Сучасні методи захисту веб-сайту

https://doi.org/10.31713/MCIT.2024.059

Кирило Курчак
Національний університет водного господарства та природокористування
м. Рівне, Україна
kurchak_ak21@nuwm.edu.ua

Вікторія Рейнська
Національний університет водного господарства та природокористування
м. Рівне, Україна
v.b.reinska@nuwm.edu.ua

Аннотація **– З кожним роком, зростає кількість організацій, які використовують та створюють власні веб-сайті, а також кількість користувачів, які взаємодіють з ними. Разом із цим, збільшується і кількість кіберзлочинців, так званих хакерів, які діють самостійно або в складі організованих груп. У даній статті проаналізовано основні типи атак, які використовують кіберзлочинці, для витягування даних з веб-сайтів. Наведено сучасні методі, які використовуються для захисту веб-сайтів.**

Ключові-слова **– веб-сайт; веб-ресурс; вразливість веб-сторінки; кіберзагроза; кіберзлочинність; методи захисту веб-сайтів;програми для захисту веб-сайтів;скайнери для захисту веб-сайтів;**

I. Вступ

У сучасному цифровому світі Інтернет став фундаментом багатьох сфер життя — від бізнесу і освіти, до розваг і соціальних взаємодій. Щороку збільшується кількість веб-ресурсів, що надають користувачам широкий спектр послуг, але разом із цим зростає і ризик кіберзагроз. Веб-сайти стають мішенню для хакерів, які використовують вразливості у системах безпеки для викрадення конфіденційної інформації, шантажу, поширення шкідливого програмного забезпечення та дестабілізації роботи веб-сайтів.

Сучасні кіберзлочинці вдосконалюються свої методи атак, шукаючи нові шляхи для порушення нормальної роботи сайтів і викрадення даних. У цьому контексті компанії та власники веб-сайтів змушені не тільки слідкувати за розвитком загроз, але й впроваджувати комплексні заходи безпеки. Це включає постійний моніторинг вразливостей, своєчасні оновлення систем та використання програмних рішень для забезпечення захищеності веб-ресурсів, що є життєво важливим у боротьбі з кіберзлочинністю.

II. Мета статті

Метою даної статті є аналіз найпоширеніших кіберзагроз, що впливають на безпеку веб-сайтів, а також розгляд сучасних методів їх захисту. У статті буде представлено перелік розповсюджених атак на веб-ресурси, роз’язснено механізми їх впливу на функціонування сайтів, а також запропоновано ефективні інструменти та методі для перевірки і підвищення рівне безпеки веб-сторінок.

III. Виклад основного матеріалу

Відповідно до досліджень OWASP (Open Web Application Security Project), організації, яка займається підвищенням безпеки веб-додатків на глобальному рівні, було складено ключові загрози для безпеки веб-сайтів, які використовують вразливості у системах безпеки для викрадення конфіденційної інформації, шантажу, поширення шкідливого програмного забезпечення та дестабілізації роботи веб-сайтів [1].

- Недостатній контроль доступу (Broken Access Control): ця вразливість виникає, коли веб-додатки не належним чином перевіряють, чи має користувач права на доступ до певних ресурсів або функцій. Це може дозволити зловмисникам отримати доступ до конфіденційної інформації, модифікувати дані чи виконувати дії від імені інших користувачів. Відповідно до [1], ця проблема підкреслює важливість надійних механізмів автентифікації та авторизації.

- Криптографічні помилки (Cryptographic Failures): ця загроза пов'язана з невірним використанням або налаштуванням криптографічних методів. Наприклад, нешифроване зберігання паролів або використання застарілих алгоритмів шифрування можуть призвести до витоку чутливих даних. Це підкреслює важливість використання сучасних криптографічних стандартів та регулярного оновлення механізмів безпеки [1].

- Ін'єкції (Injection): атаки типу ін'єкцій, такі як SQL-ін'єкції, XSS (Cross-Site Scripting) та Command Injection, відбуваються, коли зловмисник вставляє шкідливий код або команди в запити до бази даних. Це може призвести до викрадення даних, модифікації бази даних чи виконання небезпечних команд на сервері. За інформацією з [1], ці атаки є одними з найпоширеніших і небезпечних, тому

важливо вживати заходів для запобігання їм.

- Небезпечний дизайн (Insecure Design): ця загроза виникає, коли в процесі розробки веб-додатків не враховуються принципи безпеки, що призводить до недоліків у проектуванні системи. Відсутність правильної моделі загроз або недостатня увага до принципів безпеки може зробити систему уразливою до атак.

- Неправильна конфігурація безпеки (Security Misconfiguration): Ця уразливість виникає, коли система не налаштована належним чином, що може дозволити зловмисникам отримати доступ до чутливих даних або функцій. Наприклад, якщо сервери залишаються з налаштуваннями за замовчуванням або недостатньо захищені, це робить їх мішенню для атак. Як зазначається в [2], що навіть невеликі помилки конфігурації можуть призвести до серйозних наслідків, таких як витік даних або недоступність веб-додатків..

- Вразливі та застарілі компоненти (Vulnerable and Outdated Components): використання застарілого програмного забезпечення та бібліотек, які містять відомі вразливості, є серйозною загрозою безпеці. Наприклад, незахищені плагіни або старі версії фреймворків можуть стати мішенню для атак.

- Серверні запити (Server-Side Request Forgery): Ця атака дозволяє зловмисникам змусити сервер відправляти запити до небезпечних адрес, що може призвести до витоку даних або компрометації системи. У [3] наведено приклади, як цей тип атаки може вплинути на безпеку веб-додатків.

- Невідповідний моніторинг і ведення журналів (Security Logging and Monitoring Failures): Неналежний моніторинг може завадити своєчасному виявленню загроз та інцидентів безпеки, що може призвести до серйозних наслідків, включаючи довготривалу компрометацію системи. Якщо система не веде адекватні журнали безпеки, зловмисники можуть діяти безкарно. У [4] зазначається, що слабке ведення журналів часто стає причиною того, що інциденти не виявляються вчасно, що дає хакерам більше можливостей для атаки.

- Проблеми з ідентифікацією та автентифікацією (Identification and Authentication Failures): Ці вразливості виникають, коли системи не належать достатньо надійні механізми перевірки особи користувачів, що дозволяє зловмисникам отримувати доступ до захищених ресурсів. Наприклад, слабкі паролі, відсутність двофакторної аутентифікації або неправильне управління сесіями можуть призвести до несанкціонованого доступу. Як вказується в [5], усунення таких вразливостей є критично важливим для забезпечення безпеки веб-додатків.

- Помилки цілісності програмного забезпечення та даних (Software and Data Integrity Failures): Ці вразливості пов’язані з припущеннями щодо цілісності програмних оновлень, критичних даних і процесів безперервної інтеграції/безперервної доставки (CI/CD). Якщо оновлення або дані не перевіряються на цілісність, зловмисники можуть маніпулювати ними, що призводить до серйозних наслідків. Як зазначається в [6], важливо впроваджувати належні методи верифікації для забезпечення цілісності даних і програмного забезпечення.

Усі ці кіберзагрози можуть призвести до втрати чутливої інформації, що ставить під загрозу фінансову безпеку користувачів. Крім того, збої в роботі сайту можуть призвести до тимчасового закриття онлайн-магазинів чи блогів, що негативно вплине на доходи. Атаки можуть також спричинити фінансові санкції за недотримання стандартів безпеки, таких як PCI DSS. Важливим є також ризик потрапляння в чорний список пошукових систем, як-от Google, через наявність шкідливого коду на сайті, що може суттєво знизити видимість та трафік [7].

Всі ці фактори можуть серйозно зашкодити репутації бізнесу, адже навіть один інцидент може відштовхнути клієнтів і знизити довіру до бренду. Важливо усвідомлювати ці ризики та вживати заходів для їх запобігання, щоб зберегти безпеку та стабільність у цифровому середовищі[7].

Для захисту веб-ресурсів від зазначених загроз використовуються різні інструменти та методи, які допомагають ідентифікувати вразливості та запобігати атакам.

1) Використання SSL/HTPS

Використання SSL-сертифікатів для шифрування трафіку між користувачем і сервером є одним із основних засобів захисту. Це допомагає захистити конфіденційні дані, такі як паролі та фінансова інформація, від перехоплення. Багато компаній, зокрема Cloudflare, пропонують рішення для забезпечення HTTPS, що робить його доступним для власників веб-сайтів.[8]

2) Web Application Firewalls (WAF)

Міжмережний екран (він же брандмауер чи фаєрвол) — це захисний механізм, що моніторить та фільтрує HTTP-запити, блокуючи підозрілі дії. Це дозволяє захистити веб-додатки від атак, таких як ін'єкції та XSS. Платформи, як-от Cloudflare, надають послуги WAF, щоб захистити веб-сайти від численних загроз [8].

3) Сканери безпеки

Спеціалізовані сканери безпеки дозволяють виявляти вразливості на веб-сайтах, автоматично перевіряючи код на предмет наявності помилок або шкідливого програмного забезпечення. Наприклад, такі інструменти, як Sucuri та SiteLock, можна використовувати для регулярного моніторингу безпеки, що дозволяє оперативно виявляти потенційні загрози. [9,10]

4) Своєвчасні оновлення програмного забезпеченн

Регулярне оновлення всіх компонентів веб-сайту, таких як бібліотеки, плагіни та основне програмне забезпечення, є критично важливим для забезпечення безпеки. Застаріле програмне забезпечення часто містить вище згадані вразливості, які зловмисники можуть використовувати для атак. Коли виробники випускають оновлення, вони зазвичай усувають ці вразливості та впроваджують нові функції, що підвищують загальний рівень захисту

5) Двохфакторна автентифіцкація (2FA)

Двофакторна автентифікація забезпечує додатковий рівень захисту, вимагаючи від користувачів не лише введення пароля, а й підтвердження своєї особи за допомогою другого фактора, наприклад, коду, надісланого на мобільний телефон. Даний метод як можна впровадити свій сайт через написання коду, так і через використання таких сервісів, як Duo Security [11]

6) Резервне копіювання даних

Регулярне резервне копіювання інформації дозволяє відновити дані в разі втрати або атаки. Це важливий крок для запобігання втратам важливої інформації. Один зі способів впровадження цього методу — використання автоматизованих систем резервного копіювання, такі як Idrive, Backblaze, які регулярно зберігають копії даних на віддалених серверах або в хмарі. Це забезпечує надійний захист, оскільки дані не зберігаються на одному пристрої і можуть бути легко відновлені. Інший спосіб — зберігання резервних копій на фізичних носіях, таких як зовнішні жорсткі диски або USB-накопичувачі. Цей метод дає змогу мати фізичну копію даних, що може бути корисним у випадку збою системи або кібератаки, яка заважає доступу до основних даних. [12,13]

IV. Висновок

У сучасному цифровому світі захист веб-сайтів від кібератак є критично важливим для забезпечення безпеки особистої інформації та підтримки бізнес-процесів. Виявлені загрози, такі як ін'єкції, атаки честарез конфігурації, фальшиві аутентифікації та інші, можуть призвести до серйозних наслідків, включаючи втрату чутливої інформації, фінансові втрати і шкоду репутації. Впровадження ефективних заходів безпеки, таких як своєчасне оновлення програмного забезпечення, резервне копіювання даних, використання надійних паролів та шифрування, є необхідним кроком для мінімізації ризиків.

Успішна реалізація методів, які наведено в статті дозволяє не лише запобігти можливим атакам, а й забезпечити безперервність бізнес-процесів. Сьогодні важливо не лише реагувати на загрози, але й проактивно підходити до кібер-безпеки, щоб захистити веб-ресурси від потенційних ризиків у майбутньому.

Література

[1] OWASP Top Ten : веб-сайт. URL:https://owasp.org/Top10/ (дата звернення 14.10.2024).

[2] What Is Security Misconfiguration? : веб-сайт. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/security-misconfiguration/ (дата звернення: 14.10.2024).

[3] SSRF (Server-Side Request Forgery) : веб-сайт. URL: https://cqr.company/ua/web-vulnerabilities/ssrf/. (дата звернення 14.10.2024).

[4] Risk of Security and Monitoring Logging Failures : веб-сайт. URL: https://www.softwaresecured.com/post/risk-of-security-and-monitoring-logging-failures (дата звернення 14.10.2024).

[5] Intro to Identification and Authentication Failures : веб-сайт. URL: https://www.softwaresecured.com/post/intro-to-identification-and-authentication-failures (дата звернення 14.10.2024).

[6] Software and Data Integrity Failures: Explanation, Examples, Prevention : веб-сайт: URL: https://qawerk.com/blog/software-and-data-integrity-failures/ (дата звернення 14.10.2024).

[7] How to Make a Website Secure with 9 Quick Tips: веб-сайт. URL: https://www.sitelock.com/blog/building-a-secure-website/ (дата звернення 14.10.2024)

[8] Cloudflare: Connect, Protect and Build Everywhere : веб-сайт. URL: https://www.cloudflare.com (дата звернення 14.10.2024)

[9] Sucuri - Complete Website Security, Protection & Monitoring… : веб-сайт. URL: https://sucuri.net/ (дата звернення 14.10.2024).

[10] SiteLock: Website Security Monitoring & Malware Protection : веб-сайт. URL: https://www.sitelock.com/ (дата звернення 14.10.2024).

[11] Duo Security: Identity Security, MFA & SSO : веб-сайт. URL: https://duo.com/ (дата звернення 14.10.2024).

[12] IDrive : веб-сайт. URL: https://www.idrive.com/ (дата звернення 14.10.2024).

[13] Backblaze: The Leading Open Cloud Storage Platform : веб-сайт. URL: https://www.backblaze.com/ (дата звернення 14.10.2024).