, якщо дані підпадають під дію будь-якого закону про конфіденційність, таких як GDPR, CCPA та інші.

Усунення криптографічних збоїв

У формах, які збирають дані, вимкніть автозаповнення.

Зменшіть/мінімізуйте розмір області поверхні даних.

Шифруйте дані, коли вони перебувають у дорозі та у стані спокою.

Використовуйте найсучасніші методи шифрування.

Вимкнути кешування форм збору даних.

Використовуйте сильні адаптивні та солоні функції хешування під час збереження паролів.

3. Ін’єкції

Вразливості застосування можуть виникати, коли запит або команда використовуються для вставки ненадійних даних в інтерпретатор через SQL, ОС, NoSQL або використання LDAP. Ворожі дані, введені через цей вектор атаки, обманюють інтерпретатор, змушуючи програму робити те, для чого вона не призначена, наприклад, генерувати ненавмисні команди або отримувати доступ до даних без належної аутентифікації.

Будь-який додаток, який приймає параметри як вхідні дані, може бути підданий атакам шляхом впровадження. Рівень загрози тісно пов'язаний із ретельністю заходів перевірки вхідних даних програми.

Ін'єкційні атаки можна запобігти будь-якій комбінації наступних підходів:

Відокремлюйте команди від даних, щоб уникнути атак, які замінюють дані ненавмисним виконанням команд.

Кодуйте запити SQL з параметрами, а не структуруйте команду лише з вмісту, введеного користувачем. Вони називаються параметризованими запитами чи підготовленими операторами.

Повністю усуньте інтерпретатор за рахунок використання безпечного API.

Впровадьте позитивну перевірку на стороні сервера, а також систему виявлення вторгнень, яка виявляє підозрілу поведінку на стороні клієнта.

4. Небезпечний дизайн

Небезпечний дизайн - це широкий термін, який охоплює безліч недоліків і визначається як "відсутній або поганий дизайн управління". Моделювання загроз, безпечні шаблони проектування та еталонні архітектури входять до нових категорій на 2021 рік, що потребує більш широкого використання моделювання загроз, безпечних шаблонів проектування та еталонних архітектур.

Виправлення небезпечного дизайну

Щоб допомогти проаналізувати та розробити заходи, пов'язані з безпекою та конфіденційністю, створіть та використовуйте безпечний життєвий цикл розробки разом із спеціалістами AppSec.

Створіть та використовуйте бібліотеку безпечних шаблонів проектування або компонентів, які готові до використання.

Використовуйте моделювання загроз для важливої автентифікації, контролю доступу, бізнес-логіки та ключових потоків.

Історії користувача повинні включати мову безпеки та елементи керування.

Інтегруйте перевірки правдоподібності у програму на кожному рівні (від інтерфейсу до сервера).

Щоб переконатися, що всі важливі потоки є стійкими до моделі загроз, напишіть модульні та інтеграційні тести. Складіть список варіантів використання та випадків неправильного використання для кожного рівня вашої програми.

Залежно від вимог до експозиції та захисту розділіть рівні на системний та мережевий рівні.

Обмежте споживання ресурсів користувачами та службами.

5. Неправильне налаштування безпеки

За оцінками Gartner, до 95% порушення безпеки хмари є результатом людських помилок. Неправильні параметри безпеки є одним з основних факторів, що впливають на цю статистику, і OWASP зазначає, що з першої десятки ця вразливість є найбільш поширеною. Існує багато типів неправильної конфігурації, які наражають компанію на ризик кібербезпеки, в тому числі:

– Прийняття небезпечних налаштувань за умовчанням
– Надмірно доступні ресурси хмарного сховища
– Неповні конфігурації
– Неправильно настроєні заголовки HTTP
– Детальні повідомлення про помилки, що містять конфіденційну інформацію
– Виправлення неправильної конфігурації безпеки

Неправильні налаштування безпеки можуть виникнути практично в будь-якому місці середовища, включаючи підключені до мережі пристрої, бази даних, веб-сервери та сервери програм, а також контейнери. Наступні методи можуть допомогти підтримувати добре налаштоване середовище:

Використовуйте шаблони для розгортання середовищ розробки, тестування та виробництва, які попередньо налаштовані відповідно до політик безпеки організації.

Використовуйте сегментовані архітектури програм, які зводять до мінімуму ризик небезпечно налаштованого елемента; підтримувати бібліотеку правильно налаштованих образів контейнерів.

Розгорніть мінімальні платформи та видаліть функції та служби, які не використовуються.

Безперервно відстежуйте хмарні ресурси, програми та сервери на наявність неправильних налаштувань безпеки та усувайте виявлені проблеми в режимі реального часу, по можливості використовуючи автоматизовані робочі процеси.

6. Уразливі та застарілі компоненти

Сучасні розподілені веб-програми часто включають компоненти з відкритим вихідним кодом, такі як бібліотеки та фреймворки. Будь-який компонент з відомою вразливістю стає слабкою ланкою, яка може вплинути на безпеку всієї програми.

Хоча використання компонентів з відкритим вихідним кодом з відомими вразливістю посідає низьке місце з погляду серйозності проблеми безпеки, воно посідає перше місце у рейтингу OWASP Top 10 як часто вразливість була основною причиною фактичного порушення даних.

Виправлення вразливих та застарілих компонентів

Найефективніший захист – безперервне сканування всіх компонентів коду на наявність відомих уразливостей та розгортання виправлення або іншого засобу захисту при виявленні вразливості. Існує низка передових практик, що підвищують ефективність цієї лінії захисту:

Усі компоненти, інтегровані у фреймворки компанії, повинні бути під управлінням конфігурацією.

Сканер повинен мати можливість автоматично виявляти всі компоненти моніторингу.

Сканування має проводитися на тлі комплексної бази даних уразливостей в якій зібрані дані про загрози.

Робочі процеси управління виправленнями для визначення, тестування та розгортання потрібного виправлення повинні бути максимально автоматизовані, щоб мінімізувати операційний ризик, пов'язаний із встановленням виправлень.

7. Помилки ідентифікації та аутентифікації

Коли програми неправильно виконують функції, пов'язані з керуванням сеансом або автентифікацією користувачів, зловмисники можуть отримати можливість скомпрометувати паролі, ключі безпеки або токени сеансу і назавжди або тимчасово привласнити посвідчення та дозволи інших користувачів. Ця вразливість є серйозною загрозою безпеці програми та ресурсів, до яких вона звертається, а також може поставити під загрозу інші активи, підключені до тієї ж мережі.

Виправлення автентифікації

Основні рекомендації OWASP щодо усунення вразливостей непрацюючої аутентифікації:

Використовувати багатофакторну автентифікацію.

Не розгортайте облікові дані за замовчуванням, особливо для користувачів з правами адміністратора.

Використовуйте надійні паролі.

Уважно відстежуйте невдалі спроби входу до системи.

Використовуйте безпечний менеджер сеансів, який створює випадкові ідентифікатори сеансів з обмеженням часу. Ніколи не вмикайте ідентифікатори сеансів у URL-адресу.

8. Програмне забезпечення і помилки цілісності даних

Код та інфраструктура, які не захищають від порушень цілісності, називаються збоями цілісності програмного забезпечення та даних. Прикладом цього є програма, яка використовує плагіни, бібліотеки чи модулі з ненадійних джерел, репозиторіїв чи мереж доставки контенту (CDN). Несанкціонований доступ, шкідливий код або компрометація системи може бути ризиком незахищеного конвеєра CI/CD. Нарешті, багато програм тепер мають можливості автоматичного оновлення, які дозволяють отримувати оновлення без необхідних перевірок цілісності та застосовувати їх до довірених додатків. Зловмисники потенційно можуть поширювати та запускати свої власні оновлення у всіх системах із цією функціональністю.

Усунення збоїв програмного забезпечення та цілісності даних

Використовуйте цифрові підписи або інші подібні заходи, щоб гарантувати, що програма або дані є справжніми та не підроблені.

Щоб знизити ризик впровадження шкідливого коду або конфігурації у конвеєр розробки, переконайтеся, що існує процедура перевірки коду та модифікацій конфігурації.

Переконайтеся, що бібліотеки та залежності, такі як npm або Maven, використовують довірені репозиторії. Розгляньте можливість розміщення

внутрішнього затвердженого наперед справного репозиторію, якщо у вас більш високий профіль ризику.

Щоб захистити цілісність коду, що проходить через процеси складання та розгортання, переконайтеся, що ваш конвеєр CI/CD включає належний поділ, налаштування та контроль доступу.

Переконайтеся, що непідписані або незашифровані серіалізовані дані не будуть доставлені ненадійним клієнтам без будь-якої перевірки цілісності або цифрового підпису для виявлення зміни або відтворення.

9. Недостатня реєстрація і моніторинг

Дослідження показують, що час від атаки до виявлення може тривати до 200 днів, а часто й довше. Це вікно дає кібер-злодіям достатньо часу, щоб втрутитися в сервери, пошкодити бази даних, вкрасти конфіденційну інформацію та впровадити шкідливий код.

Виправлення

Використовуйте доступне програмне забезпечення для ведення журналів та аудиту, щоб швидко виявляти підозрілі дії та спроби несанкціонованого доступу. Навіть якщо виявлена атака зазнала невдачі, ведення журналу та моніторинг надають безцінні інструменти для аналізу джерела та вектора атаки та вивчення того, як можна посилити політики безпеки та засоби контролю для запобігання вторгненням.

10. Підробка запитів на серверній стороні (SSRF)

Підробка запиту на стороні сервера(також звана SSRF) — це вразливість у веб-безпеці, яка дозволяє зловмиснику змусити серверну програму відправляти HTTP-запити на будь-який домен, вибраний зловмисником.

Коли веб-додаток витягує віддалений ресурс без перевірки наданої користувачем URL-адреси, виникає помилка SSRF. Навіть якщо програма захищена брандмауером, VPN або іншим списком контролю доступу до мережі, зловмисник може змусити її надіслати фальшивий запит у несподіване місце.

Виправлення

Реалізувати перевірку введення.

Використовуйте регулярні вирази (RegEx).

Приймайте лише передбачуваний формат IP-адреси (IPv4 або IPv6).

Для порівняння зі списком дозволів використовуйте значення бібліотеки методів/вихідних даних як IP-адресу.

Перевіряйте вхідні доменні імена [7].

1.4 Аналіз існуючих технологій для забезпечення безпеки Web-додатків

В таблиці 1.1 наведено актуальну загальну класифікацію методів захисту веб-додатків. Описана класифікація використовує два незалежні набори властивостей для категоризації методів захисту. А саме «Предмет спостереження» та «Підстава прийняття рішень».

Властивість "Предмет спостереження" включає "Входи", "Додаток" і "Виходи", а властивість "Підстава прийняття рішень" складається з "Статистики", "Політики" та "Наміри".

Як випливає з назви, перша властивість визначає, що аналізує захист. Наприклад, захист може контролювати вихід користувача або програми.

Друга властивість визначає, на чому ґрунтуються рішення. Рішення, що ґрунтуються на «статистиці» (зазвичай звані виявленням аномалій), побудовані на припущенні, що атаки є аномальними (рідкісними) подіями.

Рішення на основі «політики» побудовані на попередніх знаннях або побажаннях розробника захисту та зазвичай використовуються у підходах, що ґрунтуються на правилах.

На відміну від рішень на основі «політики», рішення, що ґрунтуються на «намірах», явно розглядають наміри розробника додатків (зазвичай за допомогою аналізу вихідних програм).

Таблиця 1.1.

Класифікація методів захисту веб-додатків

Підстава прийняття рішень	A. Статистика (аномалії - імовірнісний погляд)	B. Політика (знання або побажання розробника захисту, що базуються на правилах)	C. Намір (намір розробника додатків)
Предмет спостереження	1) Входи (параметри HTTP GET/POST, файли cookie, заголовок, URL-адреси – поведінка користувача)	2) Додаток (вихідний код та підхід «біла скринька»)	3) Виходи (згенерована сторінка, активність бази даних/мережі/файлової системи — поведінка програми)

Для визначення класу, до якого належить технологія захисту, потрібні два набори властивостей. Наприклад, B1 позначає захист, що контролює вхідні дані додатка, та прийняття рішень на основі політик, які визначають користувач захисту (традиційні підходи, засновані на правилах).

Більш складним прикладом може бути A1/3 або A3 - типові виявлення аномалій методом "чорної скриньки".

Методи захисту веб-застосунків можуть бути класифіковані за кількома факторами. Такі фактори можуть включати тип веб-програми, що захищається, клас атак, які метод захисту виявляє або запобігає, різні загальні риси підходу або об'єкта, що захищається.

Безпека повинна бути важливою частиною будь-якої програми. Важливо мати надійний захист програм, щоб не допустити наступних втрат:

- Втрата даних клієнта
- Втрата доходу

Перебої в обслуговуванні та простої можуть коштувати компанії великих грошей, не кажучи вже про репутаційні збитки внаслідок злому.

– Втрата довіри клієнтів

Втрата даних клієнтів через порушення кібербезпеки може мати руйнівні наслідки як іміджу бренду, так довіри клієнтів. Втрата даних клієнтів може навіть призвести до закриття бізнесу.

– Відповідність та штрафи

Уряди запроваджують стандарти безпеки, такі як GDPR, HIPAA, PCI та ISO 27001, щоб гарантувати, що компанії не нехтують безпекою. Недотримання Вашої компанії цих стандартів може призвести до штрафів, санкцій або судових позовів.

Розглянемо наступні методи та засоби для забезпечення безпеки веб-додатків:

– Повномасштабний аудит безпеки
– Шифрувати дані
– Моніторинг безпеки в режимі реального часу
– Належні методи ведення журналу
– Вжити заходів щодо посилення безпеки
– Регулярні перевірки вразливостей та оновлення

1. Повномасштабний аудит безпеки

Один із найкращих способів переконатися, що у веб-додатках немає лазівок у безпеці, – це проводити регулярні аудити безпеки.

Аудит безпеки може включати одну або кілька таких дій:

Аудит безпеки «black box»: це «хакерський підхід». Додаток тестується на вразливості, що експлуатуються, без доступу до вихідного коду.

Аудит безпеки «white box»: на відміну від аудиту безпеки чорної скриньки, в аудиті безпеки білої скриньки ви або команда, яка виконує аудит, маєте доступ до інформації, включаючи базу коду. Цей тип аудиту безпеки гарантує, що ви дотримуєтеся всіх передових методів, починаючи з методів безпечного кодування.

Аудит безпеки «grey box»: як випливає з назви, це поєднання аудиту безпеки «white box» та «*black box*». За такого підходу деяка важлива інформація надається перед аудитом.

Якщо після аудиту виявлено якісь вразливості, найкращий підхід — класифікувати їх за їх впливом, визначити пріоритет їх усунення та почати виправляти їх насамперед із вразливостей з найбільшим впливом (критична/висока).

2. Шифрування даних

Відвідувачі та клієнти можуть ділитися конфіденційною інформацією на веб-сайті. Дані, що передаються між браузером відвідувача та сервером, мають бути зашифровані.

Проте не лише дані, які передаються, мають бути зашифровані. Також потрібно зашифрувати дані, що зберігаються, щоб зловмисники не могли просто скопіювати або знищити їх.

Введення мережевих брандмауерів. Це допоможе запобігти загрозам зсередини мережі.

3. Моніторинг безпеки у реальному часі

Окрім регулярних перевірок безпеки, потрібно налаштувати надійний моніторинг в режимі реального часу. Використання брандмауера веб-застосунків (WAF) допоможе блокувати будь-яку шкідливу активність у режимі реального часу.

Оскільки брандмауери веб-програм можуть вказувати на помилкові спрацьовування або пропускати деякі загрози, також існує можливість використання додатково ASMP або RASP.

Платформа управління безпекою програм (ASMP) відстежує протоколи за межами рівня програм і допомагає захистити програми від невідомих загроз у режимі реального часу. Хоча ASMP вбудований у програму, RASP працює на сервері і відстежує поведінку ваших веб-додатків і контекст введення користувача. Якщо RASP виявить підозрілу активність, він негайно перерве сеанс і заблокує користувача-зловмисника.

4. Належна практика ведення журналу

Щоб мати уявлення про події у додатку, наприклад про те, що сталося в певний період часу, чи відбувалося щось ще в той же час і як це вплинуло на

ситуацію, що виникла, необхідно правильно вести журнал. Хоча це важлива інформація, яку необхідно постійно мати та відстежувати, вона особливо важлива у разі порушення безпеки.

Криміналістична експертиза після інциденту може стати складним завданням без належного ведення журналу. З іншого боку, при правильному механізмі ведення журналу завдання аналізу причини та розуміння зловмисника у разі витоку даних стає набагато простіше.

5. Інші заходи щодо посилення безпеки

Налаштувань за замовчуванням буде недостатньо для деяких компонентів, і будуть потрібні заходи щодо посилення безпеки, такі як:

Максимальний час виконання скрипта: встановлення максимального часу, протягом якого конкретний скрипт може виконуватись на сервері.

Вимкнення модулів: потрібно вимкнути на сервері модулі та розширення, які не використовуються програмою.

Розробка політики безпеки контенту: хороша політика безпеки контенту може допомогти запобігти проникненню таких шкідливих програм, як шкідливі програми перенаправлення.

6. Регулярні перевірки для виявлення вразливостей та оновлення

Хакери швидко знаходять веб-сайти, на яких запущено вразливе програмне забезпечення. Проводячи регулярне сканування вразливостей та виявляючи вразливості у веб-додатках або веб-сайтах до того, як вони потраплять у робоче середовище, мінімізує ймовірність атаки на веб-ресурс [6].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВЕБ-ДОДАТКІВ НА БАЗІ РІШЕННЬ QUALYS

2.1 Аналіз основних функцій WAF

Брандмауер веб-застосунків (WAF) допомагає захистити веб-програми компанії, перевіряючи та фільтруючи трафік між кожною веб-програмою та Інтернетом. WAF може допомогти захистити веб-програми від атак, таких як підробка міжсайтових запитів (CSRF), міжсайтовий скриптинг (XSS), включення файлів та впровадження SQL.

WAF може бути особливо корисним для компанії, яка надає сайт електронної комерції, онлайн-фінансові послуги або будь-який інший тип веб-продукту або послуги, пов'язані з взаємодією з клієнтами або діловими партнерами. У цих випадках WAF можуть бути особливо корисними для запобігання шахрайству та крадіжці даних. Однак, оскільки WAF не призначений для захисту від усіх типів атак, найкраще працює у складі набору інструментів, що підтримують комплексну програму безпеки додатків.

Ключові переваги WAF

WAF може забезпечити критично важливий захист будь-якого онлайн-бізнесу, який має безпечно обробляти особисті дані клієнтів. Компанії зазвичай розгортають WAF для захисту своїх веб-застосунків від витончених і цілеспрямованих атак, таких як міжсайтовий скриптинг (XSS), а також SQL-ін'єкцій, що може призвести до шахрайства чи крадіжки даних. У разі успіху, такі вторгнення можуть серйозно підірвати довіру клієнтів і навіть призвести до штрафних санкцій з боку регулюючих органів. Додатковий захист, який забезпечує WAF, може допомогти захистити репутацію та становище компанії на ринку.

WAF також полегшує адміністративний тягар забезпечення належного тестування безпеки веб-додатків на постійній основі. Допомагаючи

заздалегідь встановлювати керівні принципи та правила, групи безпеки додатків можуть відстежувати, що повинно бути дозволене через WAF. Звідти команди можуть отримувати своєчасні повідомлення про атаку, щоб вони могли набагато швидше реагувати на потенційні інциденти безпеки.

Оскільки WAF надає адміністраторам безпеки видимість додатків, необхідну для демонстрації відповідності нормативним стандартам, таким як PCI, HIPAA та GDPR, він також може бути корисним з точки зору відповідності. У сукупності всі ці переваги можуть допомогти компанії зміцнити безпеку своїх веб-застосунків і краще захистити дані клієнтів від нових загроз.

WAF без збереження стану та WAF зі збереженням стану

WAF знаходиться між веб-програмами компанії та запитами, що надходять з Інтернету. Через зворотний проксі-сервер він відстежує, фільтрує або блокує пакети даних, коли вони переміщуються до веб-додатку та з нього. При цьому він намагається відфільтрувати потенційно небезпечний трафік, який може призвести до веб-експлойтів. WAF може бути у вигляді хмарного рішення, пристрою, серверного плагіна або фільтра.

Ранні WAF, відомі як WAF без збереження стану, використовували статичні правила для аналізу потенційних загроз, що надходять через запити до серверів веб-додатків компанії. Використовуючи розпізнавання шаблонів, вони ефективно генерували обґрунтовані припущення про те, як веб-додаток може реагувати на конкретну форму атаки, використовуючи певні моделі поведінки програми та поведінки при атаці. Наприклад, WAF без збереження стану можуть перевіряти, як швидко надходять запити, чи виходять вони з одного джерела, а також інші поведінкові показники, які можуть вказувати на наявність шкідливої активності.

Друге покоління WAF, відоме як WAF з відстеженням стану, пропонує гнучкіший захист, ніж його попередник. WAF з відстеженням стану можуть збагачувати зібрані дані відповідним контекстом та аналізувати поточну картину загроз веб-програми. Оскільки WAF з відстеженням стану беруть до

уваги ширше та контекстуальне уявлення, вони краще виявляють критичні проблеми, такі як DDoS-атаки та «низькі та повільні» атаки, які намагаються підірвати безпеку, ховаючись від радарів.

Оскільки кібератаки стають дедалі складнішими, підприємства та організації мають знайти себе у кращому становищі, щоб захистити себе та своїх клієнтів від зловмисних намірів. Компанії, що займаються електронною комерцією, онлайн-фінансовими послугами та різними іншими веб-продуктами, стикаються з постійною загрозою шахрайства та крадіжки даних, що робить їх вразливими до скомпрометованої довіри клієнтів та можливих нормативних дисциплін.

Поряд із набором інструментів, WAF можуть додати важливий додатковий рівень захисту до вже надійного веб-додатку. Фахівці з безпеки можуть використовувати брандмауер веб-застосунків для відстеження можливих атак у процесі, одержуючи оповіщення про дії, які порушують заздалегідь визначені рекомендації та правила. Така видимість гарантує, що фахівці з безпеки мають необхідні можливості для дотримання нормативних стандартів, при цьому зберігаючи максимальний захист даних клієнтів [4].

2.2 Призначення та властивості рішень щодо захисту веб-додатків від Qualys

Веб-додатки агресивно розгортаються організаціями та впроваджуються – часто без дозволу – співробітниками. Qualys виявляє і каталогізує всі веб-додатки (затверджені або незатверджені), де б вони не знаходилися - локально, у хмарі, на мобільних пристроях, в системах Інтернету речей - і дозволяє помічати їх мітками користувача.

Виявлення вразливостей

Qualys постійно відстежує всі веб-програми на наявність вразливостей та неправильних конфігурацій за допомогою глибокого сканування з автентифікацією, включаючи API-інтерфейси на основі SOAP та REST, та

інтелектуального прогресивного сканування. Qualys масштабується від кількох до тисяч додатків та допомагає визначити пріоритети виправлення шляхом виявлення критичних ризиків. Також важливою характеристикою є візуалізація результатів сканування за допомогою звітів, що настроюються, та інтерактивних інформаційних панелей.

Тестування

Qualys проводить глибоке тестування веб-додатків в інформаційній системі, у внутрішніх мережах, на віддалених та мобільних пристроях, а також у загальнодоступних хмарних середовищах за допомогою автентифікованих та складних сканувань. Підтримуючи сучасні процеси, такі як DevOps, Agile та Continuous Delivery, Qualys виявляє проблеми на етапах розробки та контролю якості, а також після запуску веб-додатків у виробництво.

Виявлення шкідливого ПЗ

Веб-сайти щодня заражаються шкідливими програмами, які впливають на клієнтів, завдають шкоди брендам та призводять до включення до чорного списку. Qualys сканує веб-сайти, видає попередження та усуває шкідливі програми, у тому числі загрози нульового дня за допомогою поведінкового аналізу. Панель моніторингу відображає активність сканування та дозволяє запускати виправлення з її інтерфейсу. Звіти про діяльність можуть бути вилучені для отримання детальних відомостей та безпечно розподілені.

Блокування атак на веб-сервера

З центральної консолі Qualys надає уніфіковану наскрізну платформу із вбудованим сканером та брандмауером для швидкого виявлення та виправлення вразливостей веб-застосунків, включаючи створення віртуальних виправлень одним клацанням миші. Qualys пропонує комплексні політики і шаблони безпеки, а також дозволяє створювати правила безпеки для налаштування захисту брандмауера [8].

2.3 Аналіз основних функцій та характеристика WAS від Qualys

Глибоке сканування

Динамічне глибоке сканування Qualys WAS охоплює всі програми у внутрішньому середовищі та активній розробці, і навіть API, які підтримують мобільні пристрої. Він також охоплює екземпляри загальнодоступної хмари та дає миттєву інформацію про вразливості, такі як SQLi та XSS. Підтримуються автентифіковані, комплексні та прогресивні сканування. За допомогою програмного сканування сервісів SOAP та REST API Qualys WAS тестує сервіси та API Інтернету речей, які використовуються мобільними додатками та сучасними мобільними архітектурами.

Інструмент безпеки DevOps

Qualys WAS може забезпечити безпеку при розробці та розгортанні додатків у середовищах DevOps. За допомогою WAS можна вчасно та часто виявляєти проблеми з безпекою коду, перевіряти якість та створювати звіти.

Виявлення шкідливих програм

WAS сканує веб-сайти організації, виявляє та повідомляє про зараження, включаючи загрози нульового дня, за допомогою поведінкового аналізу. Детальні звіти про зараження шкідливим програмним забезпеченням супроводжують заражений код для виправлення. Центральна панель інструментів відображає активність сканування, заражені сторінки та тенденції зараження шкідливим програмним забезпеченням, а також дозволяє користувачам ініціювати дії безпосередньо з її інтерфейсу. Функціональність виявлення шкідливих програм надається за допомогою додаткового доповнення.

Веб-програми, які часто страждають від вразливостей та неправильних конфігурацій через погане кодування та помилкових політик захисту, можуть бути розміщені умережі практично будь-ким. У великих організаціях є сотні та навіть тисячі додатків. Qualys WAS забезпечує

прозорість та контроль, знаходячи офіційні та «неофіційні» додатки у середовищі та дозволяє класифікувати їх.

Qualys WAS допомагає знайти схвалені та незатверджені веб-програми у мережі за допомогою безперервного сканування та каталогізації програм.

Сканування

Небезпечні веб-додатки пропонують хакерам привабливу поверхню для атаки та зручну точку входу до інформаційної системи. При зломі веб-додатки можуть розкрити величезні обсяги конфіденційних бізнес-даних. Qualys WAS захищає за допомогою чіткого, ретельного та точного сканування, масштабування до тисяч веб-додатків та з невеликою кількістю помилкових спрацьовувань.

Захист дуже великих веб-програми за допомогою прогресивного сканування, яке дозволяє виконувати поетапне сканування та обходити обмеження, що перешкоджають скануванню всієї програми.

Виявлення 10 основних ризиків OWASP, таких як впровадження SQL, міжсайтовий скриптинг (XSS), підробка міжсайтових запитів (CSRF) та неперевірене перенаправлення

Досягти максимального охоплення сканування можливо за допомогою сканування з автентифікацією, включаючи розширені сценарії з використанням Selenium, системи автоматизації браузера з відкритим вихідним кодом для тестування веб-додатків.

За допомогою функцій планування можна встановити точний час початку та тривалість сканування.

Виявлення зловмисного програмного забезпечення, яке знаходиться на веб-сайтах та програмах, в тому числі про ШПЗ, що вислизають від антивірусного програмного забезпечення, які модуль виявлення шкідливих програм Qualys WAS позначає за допомогою поведінкового аналізу.

У міру того, як організації переоснащують та розширюють можливості своїх веб-додатків для впровадження інновацій у цифрову трансформацію, можливості інтерактивної звітності Qualys WAS дають

загальну картину стану безпеки веб-додатку та дозволяють його деталізувати.

Інтеграція з Qualys WAF

Qualys пропонує неперевершену безпеку веб-додатків завдяки повній інтеграції Qualys WAS та Qualys WAF, який дозволяє в один клік встановлювати виправлення для веб-застосунків, включаючи мобільні програми та служби Інтернету речей.

За допомогою єдиної консолі можна виявляти вразливості програм за допомогою WAS і швидко захищати їх від атак за допомогою WAF, забезпечуючи справжню інтегровану безпеку веб-застосунків.

Інтеграція даних сканування веб-застосунків за допомогою широкого набору API-інтерфейсів в інші системи безпеки та відповідності вимогам, такі як брандмауери, а також рішення SIEM та ERM [9].

2.4 Аналіз основних функцій та характеристик WAF від Qualys

Qualys надає єдину інтерактивну консоль для виявлення вразливостей веб-застосунків

Хмарність

Не вимагаючи придбання та обслуговування спеціального обладнання, віртуальний пристрій Qualys WAF можна швидко розгорнути та масштабувати у локальному середовищі за допомогою VMware, Hyper-V або Docker; та на загальнодоступних хмарних платформах, таких як AWS, Azure або Google Cloud Platform. Трафік програм залишається у середовищі, щоб звести до мінімуму затримки та зберегти контроль. Qualys WAF постійно взаємодіє з хмарною платформою Qualys, відстежуючи зміни конфігурації та надсилаючи йому останні події безпеки.

Qualys WAF надає повну інформацію про свої дані для безперервного моніторингу, оцінки ризиків та складання планів виправлення. На панелі інструментів узагальнюється інформація про трафік веб-сайту та тенденції

безпеки, детальну інформацію про загрози, що дозволяє оцінити серйозність та налаштувати параметри безпеки. Пошук підозрілої активності та деталізація даних про загрози, щоб отримати корисну інформацію. Qualys WAF постійно індексує події безпеки у локальних кластерах Elasticsearch або Splunk, що дозволяє миттєво виявляти дані.

Політики безпеки

Qualys WAF захищає веб-застосунки за допомогою політик безпеки, підтримуваних аналітикою безпеки Qualys, та реагуванням одним клацанням миші на події безпеки. Стандартні політики Qualys розроблені для таких популярних платформ як WordPress, Joomla, Drupal, Outlook Web Application і Sharepoint. Він також включає загальні шаблони для невідомих додатків та фреймворків. Впровадження нових підходів до безпеки веб-застосунків за допомогою адаптивних політик Qualys WAF, які завжди актуальні і не потребують спеціальних знань або складних наборів правил для налаштування та обслуговування.

Захист веб-серверів

Для того, щоб захистити інформаційну систему від незатверджених пристроїв або неавторизованого програмного забезпечення, Qualys забезпечує повну горизонтальну видимість всього апаратного та програмного забезпечення, масштабуючи до мільйонів активів – локально, у хмарних екземплярах та на мобільних кінцевих точках.

Основні характеристики Qualys WAF

1) Завдяки масштабованості віртуальномого середовища можливо додавати будь-яку кількість веб-додатків.

2) Забезпечення високої продуктивності та доступності важливих для бізнесу веб-додатків завдяки вбудованому балансуванню навантаження та моніторингу програм.

3) Налаштування Qualys WAF за допомогою універсальних шаблонів Qualys або вбудованих політик безпеки для популярних платформ, таких як WordPress, Joomla, Drupal та Outlook Web Application, Sharepoint.

4) Захист від поточних і майбутніх загроз за допомогою настроюваного захисту

5) Блокування широкого спектру атак, таких як міжсайтовий скриптинг (XSS), впровадження SQL, віддалене виконання команд, XXE та інші за допомогою вбудованого захисту. У міру появи нових загроз експерти з безпеки Qualys оновлюють правила Qualys WAF, які потім завантажуються та виявляються пропрієтарним механізмом виявлення.

6) Налаштування реагування на різні типи загроз, від простої реєстрації події до активного блокування.

7) Підтримка безперебійної роботу веб-додатку, доповнюючи мережевий захист від DDoS-атак засобами керування затримкою програм.

8) Інтеграція Qualys WAF API у середовище DevOps та захист веб-серверів, на яких розміщуються програми.

Інтеграція Qualys WAF та Qualys WAS

Завдяки новій функції ScanTrust Qualys WAF поєднує у собі Qualys WAS, щоб забезпечити справжню видимість веб-додатків: виявлення за допомогою Qualys WAS, захист за допомогою Qualys WAF та масштабоване сканування, усунення помилкових спрацьовувань та встановлення виправлень у веб-додатки одним клацанням миші.

З єдиної консолі можна використовувати Qualys WAS для виявлення вразливостей у веб-додатках, включаючи мобільні програми та IoT, усувати їх за допомогою віртуальних виправлень Qualys WAF.

Правила безпеки

Продовжує зростати кількість та складність постанов, галузевих стандартів, нормативних документів та внутрішніх політик, що впливають на технології та процеси інформаційної безпеки. Qualys WAF допоможе виконати вимоги безпеки, такі як PCI DSS 6.6, що контролює брандмауери веб-додатків.

Дане рішення допомагає дотримуватись політик і правил, які забороняють доступ до певних веб-додатків або інформації з певних місць, обмеження

доступу з певних країн або блокування мережевих адрес. А також запобігає передачі конфіденційних даних, заблокувавши можливість користувачів завантажувати або завантажувати контент або файли в незатверджених або підозрілих форматах.

Візуалізація та звіти

Дане рішення надає простий, інтуїтивно зрозумілий спосіб зрозуміти безпеку всіх веб-додатків одночасно. Qualys WAF дає групі безпеки повний огляд своїх даних для безперервного моніторингу, оцінки ризиків та шляхів виправлення. Інструменти Qualys WAF для візуалізації та створення звітів включають графічну інформаційну панель, інтерактивну аналітику та детальну інформацію про кожну загрозу та способи її усунення.

На панелі моніторингу можна побачити незвичайні шаблони та зведену інформацію про трафік веб-сайту та тенденції безпеки Qualys WAF, у тому числі час їх виникнення та джерело.

Використовуючи детальну інформацію про кожну загрозу, можливо швидко оцінювати серйозність і налаштовувати параметри безпеки для агресивного пом'якшення або мінімізації помилкових спрацьовувань.

Використовуючи великі можливості фільтрації та динамічного пошуку для виявлення підозрілої активності, деталізації даних про загрози та бази знань Qualys, а також отримання корисної інформації про загрози [8].

2.5 Особливості роботи з Qualys Cloud Platform

Qualys Cloud Platform – це платформа інтегрованих рішень, яка надає підприємствам засоби виявлення активів, мережевої безпеки, безпеки веб-застосунків, захисту від загроз та моніторингу відповідності вимогам. Все це знаходиться в хмарі – авторизація облікового запису з будь-якого веб-браузера, щоб отримати все необхідне для захисту всіх IT-ресурсів.

Qualys Cloud Platform надає комплексне рішення, що дозволяє уникнути витрат та складнощів, пов'язаних з керуванням кількома постачальниками

систем безпеки. Хмарна платформа Qualys автоматично збирає та аналізує дані про IT, безпеку та відповідність вимогам у масштабованій сучасній серверній частині. Підготувати будь-який із спочатку інтегрованих додатків безпеки та відповідності вимогам Qualys – двадцять і більше – так само просто, як поставити галочку.

Завдяки технології Cloud Agent немає потреби планувати вікна сканування або керувати обліковими даними для сканування. Понад те, служба безперервного моніторингу дозволяє заздалегідь усувати потенційні загрози. Щоразу, коли з'являються нові вразливості та погрози, атаки або підозрілі дії, оповіщення в режимі реального часу негайно повідомляють, щоб можна вжити заходів — будь то глобальне розгортання найбільш відповідного виправлення одним клацанням миші, розміщення в карантин вразливих активів або файлів, видалення програмного забезпечення; завершення процесу. мережеві підключення та багато іншого.

Qualys Cloud Platform доступна прямо в браузері, ніяких плагінів не потрібно. А завдяки потужній інформаційній панелі фахівці та менеджери з безпеки та відповідності вимогам отримують повне та постійно оновлюване уявлення про всі свої IT-ресурси — з єдиного інтерфейсу.

Це панель інструментів, що повністю настроюється, яка дозволяє бачити загальну картину, деталізувати деталі та створювати звіти для колег та аудиторів. Його інтуїтивно зрозумілі та прості у створенні динамічні інформаційні панелі об'єднують та зіставляють усі ваші дані про IT, безпеку та відповідність вимогам в одному місці з усіх різних хмарних додатків Qualys. Завдяки потужним кластерам Elasticsearch тепер можна шукати будь-які активи, включаючи локальні ресурси, кінцеві точки та хмарні ресурси з 2-секундною видимістю.

Переваги

1) Не потрібне додаткове обладнання
2) Просте глобальне сканування

Легко виконуйте сканування в географічно розподілених та сегментованих мережах як по периметру, за брандмауером, динамічних хмарних середовищах та кінцевих точках.

3) Актуальні ресурси

Qualys має найбільшу в галузі базу знань про сигнатури вразливостей і виконує понад 6 мільярдів сканувань IP-адрес на рік. Усі оновлення безпеки виконуються в режимі реального часу.

4) Нижчі експлуатаційні витрати

Оскільки все перебуває у хмарі, не потрібні капітальні витрати, додаткові людські ресурси, а також інфраструктура чи програмне забезпечення, які потрібно купувати та обслуговувати.

5) Безшовне масштабування

Qualys Cloud Platform - це комплексне комплексне рішення для всіх аспектів IT-безпеки. Після розгортання легко додавайте нове покриття, користувачів та послуги за необхідності.

6) Надійно збережені дані

Дані про вразливості надійно зберігаються та обробляються на багаторівневій архітектурі серверів із балансуванням навантаження [10].

3 ТЕХНОЛОГІЯ ЗАХИСТУ WEB-РЕСУРСІВ В КОРПОРАТИВНІЙ ІС НА БАЗІ QUALYS

3.1. Розроблення рекомендацій щодо застування технології WAF для захисту веб-ресурсів

HTTP(S) є основою передачі даних для Всесвітньої павутини та функціонує як протокол запиту-відповіді для зв'язку. Мобільні програми, хмарні обчислення, зв'язок через API, програми для інтрамережі та веб-пошта – це звичайні інструменти, якими користуютья щодня. Всі ці програми взаємодіють через HTTP(S).

Qualys надає програми, що дозволяють сканувати та виявляти вразливості – Qualys Vulnerability Management (VM) та Qualys Web Application Scanning (WAS).

Досвід показує, що виправлення вихідного коду веб-сайту може зайняти більше часу, ніж очікувалося, залежно від порушеного компонента, ресурсів розробки та гнучкості компанії у застосуванні та перевірці оновлень програмного забезпечення.

Ось де Qualys Web Application Firewall (WAF) приходить на допомогу. Це інструмент негайного виправлення, який здатний захистити веб-застосунки від атак і дає команді розробників час для усунення важливих проблем безпеки [8].

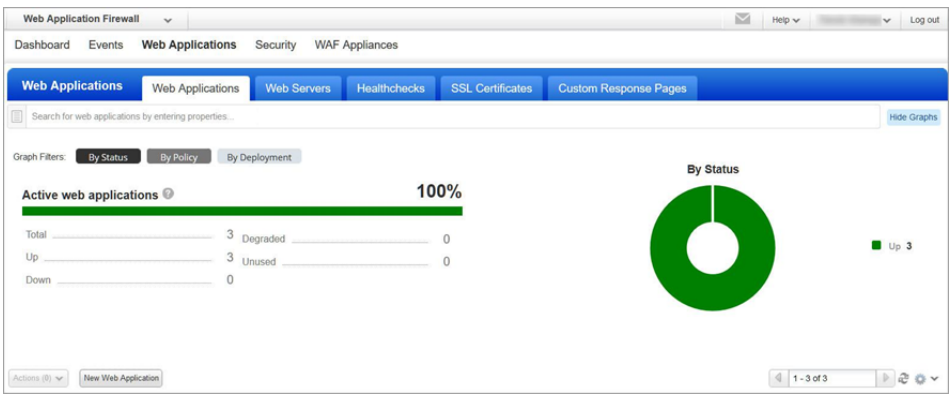

Рис. 3.1. Інтерфейс Qualys WAF

Використовуючи WAF, користувачі можуть розгорнути кілька екземплярів брандмауера для веб-застосунків. Кожен брандмауер складається з віртуального пристрою, який налаштований для зворотного проксіювання вашого HTTP(S)-трафіку. Цей пристрій буде розміщено на платформі віртуалізації (Amazon EC2, Microsoft Azure, Google Cloud, VMware або Hyper-V), на сервері або в докері (контейнері).

Qualys пропонує потужний брандмауер веб-застосунків наступного покоління, який використовує постійно оновлюваний набір правил безпеки для захисту додатків. Цей сучасний брандмауер використовує хмарний підхід та забезпечує класичний режим роботи та розгортання.

Всі події безпеки спрямовуються через хмарну платформу Qualys. Вони постійно відстежуються та аналізуються дослідниками безпеки, щоб обчислити найкращий набір правил для блокування найновіших атак та вразливостей нульового дня. Користувачі Qualys WAF налаштовують політики безпеки для своїх веб-застосунків на основі правил фільтрації, моніторингу, блокування та складання звітів про події.

Qualys WAF спрощує розуміння безпеки всіх веб-застосунків одночасно. Коротка візуальна інформаційна панель підсумовує різні події, що відбулися, коли вони походять і звідки вони походять. Легко отримуйте інтерактивні відомості про потенційні загрози та знайдіть докладну інформацію про кожну потенційну загрозу та способи її усунення.

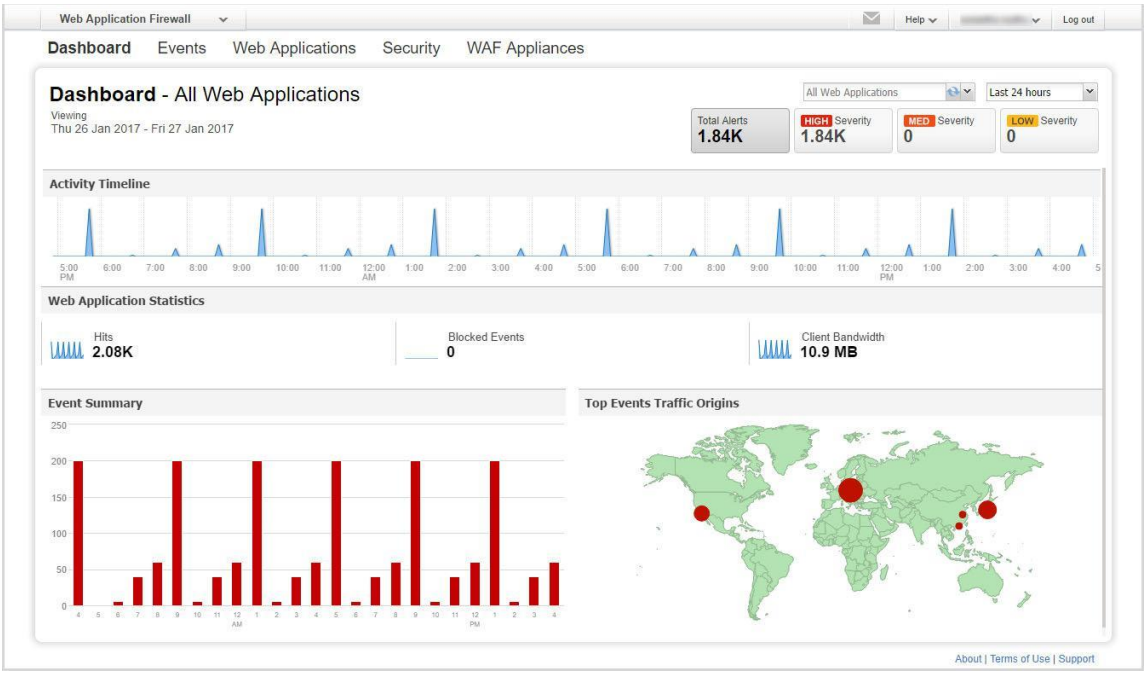

Рис. 3.2. Панель інструментів

Створення кластера WAF

Кластер WAF — це зв'язувальна ланка між веб-програмою та пристроєм, через який вона проксується. Це група з одного або декількох пристроїв WAF (або проксі-набір). Кластер WAF може містити кілька пристроїв, але кожен з них діятиме як автономне, при цьому трафік оброблятиметься однаково для всіх пристроїв, зареєстрованих у зазначеному кластері. Веб-додаток може бути проксований через кілька кластерів.

При виявленні зміни конфігурації в будь-якій веб-програмі пристрій WAF отримує конфігурації для всіх розгорнутих веб-застосунків. Коли сервер WAF отримує зміни конфігурації, він перезавантажує конфігурацію під час виконання, щоб застосувати зміни. Час, необхідний серверу WAF для перезавантаження конфігурації, залежить від розміру конфігурації, який, у свою чергу, залежить від кількості веб-застосунків та індивідуальних параметрів поведінки, налаштованих для кожної веб-програми.

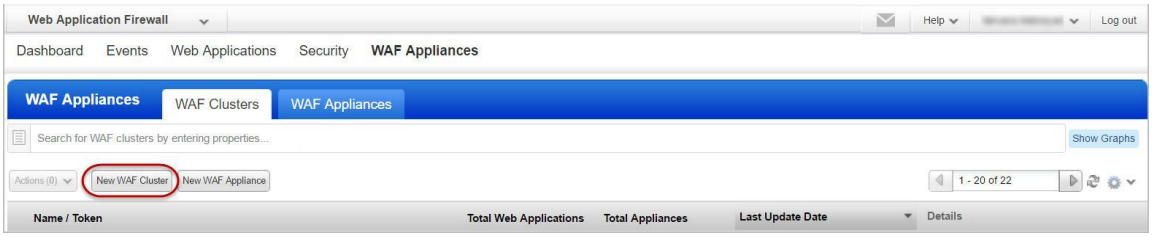

Рис. 3.3. Створення кластеру

В налаштуваннях можна вказати IP-адресу/діапазон/мережа довірених проксі-серверів або балансувальників навантаження, налаштованих в режимі повного проксі. Якщо запит не є надійним джерелом, значення заголовка X-Forwarded-For автоматично відкидаються. Якщо не надається IP-адреса для довірених вихідних проксі-серверів або балансувальників навантаження, то IP-адреси відповідно до RFC1918 є довіреними.

Щоразу, коли запит адресований неіснуючому повному домену, можна вибрати відображення сторінки помилки WAF за замовчуванням, сторінки відповіді або перенаправити запит у вказане місце. Це відбувається, якщо зловмисник підробляє запит із помилковим заголовком хоста або запитаний хост відсутній у псевдонімі, налаштованому для вашого веб-сайту.

Налаштування веб-додатків

Віртуальний пристрій WAF можна додати та налаштувати у середовищі (Amazon EC2, Microsoft Azure, Google Cloud, VMware або Microsoft Hyper-V), на сервері або в докері (контейнері).

Правила брандмауера/групи безпеки EC2:

- Дозволити трафік HTTP(S) (TCP-80,443 або будь-який інший) до пристрою WAF з Інтернету.
- Дозволити SSH (TCP-22) для пристрою WAF лише з довіреної мережі керування.
- Дозволити мінімальний доступ до вихідного веб-сервера: тільки IP-адреса пристрою WAF повинна мати доступ до продукції веб-серверів [ip:port]. Будь-який прямий доступ повинен бути обмежений лише адміністративною мережею.

Рекомендації щодо балансування навантаження

- Балансувальники навантаження повинні бути налаштовані на передачу вузлів кластера WAF, щоб в Qualys могли належним чином налаштувати надмірність в інфраструктурі.

- Пристрій WAF працює як зворотний проксі-сервер. Важливо, щоб будь-які конфігурації DNS, брандмауера NAT або конфігурації балансувальника навантаження були налаштовані на перенаправлення трафіку на пристрій WAF. Потім він перевірить вхідний запит і на основі вашої конфігурації передасть відповідному вихідному серверу.

В рішенні Qualys WAF можна створити новий веб-додаток, або додати існуючий. Для створення нового веб-ресурсу потрібно виконати наступні кроки:

1) Деталі активу: в даному розділі потрібно вказати ім’я веб-додатку, основну URL-адресу, встановити користувацькі атрибути та призначити теги, якщо вони є.

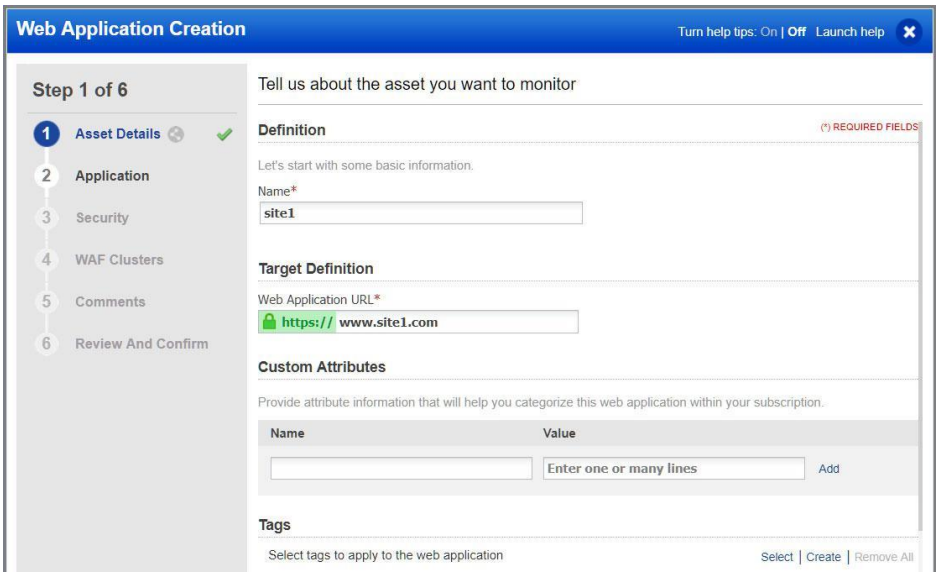

Рис. 3.4. Налаштування веб-додатку

Налаштування додатку та мережі: дає змогу вказати вторинні URL-адреси, використовувані профілі, створені для Інтернету, пул серверів та сертифікат SSL.

WAF дозволяє вибрати профіль SSL, відповідні протоколи, рівні безпеки та шифри. Профіль SSL містить відомості про сертифікат безпеки. Список доступних шифрів залежить від вибраних протоколів та рівнів безпеки. Для сертифікатів SSL підтримуються протоколи TLS 1.0, TLS 1.1, TLS 1.2 та TLS 1.3. Стандартні протоколи — TLS 1.1, 1.2 і TLS 1.3, а стандартні фільтри — Strong і Good. Шифри використовуються в порядку, в якому вони відображаються.

2) Безпека: в даному розділі налаштовуються політики безпеки та профілі HTTP.

Вибір опції «Блокувати з налаштованою відповіддю» дозволяє відображати повідомлення для користувача, якщо політика безпеки блокує певний розділ або сторінку на веб-сайті.

Додавання одного або кілька правил, щоб дозволити або заблокувати доступ до певних ресурсів веб-додатків.

3) Кластери WAF: вибір кластеру, щоб розгорнути веб-програму. Кластер містить один або кілька пристрої (зворотні проксі).

При виявленні зміни конфігурації в будь-якій веб-програмі пристрій WAF отримує конфігурації для всіх розгорнутих веб-застосунків. Коли сервер WAF отримує зміни конфігурації, він перезавантажує конфігурацію під час виконання, щоб застосувати зміни. Час, необхідний серверу WAF для перезавантаження конфігурації, залежить від розміру конфігурації, який, у свою чергу, залежить від кількості веб-застосунків та індивідуальних параметрів поведінки, налаштованих для кожної веб-програми. Декілька кластерів WAF можуть відстежувати один і той же веб-додаток.

Налаштування політик безпеки

Політика безпеки, яка призначається веб-застосунку, визначає критерії перевірки WAF і рівень чутливості — це впливає на те, про яке порушення повідомляється для даного веб-додатку і чи буде позначатися трафік як шкідливий.

Вибір один із готових шаблонів політик надане Qualys - Drupal, Joomla, Wordpress та OWA. Не можна змінити вбудовані шаблони та системні політики. Окрім готових шаблонів є можливість створення нової політики та налаштувати параметри політики. Можна створити декілька політик і призначити їх різним веб-застосункам (по одній для кожної веб-програми).

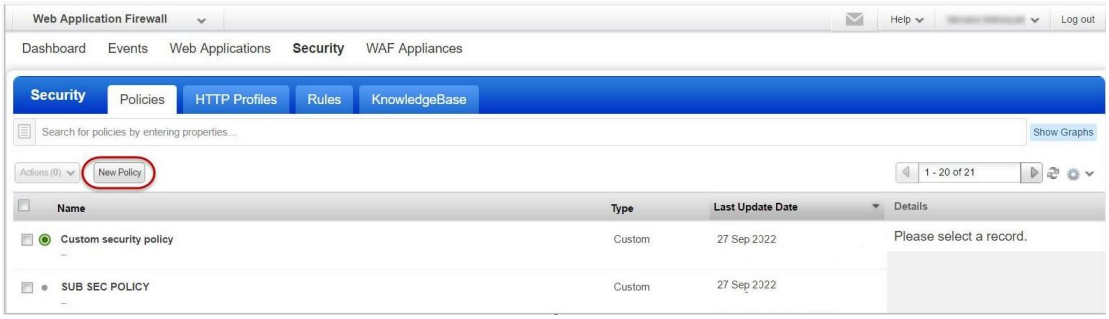

Рис. 3.5. Налаштування політик безпеки

Безпека додатків: налаштування рейтингу чутливості (від 20 до 80) для різних категорій виявлення. Це впливає на те, яка перевірка виконуватиметься шляхом фільтрації потенційно важливих подій.

Контроль: встановлення для загроз порогові значення рівня (від 1 до 100) для реєстрації та блокування. Це впливає на те, які події будуть реєструватися та блокуватися.

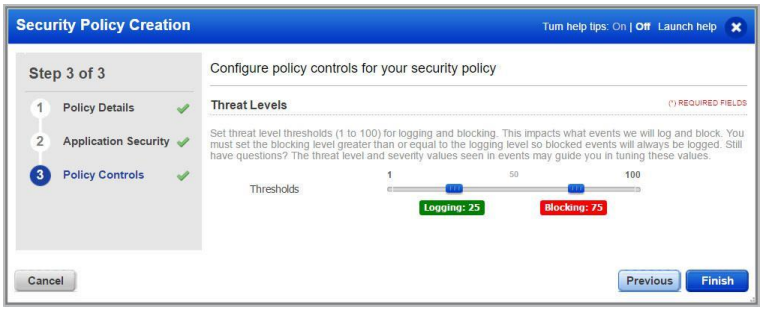

Рис. 3.6. Параметри політик безпеки

Створення профілів додатків

Qualys WAF тепер дозволяє створювати багаторазові профілі для налаштувань, які зазвичай можна використовувати кількома веб-додатками. Багаторазові профілі можуть бути створені для пулів веб-серверів, параметрів перевірки працездатності, сертифікатів SSL та фільтрів протоколу HTTP [11].

Профіль пула веб-серверів

Якщо немає спеціального балансувальника навантаження завдяки новим пулам веб-серверів Qualys WAF тепер може балансувати навантаження трафіку між кількома вихідними серверами. В якості альтернативи, якщо веб-додаток знаходиться в докері (контейнері), увімкніть платформу Docker для надання інформації про докер. Можна вибрати один пул веб-серверів для кожної веб-програми.

Використовуючи ваги WAF для розподілення навантаження запитів на різні сервери в пулі веб-серверів. Для цього потрібно додати вагу (число) поряд з адресою сервера. Також можливо додати ваги до існуючого пулу. За замовчуванням – 1. Максимально допустиме значення – 256.

Розглянемо пул, що складається з чотирьох вихідних серверів з вагами 1, 2, 3 і 3. Загальна вага, призначена всім серверам, дорівнює 9. WAF розподіляє 1/9 загального навантаження на сервер 1, потім 2/9 загального навантаження на сервер. 2 і так далі.

Потім виберіть метод балансування навантаження, щоб визначити, який сервер отримує з'єднання.

Профіль Healthcheck

Створюйте профілі перевірки працездатності, щоб відстежувати доступність програм до веб-серверів (контейнерів). Виберіть один профіль перевірки працездатності для кожної веб-програми. Він буде виконуватися для всіх веб-серверів, перерахованих в пулі серверів, або для всіх контейнерів, створених з ідентифікатора докеру образу, відповідно до заданої користувачем періодичністю. Якщо один внутрішній веб-сервер (контейнер) не проходить перевірку працездатності після X спроб, він буде вважатися вимкненим, і запити до нього не надсилатимуться доти, доки служба не повернеться. Тим часом брандмауер продовжуватиме перевіряти серверну частину.

Отже, якщо всі внутрішні веб-сервери (контейнери) не пройдуть перевірку працездатності, всі вони будуть вважатися відключеними брандмауером, що призведе до недоступності програми, тобто WAF

припинить пересилання трафіку на стороні сервера. Натомість він відповість клієнту кодом відповіді HTTP, який визначається користувачем. Цей код відповіді на помилку задається в самому веб-додатку на вкладці Додаток. При створенні профілю перевірки працездатності вкажіть бажаний метод HTTP для запиту програми, URL-адресу для перевірки та код відповіді, що повертається у разі успіху. Також є функція, яка дає вказати інтервали та входження «вгору» та «вниз», щоб зафіксувати частоту зонди, а також кількість успішних чи невдалих спроб перед зміною стану внутрішнього веб-сервера. Залежно від результату перевірки працездатності статус сервера встановлюється активним або неактивним.

На вкладці «Пристрої WAF» відображається стан перевірки працездатності для всіх серверів, на які поширюється пристрій. Ця інформація перевірки працездатності сервера згрупована за кожною веб-програмою, що відстежується пристроєм.

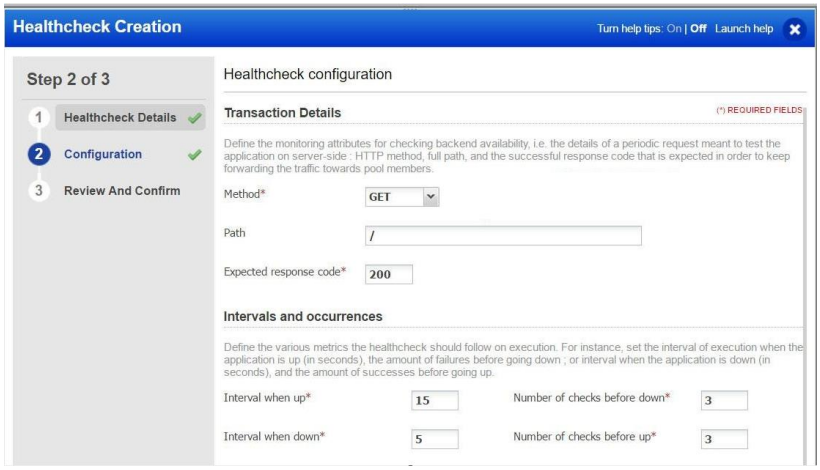

Рис. 3.7. Профіль Healthcheck

HTTP-профіль

Налаштування профіль HTTP необхідне для фільтрації атрибутів, орієнтованих на протокол (методи, тип вмісту, декларативна безпека та атрибути витоку інформації). Можна вибрати один профіль HTTP для кожної веб-програми.

HTTP-протокол- налаштування аналізу протоколу HTTP для політики.

Захист веб-сервісів - увімкніть синтаксичний аналіз XML/JSON у профілях HTTP, щоб переконатися, що передані корисні дані сумісні з XML/JSON.

Витік інформації - вибір параметрів маскування сервера, придушення конфіденційних заголовків.

Декларативна безпека - налаштування відповіді на файли cookie, сніфінг типів контенту та міжсайтові сценарії браузера.

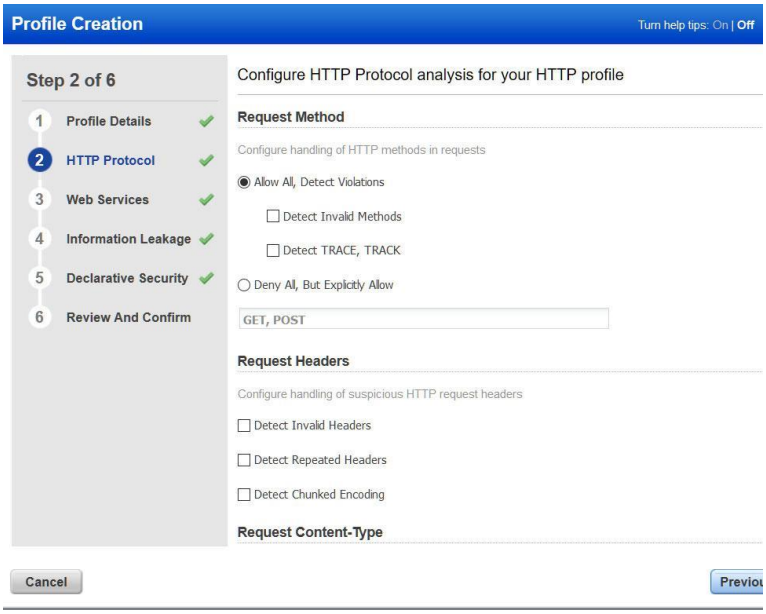

Рис. 3.8. Налаштування HTTP профілів

Додати винятки

Використовуйте винятки, коли проходить ідентифікація на хибнопозитивну або хибнонегативну подію. Помилкове спрацювання — це законний запит, який несподівано заблоковано. Хибнонегативний результат - це незаконний запит, який був авторизований, хоча цього не мало бути.

З Qualys WAF можна помітити подію як неправдивопозитивну. Для цього потрібно виконати наступне: «Події» > «Список подій», виберіть подію, клацніть стрілку та виберіть «Позначити як помилкове спрацювання». Майте на увазі, що це простий маркер, він не впливає на поведінку під час обробки трафіку.

Щоб створити виняток, виберіть подію, натисніть на стрілку і виберіть "Створити виняток" або виберіть цю опцію в меню "Дії" під час перегляду події. Винятки створюються у вигляді користувацьких правил.

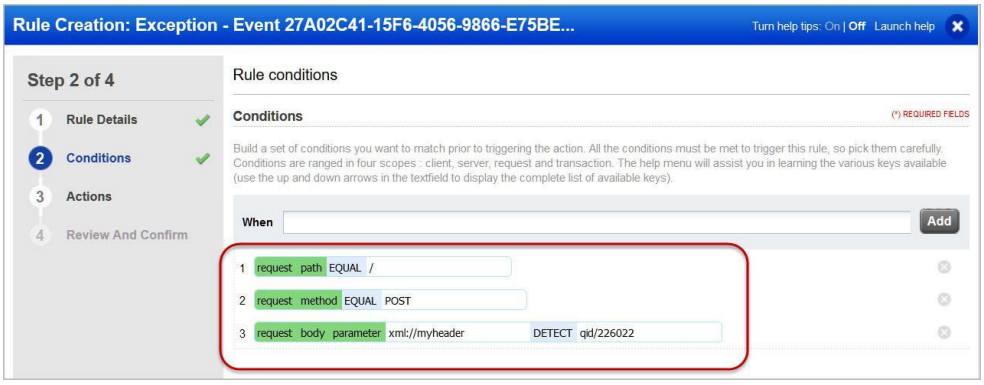

Рис. 3.9. Створення винятків

Події

Ознайомтеся з подіями безпеки (порушеннями), які були виявленні у веб-додатку.

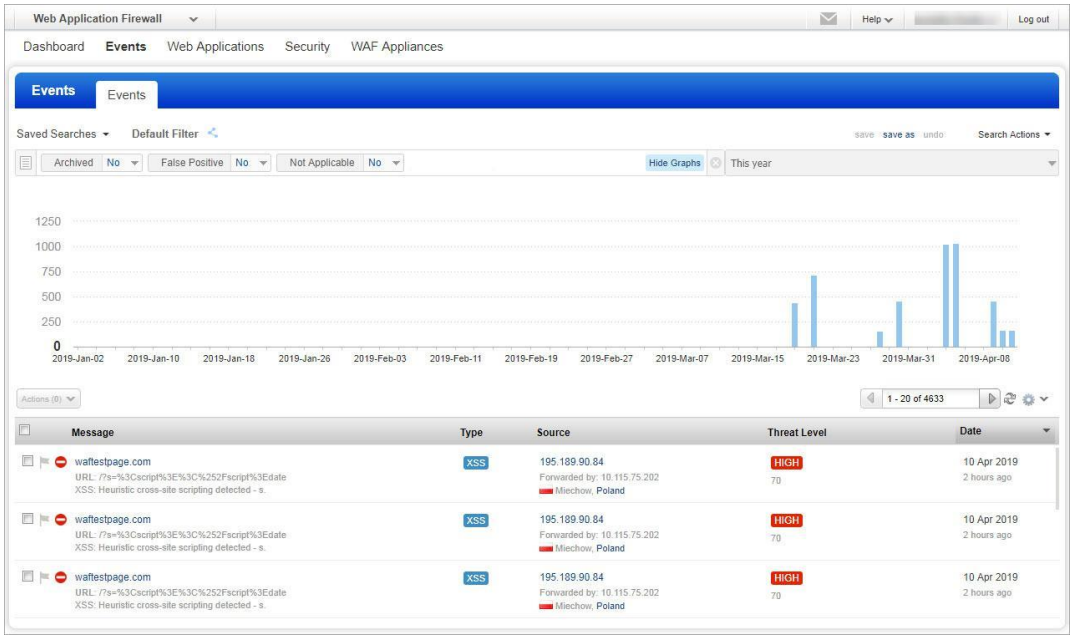

Рис. 3.10. Вкладка подій

Можливо переглянути детальну інформацію про кожну потенційну загрозу. Перегляньте відомості про подію і виконайте дії в меню, тобто

позначте подію як позначену прапорцем, хибне спрацювання або незастосовне.

Натиснувши на QID, дозволить перейти до всеосяжної бази знань Qualys, яка містить додаткову інформацію про кожну загрозу та способи її усунення [12].

3.2. Застування технології WAS для захисту веб-ресурсів

Qualys Web Application Scanning (WAS) надає організаціям простоту використання, централізоване управління та можливості інтеграції, необхідні для захисту від зловмисників та забезпечення безпеки веб-додатків. Qualys WAS дозволяє організаціям оцінювати, відстежувати та усувати вразливості веб-застосунків.

Ключові особливісті:

– Сканувати веб-програми (Інтранет, Інтернет) та сканувати їх на наявність уразливостей

– Повністю інтерактивний інтерфейс користувача з гнучкими робочими процесами та звітами

– Визначте, як веб-програми обробляють конфіденційні або секретні дані.

– Налаштування: чорні/білі списки, robots.txt, sitemap.xml та ін.

– Підтримує поширені схеми автентифікації

– Звіти з рекомендованою практикою кодування безпеки та конфігурацією

– Надійні масштабовані можливості сканування

– Підтримує сканування веб-додатків HTML з JavaScript та вбудованим Flash

– Комплексне виявлення вразливостей власних веб-додатків, включаючи 10 основних уразливостей OWASP.

– Відрізняє проблеми, що експлуатуються, впровадження помилок від простого розкриття інформації

– Профілює поведінку власних веб-додатків

– Налаштовує продуктивність сканування з рівнем продуктивності, що настроюється [13].

Нові технології, реалізовані в бекенді на основі Java, пропонують безліч переваг для користувачів:

- Інтерфейс користувача з динамічними та інтерактивними інтерфейсами, майстрами та новими шаблонами звітів для представлення даних сканування з широким набором параметрів представлення.

- Настроюваний механізм створення звітів на основі шаблонів виводить звіти у різних форматах (html, pdf, зашифрований pdf, ppt, xml, cvs).

- Швидкий пошук у кількох великих наборах даних Qualys, включаючи результати сканування, дані активів, профілі сканування, користувачів та вразливості.

- Створюйте та керуйте тегами (статичними та динамічними) для групування та організації веб-додатків.

- Динамічний розподіл сканування на кілька сканерів залежно від доступності та навантаження для оптимізації сканування великих мереж, що значно скорочує загальний час сканування, необхідний виконання великих завдань сканування.

Сканування REST API, інтеграція CI/CD

Qualys підтримує Swagger версії 2.0, що дозволяє командам DevOps оптимізувати оцінку REST API та швидше отримувати уявлення про стан безпеки серверних частин мобільних програм та сервісів Інтернету речей (IoT). Крім того, новий власний модуль для Jenkins забезпечує автоматизоване сканування веб-додатків на наявність вразливостей для груп, що використовують популярний інструмент безперервної інтеграції/безперервної доставки (CI/CD). У тандемі клієнти тепер можуть використовувати новий Qualys Browser Recorder, безкоштовне розширення для браузера Google

Chrome, щоб легко переглядати сценарії для навігації за складною автентифікацією та бізнес-процесами у веб-додатках.

Сканування API передачі репрезентативного стану (REST) на основі Swagger. На додаток до сканування веб-служб Simple Object Access Protocol (SOAP) Qualys WAS використовує специфікацію Swagger для тестування REST API. Користувачам потрібно лише переконатися, що файл Swagger версії 2.0 (формат JSON) видно службі сканування, і інтерфейси API будуть автоматично перевірені на наявність поширених недоліків безпеки додатків.

Розширене сканування API із підтримкою Postman. Postman - це інструмент, що широко використовується для функціонального тестування API REST. Колекція листоноші — це файл, який можна експортувати з інструмента, що поєднує пов'язані запити (кінцеві точки API) та ділитися ними з іншими користувачами. Ці колекції експортуються у форматі JSON. Після випуску підтримки Postman Collection Qualys WAS у клієнтів з'явилася можливість налаштувати сканування API за допомогою Postman Collection для свого API.

Модуль Jenkins, що підключається. Модуль Qualys WAS Jenkins, що підключається, дозволяє командам DevOps вбудовувати сканування вразливостей додатків в існуючі процеси CI/CD. Завдяки інтеграції сканування таким чином тестування безпеки програм виконується раніше в SDLC для виявлення та усунення недоліків безпеки, що значно знижує вартість виправлення порівняно з пізнішим тестуванням у SDLC.

Qualys Browser Recorder – це нове розширення для Chrome дозволяє користувачам записувати дії веб-браузера та зберігати сценарії для повторного автоматизованого тестування. Сценарії відтворюються в Qualys WAS, що дозволяє механізму сканування успішно проходити складні процеси автентифікації та бізнес-процесів. Розширення Qualys Browser Recorder є безкоштовним і доступним для всіх (не тільки клієнтів Qualys) через Інтернет-магазин Chrome [14].

Налаштування Qualys WAS включає наступні кроки:

1) Налаштування веб-додатків, які потрібно сканувати.

Просто перейдіть до «Веб-програми», виберіть «Нова веб-програма» та введіть URL-адресу веб-програми.

2) Запустіть сканування для виявлення

Для запуску внутрішнього сканування необхідно налаштувати сканер у мережі - фізичний або віртуальний пристрій.

Найкраще виконати сканування виявлення — перейдіть до «Сканування» > «Список сканування» та виберіть «Нове сканування» > «Сканування виявлення».

Сканування виявлення виконує лише перевірку зібраної інформації (виявлені форми, знайдені зовнішні посилання тощо). Це хороший спосіб дізнатися, куди піде сканування і чи є URI, які потрібно додати до списку винятків для сканування вразливостей.

Перегляньте звіт про сканування виявлення, коли сканування буде завершено. Перейдіть до розділу «Сканування» > «Список сканування», виберіть своє сканування та виберіть «Переглянути звіт» у меню «Швидкі дії». Прокрутіть вниз до "Результати", потім "Зібрана інформація" і розгорніть вниз, щоб побачити подробиці виявлення. Обов'язково ознайомтесь із цими QID (ідентифікаторами Qualys): 150009 - просканово посилань та 150021 - діагностика сканування.

3) Запуск сканування для виявлення вразливостей

Qualys проведе оцінку вразливості веб-додатку. Просто перейдіть до «Сканування» > «Список сканування» та виберіть «Нове сканування» > «Сканування вразливостей».

Після завершення сканування обов'язково перегляньте звіт про сканування вразливостей. Перейдіть до розділу «Сканування» > «Список сканування», виберіть своє сканування та виберіть «Переглянути звіт» у меню «Швидкі дії». Прокрутіть вниз до розділу «Результати» та перейдіть до подробиць виявлення в розділах «Уразливості», «Зібрана інформація» та «Конфіденційний вміст» (якщо є).

Використання аутентифікації

Для виявлення багатьох уразливостей потрібне сканування з автентифікацією. Підтримуються кілька типів аутентифікації – Form, HTTP Basic та Digest. Можна сканувати один і той же веб-додаток кілька разів з різними обліковими даними. Для цього можна додати кілька записів і надати значні заголовки, пов'язані з рівнем привілеїв, наприклад, «Анонімний», «Користувач», «Адміністратор». Наприклад, запис «Користувач» може знайти 300 посилань та 10 вразливостей, тоді як запис «Анонім» може знайти лише 100 посилань та жодної вразливості.

Публічні та внутрішні

Внутрішнє сканування використовує сканер, розміщений у мережі. Виберіть сканер, який потрібно використовувати, на ім'я в меню Scanner Appliance у налаштуваннях веб-програми.

Зовнішнє сканування завжди доступне за допомогою хмарних сканерів, встановлених у Центрах управління безпекою (SOC) Qualys. Для цього виберіть «Зовнішній» у меню Scanner Appliance у налаштуваннях веб-програми.

Якщо увімкнути функцію моніторингу шкідливих програм в налаштуваннях зовнішньої веб-програми, сканер буде запускати щоденне сканування веб-програми на наявність шкідливих програм. Можна вказати час для цих сканувань та отримати повідомлення електронною поштою.

Маркування веб-додатків

Теги допомагають упорядковувати веб-програми та інші об'єкти у системі та контролювати доступ користувачів до цих об'єктів. Використовуючи тег до веб-застосунку, надається доступ до нього користувачам з таким же тегом у своїх областях. Також можна використовувати теги для фільтрації списку веб-додатків, створення звітів веб-додатків та багато іншого. Перейдіть до керування активами CyberSecurity (CSAM) [13].

Область сканування

Область сканування, яка вибирається в налаштуваннях веб-застосунку, визначає, куди буде направлено сканування.

Наприклад:

Обмежити ім'я хоста URL

Це означає, що сканер обмежить сканування ім'ям хоста в URL-адресі, використовуючи HTTP або HTTPS та будь-який порт. Припустимо, початкова URL-адреса - http://www.test.com.

Які посилання скануватимуться — скануватимуться всі посилання, виявлені в домені www.test.com. Також зверніть увагу, що http://www.test.com/* (* тут як підстановочний знак) буде просканово. Усі посилання, виявлені на http://www.test.com/support та https://www.test.com:8080/logout тощо, будуть просканованi.

Які посилання НЕ скануватимуться - не переходитимуть за посиланнями з піддоменів www.test.com. Це означає http://www2.test.com. та/або http://sub1.test.com/ не скануватимуться.

Обмежити вміст, розташований у підкаталозі URL або нижче

Це означає, що будуть скануватися всі посилання, що починаються з підкаталогу URL, використовуючи HTTP або HTTPS та будь-який порт. Припустимо, ваша початкова URL-адреса - http://www.test.com/news.

Які посилання скануватимуться — скануватимуться всі посилання, що починаються з http://www.test.com/news. Також будуть просканованi http://www.test.com/news/headlines та https://www.test.com:8080/news/.

Які посилання НЕ скануватимуться. Такі посилання, як http://www.test.com/agenda та http://www2.test.com, не будуть скануватися.

Обмеження до URL-імені хоста та вказаного піддомену

Це означає, що будуть скануватися лише URL-адресу хоста та один вказаний піддомен, використовуючи HTTP або HTTPS та будь-який порт. Допустимо, початкова URL-адреса - http://www.test.com/news/, а субдомен - sub1.test.com.

Які посилання скануватимуться - будуть скануватися всі посилання, виявлені на www.test.com і в sub1.test.com, а також на будь-якому з його піддоменів. Також будуть скануватися такі домени: http://www.test.com/support, https://www.test.com:8080/logout, http://sub1.test.com/images/ та http:// відео .sub1.test.com.

Які посилання НЕ скануватимуться. Посилання, домен яких не збігається з ім'ям хоста URL-адреси веб-програми або не є субдоменом sub1.test.com, не відстежуватимуться. Це означає, що http://videos.test.com не скануватиметься.

Обмеження URL-адресою імені хоста та вказаними доменами

Це означає, що будуть скануватися лише URL-адресу хоста та вказані домени, використовуючи HTTP або HTTPS та будь-який порт. Допустимо, початкова URL-адреса - http://www.test.com/news/, а вказані домени - sub1.test.com і site.test.com.

Які посилання скануватимуться - будуть скануватися всі посилання, виявлені на www.test.com і в sub1.test.com, а також у всіх інших зазначених доменах. Це означає, що будуть скануватися такі домени: http://www.test.com/support, https://www.test.com:8080/logout та http://sub1.test.com/images/.

Які посилання НЕ скануватимуться. Посилання, домен яких не співпадає з ім'ям хоста URL-адреси веб-програми або одним із вказаних доменів, не відстежуватимуться. Це означає, що http://videos.test.com та http://videos.sub1.test.com не скануватимуться [14].

Списки винятків

Списки винятків налаштовуються на глобальному рівні (для всіх веб-програм), а також налаштовуються для веб-додатків. Сканер дає змогу реалізувати списки винятків, що настроюються, для своєї веб-програми і ігнорувати глобальні налаштування при створенні або редагуванні веб-додатку.

Можна використовувати список винятків, щоб повідомити, які посилання сканувати, а які ігнорувати для всіх веб-програм. Для робочої веб-програми рекомендується додавати сторінки з певною функціональністю до списку винятків, виконання яких може призвести до небажаних результатів, наприклад, до можливого надсилання занадто великої кількості електронних листів, можливої відправки кнопки «видалити все» або вимкнення/видалення облікових записів.

Списки винятків — це списки дозволів, списки винятків, список винятків даних POST та список регулярних виразів виходу із системи.

Якщо веб-програма має як список винятків, так і список дозволів, сканер розглядаємо записи списку дозволів як винятки зі списку винятків. Він не скануватимемо жодного запису списку винятків, якщо даний виняток не відповідає запису списку дозволів. Проскануються всі інші посилання, включаючи ті, які відповідають записам у білому списку.

Якщо веб-програма має лише список винятків (без списку дозволів), дане рішення пропустить всі посилання, які відповідають записам списку винятків. Якщо веб-програма має лише список дозволів (без списку винятків), він скануватиме лише ті посилання, які відповідають записам списку дозволів.

Використання скриптів Selenium для сканування

Використовуйте Qualys Browser Recorder для створення скрипту Selenium. Qualys Browser Recorder – це безкоштовне розширення для браузера, що дозволяє записувати та відтворювати сценарії для автоматизованого тестування веб-додатків. Qualys Browser Recorder включає все ядро Selenium Core, дозволяючи вам захоплювати веб-елементи та записувати дії у браузері, щоб ви могли швидко та легко створювати, редагувати та відтворювати автоматичні тестові випадки.

Можна завантажити скрипти Selenium у налаштування веб-програми, і WAS відтворinm ці скрипти під час сканування веб-програми.

Наприклад:

- Відтворення записаних кроків для сканування веб-програми, яка потребує складних робочих процесів, таких як вибір комбінацій введення користувача, які вимагають певних знань та/або взаємодії з користувачем.

- Відтворення записаних кроків, такі як натискання кількох кнопок або заповнення форм.

- Відтворення записаних кроків для виконання вимог входу та аутентифікації.

Burp Suite

Інтеграція з набором інструментів Burp Suite є першою в серії інтеграцій із проксі-інструментами для атак, які використовуються в основному для проведення більш складних ручних випробувань на проникнення та перевірки додатків. Розробники WAS розуміють, що є місце як для автоматичного сканування, так і для атакуючих проксі-серверів, і тому поєднується найкраще з обох підходів. Інтеграція з Burp Suite дає можливість зберігати результати, виявлені сканером Burp Suite, разом з даними, виявленими WAS, і ділитися цією інформацією з кількома користувачами.

Qualys WAS 3.0 також представляє інтеграцію з проксі-інструментом атаки, що використовується переважно для проведення цілеспрямованого ручного тестування проникнення та перевірки додатків. Хоча WAS спроектований так, щоб бути повністю автоматизованим і масштабованим і підходить для тестування безпеки більшості програм, існують деякі веб-програми, що вимагають вищого рівня гарантії. Ці програми зазвичай вимагають як автоматичного сканування, так і тестування ручного на проникнення. У більшості випадків тестування веб-застосунків в основному проводиться з використанням проксі-інструментів для атак. Проксі-сервери для атак забезпечують високий рівень контролю для досвідчених користувачів та допомагають проводити глибоке тестування, коли це необхідно. визнаючи,

Qualys WAS 3.0 робить перший крок у цьому розвитку, інтегруючи результати сканування з Burp Suite Professional (BSP). BSP – це інструмент, який поєднує можливості інтерактивного тестування зі скануванням.

Тестувальники, які використовують BSP, можуть сканувати окремі сторінки під час навігації по веб-застосунку і виявляти при цьому вразливості. Але BSP спочатку призначений для використання одним користувачем. Не існує централізованого сховища для результатів, яке дозволяло б спільно використовувати їх для кількох користувачів або відстежувати їх з часом. Qualys прагне подолати це обмеження, надаючи спосіб імпортування результатів сканера BSP. Це дає організаціям можливість зберігати результати, виявлені сканером BSP, разом із даними, виявленими Qualys WAS [16].

Bugcrowd Findings

Якщо використовується набір інструментів Bugcrowd для тестування веб-застосунків, можна керувати висновками сканера Bugcrowd в обліковому записі WAS. Інтеграція з Bugcrowd Suite дає можливість зберігати результати, виявлені сканером Bugcrowd Suite, разом з даними, виявленими WAS, і ділитися цією інформацією з кількома користувачами [17].

3.3. Рекомендації щодо захисту веб-додатків в інформаційній системі

Безпека веб-додатків є важливим аспектом, якому необхідно приділяти пріоритетну увагу та оновлювати його, щоб захистити програму від нових та існуючих загроз. Впровадження стандартів безпеки та безпечних методів має вирішальне значення для забезпечення загального захисту конфіденційних та особистих даних. Розгорнувши відповідні стратегії безпеки веб-додатків, можна:

– Запобігти доступу зловмисників до конфіденційної інформації/даним.

– Мінімізуйте втрати, які сталися через погані стандарти безпеки.

– Виявляйте вразливості та інші фактори загрози на ранній стадії, що призводить до мінімальної шкоди або її повної відсутності.

– Встановіть стандарти відповідності для підвищення довіри клієнтів та залучення партнерів, акціонерів та потенційних інвесторів.

Організації можуть найняти спеціалістів з безпеки веб-додатків або тестувальників проникнення веб-додатків для перевірки та оновлення методів та стратегій безпеки. Проведення оцінки вразливості з використанням тих самих методів, які зловмисники використовують для експлуатації веб-застосунків, є найбільш ефективним способом виявлення проломів у безпеці в інфраструктурі веб-додатків. Це дозволяє фахівцям з безпеки аналізувати уразливості та інші лазівки у веб-додатку. Крім того, на основі отриманих даних та рівня загрози вразливості класифікуються разом з методами, які можна використовувати для їх усунення. Після виявлення та класифікації вразливостей можна впровадити стратегії та політики безпеки для їх усунення.

Прямий спосіб захисту програм - міжмережевий екран або брандмауер. Для більшої кількості веб-застосунків застосовується прикладний мережевий екран Web Application Firewall (WAF) та сканер вразливостей (WAS).

Застосування спеціалізованих рішень з інформаційної безпеки дозволяє виявити та запобігти атакам на прикладному та мережному рівні та реалізувати комплекс заходів, щоб забезпечити доступність та безперервність роботи web-додатків за рахунок захисту від різних класів атак.

Міжмережевий екран автоматично виявляє та блокує атаки на веб-програми та визначає нелегітимних користувачів, які намагаються проникнути у веб-програму.

До основних заходів відносяться:

– перевірка даних щодо відповідності стандартам протоколів;
– контроль трафіку на основі нейронних мереж;
– сигнатурний аналіз;
– захист від SQL-ін'єкцій;
– протекція від міжмережевого скриптингу (XSS);
– контроль доступу до конфіденційних даних.

Впровадження програмно-апаратних комплексів знижує ризики несанкціонованого доступу до критичної інформації та експлуатації вразливостей системного програмного забезпечення. Більше того, наявність спеціалізованих рішень щодо інформаційної безпеки дозволяє забезпечити законодавчі вимоги щодо захисту персональних даних.

Застосування спеціалізованих систем захисту web-додатків дозволить своєчасно виявляти та запобігати спробам несанкціонованих дій зловмисників як усередині організації, так і ззовні [15].

ВИСНОВКИ

В магістерській роботі було проаналізовано проблему захисту Web-ресурсів в інформаційній системі. Було виявлено, що число компаній, які використовують веб-технології для підвищення продуктивності роботи та залучення нових клієнтів, зростає з кожним роком. Безперечно, інтернет-сервіси несуть із собою безліч переваг, але є й зворотний бік медалі — зі зростанням числа додатків збільшується і кількість кіберзагроз. Так, компанія Symantec у своєму звіті Global Internet Security Threat Report (ISTR) вказує, що кіберзлочинці при зламі веб-сайтів зазвичай використовують уразливості веб-застосунків, що працюють на сервері, або експлуатують деякі вразливості операційної системи, на якій працюють ці програми. Наприклад, за допомогою атак типу XSS хакер може перенаправити запити користувачів на шкідливі веб-сторінки, а за допомогою SQL-ін'єкцій витягувати з баз даних сайту різну конфіденційну інформацію.

У відповідь на масові злами систем безпеки було створено консорціум OWASP - Open Web Application Security Project, це відкритий проект забезпечення безпеки веб-додатків. Однак і зловмисники, і фахівці в галузі кібербезпеки продовжують знаходити вразливості у веб-додатках, які можуть призвести до серйозних втрат з боку бізнесу.

Для запобігання атакам та зниження ризиків від можливих загроз необхідно застосовувати спеціальні технології та засоби захисту web-додатків. Аналіз показує, що забезпечення захисту має здійснюватися як на етапі проектування та розробки самого web-додатка, шляхом створення безпечного коду web-додатка та планування раціонального складу системи захисту, так і в процесі його експлуатації з внесенням у разі потреби своєчасних коригувань.

В магістерській роботі було проведено аналіз основних методів та засобів захисту веб-додатків. Виходячи з дослідження, захист пропонується будувати за такими напрямками:

– контроль за безпекою коду web-додатку протягом всього життєвого циклу розробки;

– забезпечення захисту інформації під час її передачі між комп'ютером клієнта та web-сервером;

- забезпечення захисту інформації збереженої на комп'ютері клієнта;

– використання спеціалізованих засобів захисту на рівні web-сервера.

Це досягається за рахунок застосування наступних засобів та методів захисту:

- недопущення помилок у скриптах при розробці web-додатків;

- сканування коду web-програми на наявність вразливостей та встановлення спеціальних водяних знаків;

- використання систем багатофакторної автентифікації користувачів (наприклад, парольна аутентифікація із секретним кодом, сертифікати, цифрові підписи, біометрична аутентифікація);

- застосування антивірусного програмного забезпечення;

- застосування спеціалізованих міжмережевих екранів рівня додатків, які мають вбудований функціонал запобігання вторгненням та забезпечують захист від цілеспрямованих web-атак, таких як переповнення буфера, SQL ін'єкції, Cross-Site-Scripting, зміна параметрів запитів та інших. Рішення цього класу фільтрують запити на доступ до програми та блокують усі дії, які не належать до дозволеної активності користувачів.

Всі ці заходи потрібно виконувати у комплексі, оскільки захист за окремістю не принесе бажаного ефекту.

ПЕРЕЛІК ПОСИЛАНЬ

1. The importance of application security: keeping your web apps safe [Електронний ресурс] – Режим доступу: https://outpost24.com/blog/The-importance-of-web-application-security-keeping-your-web-apps-safe

2. Web Application Architecture: The Latest Guide 2022 [Електронний ресурс] – Режим доступу: https://www.clickittech.com/devops/web-application-architecture/

3. Web Application Security [Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/application-security/web-application-security/

4. Web Application Security and Scanning: Explanation and Deep Dive [Електронний ресурс] – Режим доступу: https://www.rapid7.com/fundamentals/web-application-security/

5. OWASP Top 10 2021 [Електронний ресурс] – Режим доступу: https://www.synopsys.com/glossary/what-is-owasp-top-10.html

6. Prokhorenko V., Choo K.K. R., Ashman H. Web application protection techniques: A taxonomy // Journal of Network and Computer Applications. 2016. Vol. 60. P. 95–112.

7. OWASP Top Ten [Електронний ресурс] – Режим доступу: https://owasp.org/www-project-top-ten/

8. Qualys Web Application Firewall [Електронний ресурс] – Режим доступу:https://www.qualys.com/apps/web-app-firewall/

9. Qualys Web Application Scanning [Електронний ресурс] – Режим доступу: https://www.qualys.com/apps/web-app-scanning/

10. Qualys Cloud Platform [Електронний ресурс] – Режим доступу: https://www.qualys.com/cloud-platform/

11. Web Application Firewall Getting Started Guide - Qualys, Inc. [Електронний ресурс] – Режим доступу:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjj0O7TrvP7AhV7i_0HHTfBDqUQFnoECAsQAQ&url=https%3A%2F%2Fwww.qualys.com%2Fdocs%2Fqualys-waf-getting-started-guide.pdf&usg=AOvVaw2e0DV9pRkB1mPbeaK9czZc

12. Video Library: Web Application Firewall [Електронний ресурс] – Режим доступу: https://www.qualys.com/training/library/web-application-firewall/

13. Qualys Web Application Scanning Getting Started Guide [Електронний ресурс] – Режим доступу: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwicptaOr_P7AhWpif0HHVpbAqYQFnoECFwQAQ&url=https%3A%2F%2Fwww.qualys.com%2Fdocs%2Fqualys-was-getting-started-guide.pdf&usg=AOvVaw1eUKM3lrbyEeFXZ2haQjnd

14. Video Library: Web Application Scanning [Електронний ресурс] – Режим доступу: https://www.qualys.com/training/library/was/

15. What is Web Application Security? | Attacks & Best Practices [Електронний ресурс] – Режим доступу: https://www.eccouncil.org/what-is-web-application-security/

16. All About Burp Findings [Електронний ресурс] – Режим доступу: https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/index.htm#t=burp%2Fburp_management.htm

17. All about Bugcrowd Findings [Електронний ресурс] – Режим доступу: https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/index.htm#t=bugcrowd%2Fabout_bugcrowd.htm

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)