Ключевые слова: аутентификация, криптографический протокол, решетчатая криптосистема, алгебраическая структура полиномиального кольца, шифрование.

Ключові слова: автентифікація, криптографічний протокол, решітчаста криптосистема, алгебраїчна структура поліноміального кільця, шифрування.

Keywords: authentication, cryptographic protocol, lattice cryptosystem, algebraic structure of a polynomial ring, encryption.

Толокнов Анатолій Арнольдович
Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій

ОГЛЯД І КЛАСИФІКАЦІЯ ОСНОВНИХ ПОГРОЗ WEB-ЗАСТОСУНКІВ

З ростом кількості та значення різних веб-сервісів в суспільному житті, наприклад, таких як банківські послуги, покупка товарів он-лайн та ін., також зростає значення забезпечення їх безпеки. Ефективність забезпечення безпеки може зростати якщо знати звідки чекати загрози. Попереджений – значить озброєний – прислів'я, зміст якого полягає в тому, що будучи попереджений про близьку небезпеку (або можливість такої), людина тепер до неї підготовлена і може з нею впоратися. Це в рівній мірі відноситься і до web-застосунків.

У даному невеликому огляді ми розглянемо основні загрози web-застосунків, а також наведемо приклади їх класифікації.

Повний список загроз безпеки веб-сайтів можна розглянути в розділі «Категорія: атаки» (Open Web Application Security Project) [1]. Також проект OWASP представляє стандартизований список топ 10 основних загроз web-застосунків, які повинні братися до уваги розробниками, перш ніж приступати до створення web-застосунків [2].

Крім цього Консорціум безпеки web-застосунків (WASC), www.webappsec.org, міжнародна організація, що об'єднує професіоналів в області безпеки web-застосунків, випустила

документ Threat Classification v2.0, що представляє собою класифікацію вразливостей і атак, які можуть завдати шкоди веб-сайту, інформації, яка ним обробляється або його користувачам [3]. Документ, в першу чергу, буде корисний для фахівців в області безпеки web-застосунків як довідкове керівництво.

З точки зору забезпечення безпеки інформації, що циркулює в автоматизованих (комп'ютерних) системах, вказуються такі важливі властивості інформації: конфіденційність, цілісність, доступність [4].

Зазначені властивості інформації є базовими для побудови будь-якої системи захисту інформації, незалежно від виду і характеристик об'єкта інформатизації.

Конфіденційність (*information confidentiality*) – суб'єктивно визначена властивість інформації, яка вказує на необхідність введення обмежень на коло суб'єктів, що мають доступ до неї. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила її отримання або ознайомлення з нею.

Цілісність (*information integrity*) – властивість інформації, яка полягає в її існуванні в незмінному вигляді на певному проміжку часу. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації та/або видалення.

Доступність (*information availability*) – властивість інформації бути наданою своєчасно і безперешкодно всім суб'єктам, які мають для цього належні повноваження. Інформація зберігає доступність, якщо протягом певного проміжку часу легітимним (авторизованим) користувачам немає відмови (блокування) в її отриманні.

У [5] пропонується наступна класифікація загроз безпеки web-застосунків:

1. Загрози, пов'язані з експлуатацією вразливостей в коді web-застосунка:
    a. SQL-ін'єкції
    b. XSS атаки
    c. PHP-ін'єкції
    d. Підробка міжсайтових запитів – CSRF

2. Мережеві атаки
    a. Атаки на браузер клієнта web-застосунка
    b. Перебір паролів і атаки на систему аутентифікації користувачів
    c. Відмова в обслуговуванні сервісів web-застосунків
    d. Сканування мережі
    e. Виклик виняткових ситуацій
3. Загрози випадкового характеру
    a. Збої і відмови програмно-апаратних засобів
    b. Стихійні лиха
4. Шахрайство
    a. Спам-розсилки
    b. Фішинг
    c. Відмова від зобов'язань у вчинених діях
    d. Порушення авторського права

Ось деякі з основних загроз для web-застосунків [6]:

XSS (Cross-Site Scripting – Міжсайтовий скриптинг) це термін, який використовується для опису типу атак, які дозволяють зловмисникові впроваджувати шкідливий код через веб-сайт в браузери інших користувачів. Оскільки впроваджений код надходить в браузер з сайту, він є довіреним і може виконувати такі дії, як відправка авторизаційного файлу cookie користувача зловмисникові. Коли у зловмисника є файл cookie, він може увійти на сайт, нібито б він був користувачем, і зробити все, що може користувач, наприклад, отримати доступ до даних кредитної картки, переглянути контактні дані або змінити пароль.

SQL-ін'єкції дозволяють зловмисникам виконувати довільний код SQL в базі даних, дозволяючи отримувати, змінювати або видаляти дані незалежно від дозволів користувача. Успішна ін'єкційна атака може підробити посвідчення, створити нові посвідчення з правами адміністратора, отримати доступ до всіх даних на сервері або знищити / змінити дані, щоб зробити їх непридатними для використання.

Підробка міжсайтових запитів (Cross-Site Request Forgery – CSRF) дозволяють зловмиснику виконувати дії,

використовуючи облікові дані іншого користувача, без його відома або згоди.

Інші поширені атаки / уразливості включають:

Clickjacking. У цій атаці зловмисник перехоплює кліки, призначені для видимого сайту верхнього рівня, і направляє їх на приховану нижче сторінку. Цей метод можна використовувати, наприклад, для відображення законного сайту банку, але захоплення облікових даних для входу в невидимий <iframe>, контрольований зловмисником.

Відмова в обслуговуванні (DoS) – зазвичай досягається за рахунок наповнення цільового сайту підробленими запитами, так що доступ до сайту порушується для законних користувачів. Запити можуть бути просто численними або окремо споживати великі обсяги ресурсів (наприклад, повільне читання або завантаження великих файлів).

Обхід каталогів (файл і розкриття). У цій атаці зловмисник намагається отримати доступ до частин файлової системи веб-сервера, до яких у нього не повинно бути доступу.

Включення файлу. У цій атаці користувач може вказати «ненавмисний» файл для відображення або виконання в даних, переданих на сервер.

Впровадження команд. Атаки з впровадженням команд дозволяють зловмиснику виконувати довільні системні команди в операційній системі сервера.

7 найпоширеніших типів кібератак на web-застосунки у 2020 році [7]:

1. атака з використанням SQL-ін'єкції,
2. атака міжсайтового скриптинга (XSS),
3. атака типу відмова в обслуговуванні (DoS) / розподілена відмова в обслуговуванні (DDoS),
4. атака впровадження команд ОС,
5. атака з використанням LDAP-ін'єкції (Lightweight Directory Access Protocol – Полегшений протокол доступу до каталогів),
6. атака грубої сили (brute force attack),
7. атака нульового дня.

Необхідно не забувати про дотримання базових заходів безпеки при розробці та підтримці роботи сайту: оновлювати CMS і її компоненти; регулярно міняти паролі; відмовитися від використання застарілих протоколів; налаштувати і використовувати HTTPS/HSTS.

Список використаних джерел:

1. List of Attacks / Open Web Application Security Project. [Електронний ресурс] URL: https://owasp.org/www-community/attacks/ (дата звернення: 8.11.2020).

2. Top 10 Web Application Security Risks / Open Web Application Security Project. [Електронний ресурс] URL: https://owasp.org/www-project-top-ten/ (дата звернення: 8.11.2020).

3. The WASC Threat Classification v2.0 / The Web Application Security Consortium. [Електронний ресурс] URL: http://projects.webappsec.org/w/page/13246978/Threat%20Classification (дата звернення: 8.11.2020)

4. Емельянов С. Л. Проблема защиты информации от утечки и пути ее решения: моногр. / С. Л. Емельянов. – Одесса: Фенікс, 2011. – С. 18.

5. Оладько В. С., Микова С. Ю., Нестеренко М. А. Технологии защиты интернет-технологий и web-приложений / *Международный научный журнал*, № 8, 2015. С. 81–85.

6. Веб-безопасность / MDN Web docs. [Електронний ресурс] URL: https://developer.mozilla.org/ru/docs/Learn/Server-side/First_steps/%D0%92%D0%B5%D0%B1_%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C (дата звернення: 8.11.2020)

7. Top 7 Most Common Types of Cyberattacks on Web Applications in 2020 / Penta Security, 2020–03–19 [Електронний ресурс] URL: https://www.pentasecurity.com/blog/top-7-common-types-cyberattacks-web-applications/ (дата звернення: 8.11.2020)

Ключові слова: інформаційна безпека, інтернет, загрози й атаки на web-застосунки.

Ключевые слова: информационная безопасность, интернет, угрозы и атаки на web-приложения.

Keywords: information security, internet, threats and attacks on web applications.