УДК 004.056.53

Р. А. Павлюк

"ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВЕБ-ДОДАТКІВ: ВИКЛИКИ ТА ЗАХОДИ ЗАХИСТУ"

Вінницький національний технічний університет

Анотація

У цій статті досліджується важливість безпеки веб-додатків у сучасному світі, де кіберзагрози стають все більшим викликом для користувачів та власників веб-ресурсів. Розглянуто основні види кіберзагроз, які можуть виникнути при недостатньому захисті веб-додатків та широкий спектр заходів і технологій, які можна використовувати для їх захисту.

Ключові слова: безпека, веб-додатки, кіберзагрози, ін'єкція SQL, WAF, захист, аналіз, дані, інформація, вразливості.

Abstract

This article explores the importance of web application security in today's world, where cyber threats are becoming an increasing challenge for users and owners of web resources. The main types of cyber threats that may arise in case of insufficient protection of web applications and a wide range of measures and technologies that can be used to protect them are considered.

Keywords: security, web applications, cyber threats, SQL injection, WAF, protection, analysis, data, information, vulnerabilities.

Вступ

Безпека веб-додатків - це продукти та політики, технології , спрямовані на захист веб-програм від різноманітних кіберзагроз і забезпечення їх безпеки та надійності за допомогою заходів [1].

У сучасному світі додатки стали невід'ємною частиною життя. Популярність веб-додатків робить їх привабливими цілями для кіберзлочинців. Недоліки в безпеці можуть призвести до витоку даних, крадіжки конфіденційних даних, втрати фінансових коштів та інших негативних наслідків для користувачів [1].

Результати дослідження

Веб-додатки можуть зіткнутися з різними типами атак залежно від цілей зловмисника, характеру роботи цільової організації та конкретних прогалин у безпеці програми.

Розглянемо основні види кіберзагроз, з якими стикається більшість веб-додатків:

1) Активні:
   – ін'єкція SQL;
   – міжсайтовий скриптинг (XSS або CSS);
   – «отруєння» cookie (cookie poisoning).
2) Пасивні:
   – прослуховування (Eavesdropping);
   – аналіз трафіку (Traffic Analysis).

Ін'єкція SQL – це експлойт безпеки, за якого зловмисник передає структуровану мову запитів (SQL) у формі запиту на дію через веб-форму безпосередньо до веб-програми, щоб отримати доступ до внутрішньої бази даних і/або даних програми [1].

Міжсайтовий скриптинг (XSS або CSS) — це атака веб-додатків, яка використовується для отримання доступу до приватної інформації шляхом доставки шкідливого коду кінцевим користувачам через надійні веб-сайти [1].

Cookie poisoning, також відоме як викрадення сесії – це стратегія атаки, за якої зловмисник змінює, підробляє, викрадає або іншим чином «отруює» файли cookie, які зберігаються на комп'ютері користувача, надісланий назад на сервер, для викрадення даних, обходу безпеки або обох [1].

Eavesdropping – це атака, при якій зловмисник перехоплює мережевий трафік між веб-сайтом та користувачами. Метою цієї атаки є зловживання конфіденційною інформацією, такою як паролі,

номери кредитних карт або особисті дані, які передаються між користувачем і сервером. Зловмисники можуть використовувати різні методи, такі як перехоплення незахищеного мережевого трафіку або використання програмних пристроїв для аналізу пакетів даних [2].

Traffic Analysis – це коли хтось аналізує трафік між вашим сайтом та користувачами, щоб визначити, хто вони, що вони роблять, як часто вони заходять на ваш сайт або якими ресурсами вони користуються [2].

Серед основних загроз на рівнях з використанням програмних вразливостей, зловмисники активно використовують фішингові інструменти, які побудовані на помилках людей. Сьогодні ми вже маємо змогу використовувати багато інструментів для захисту веб-додатків [3]. Один з основних, це – WAF.

WAF (Web Application Firewall) – це захисний екран рівня додатків, призначений для виявлення та блокування сучасних атак на веб-застосунки [4].

Основна робота WAF полягає в захисті веб-програм від несанкціонованого доступу, навіть за наявності критичних вразливостей [4].

Сучасний Web Application Firewall має відповідати певним вимогам:

– системні компоненти WAF мають відповідати вимогам PCI DSS;
– мати змогу реагувати на загрози, описані у OWASP Top Ten;
– інспектування повідомлень веб-сервісу, якщо веб-сервіс підключено до Інтернету (SOAP, XML);
– захист від загроз, спрямованих на WAF;
– підтримка SSL\TLS-термінації з'єднання;
– запобігання або виявлення підробки ідентифікатора сесії;
– автоматичне скачування оновлень сигнатур атак та застосування їх;
– можливість встановлення режиму fail-open та fail-close;
– підтримка пристроєм клієнтських SSL-сертифікатів;
– підтримка апаратного зберігання ключів (FIPS).

Перш за все WAF – це вузькоспеціалізований пристрій і він активно контролює тільки HTTP / HTTPS протоколи [3].

З часом WAF еволюціонував і з’явився WAAP (Web Application and API Protection), який пропонує більш просунуті автоматизовані механізми захисту для постійно змінних веб-додатків [4].

WAAP включає в себе сукупність методів та технологій, які використовуються для захисту веб-додатків та сервісів від атак та вразливостей [5].

Ще одним із популярних продуктів для захисту веб-додатків є FortiWeb від Fortinet. Система двостороннього захисту від впровадження коду [6]. Наприклад таких як SQL-ін'єкції, і міжсайтового скриптингу, яка дозволяє ефективно запобігати кібератакам, спрямованим на крадіжку даних, фінансові махінації та шпигунство. Використання власних технологій, таких як спеціалізовані процесори FortiASIC і операційна система FortiOS, дозволяє FortiWeb забезпечити високу продуктивність і оптимальний рівень безпеки. Використання FortiWeb є одним з найкращих рішень для захисту веб-додатків в компаніях середнього рівня та великих бізнесах [6].

Висновок

Безпека веб-сайтів є критично важливою в сучасному цифровому світі, особливо з урахуванням зростаючої кількості кіберзагроз, яка потребує постійної уваги та дій [2]. Загрози, які їм загрожують , а саме активні атаки, такі як ін’єкція SQL та XSS, і пасивні, такі як прослуховування та аналіз трафіку, можуть серйозно підірвати безпеку веб-додатків і викликати втрату даних, порушення конфіденційності та навіть пошкодження репутації організації. Для захисту від таких загроз використовують різні методи та технології, серед яких особливе місце використовують WAF (Web Application Firewall) та його просунута версія WAAP (Web Application and API Protection). Ці заходи допомагають забезпечити безпеку та надійність веб-додатків, захищаючи дані користувачів та організацій від кіберзагроз. Також зазначим, що продукт FortiWeb від Fortinet є ефективним рішенням для захисту веб-додатків в компаніях середнього рівня та великих бізнесів. Він забезпечує широкий спектр захисту та може бути корисним інструментом для зменшення ризиків кібератак і збереження надійності веб-додатків. Отже, використання таких продуктів та методів є важливою складовою стратегії інформаційної безпеки для будь-якої компанії чи організації, що має веб-присутність

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What Is Web Application Security?. *F5, Inc.* URL: https://www.f5.com/glossary/web-application-security (дата звернення: 03.05.2024).

2. Безпека Веб-Сайту: Загрози та Ефективні Заходи Захисту. *ONISTUDIO*. URL: https://www.onistudio.com.ua/bezpeka-veb-sajtiv/ (дата звернення: 04.05.2024).

3. Захист WEB-додатків. Чому це актуально? – Octava Capital. *Octava Capital*. URL: https://octavacapital.ua/zahyst-web-dodatkiv-chomu-ce-aktualno/ (дата звернення: 03.05.2024).

4. Сафонов Л. Web Application Firewall – захист сайта від хакерських атак. *Хабр*. URL: https://habr.com/articles/60590/ (дата звернення: 04.05.2024).

5. Web Application and API Protection (WAAP): еволюція WAF (Web Application Firewall). *MarkupUA*. URL: https://markup-ua.com/web-application-and-api-protection-waap-evolyuciya-waf-web-application-firewall/ (дата звернення: 05.05.2024).

6. Захист веб-додатків: чому це важливо? – Компанія ITBIZ. *Компанія ITBIZ*. URL: https://itbiz.ua/statti-ta-obzori/zaxist-veb-dodatkiv-chomu-ce-vazhlivo/ (дата звернення: 05.05.2024).

Павлюк Роман Андрійович – студент групи 1БС-22б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: roman.zirnij@gmail.com

Pavlyuk Roman Andriyovych – student of group 1BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: roman.zirnij@gmail.com