УДК 004.056

В.К. Бондарчук
Л.М. Куперштейн

АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ

Вінницький національний технічний університет

Анотація

Досліджено та проаналізовано основні вразливості та загрози веб-додатків, що призводять до витоку приватних та конфіденційних даних. Доведено необхідність захисту ВЕБ-додатків.

Ключові слова: веб-додаток, вразливість, загроза.

Abstract

The basic vulnerabilities and threats of web applications that leak private and sensitive data are explored and analyzed. The need to protect web applications is proved.

Keywords: web-application, threat, vulnerability

Вступ

Розвиток глобальної мережі Інтернет і збільшення доступності до ресурсів у ній, призвело до розширення спектра задач, що вирішуються з використанням WEB-технологій. В зв'язку з цим, отримав поширення особливий вид додатків — WEB-додатків, від яких залежить функціонування бізнес-процесів багатьох організацій.

Завдання, які вирішують ВЕБ-додатки:

- зберігання даних;
- обмін інформацією;
- статистика;
- продаж\купівля;
- електронний документообіг.

Хакери охоче приглядаються до державних цілей. Міністерства, відомства та уряди постійно наражаються на небезпеку складних цілеспрямованих атак. Деякі злочинні угруповання, які намагаються вкрасти гроші, роблять це шляхом нападу на уряди. Так у третьому кварталі 2019 року PT ESC виявив фішинг-розсилання TA505 до державних структур Південної Кореї, Китаю, Канади та Великобританії.

Дані, на які найбільше спрямовані атаки, зображені на рисунку 1 [1].

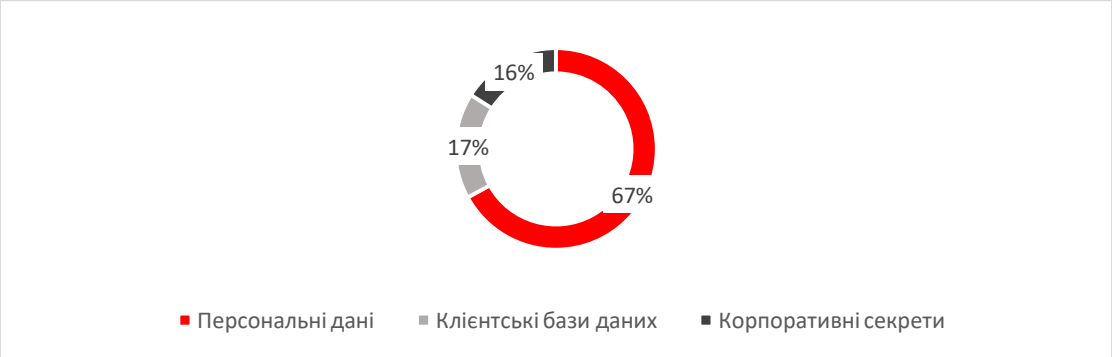

Рисунок 1 – Об’єкти атак

Результати дослідження

WEB-додаток — це клієнт-серверний додаток, де в якості клієнта виступає браузер, який відображає користувацький інтерфейс, формує запити до сервера і опрацьовує відповіді від нього. А серверна частина являє собою WEB-сервер, обробник запитів клієнтів. Взаємодія між клієнтом і сервером, як правило, реалізовується за допомогою протокола HTTP.

Статистика реалізованих загроз веб-додатків у 2019 р наведена на рис. 2 [2].

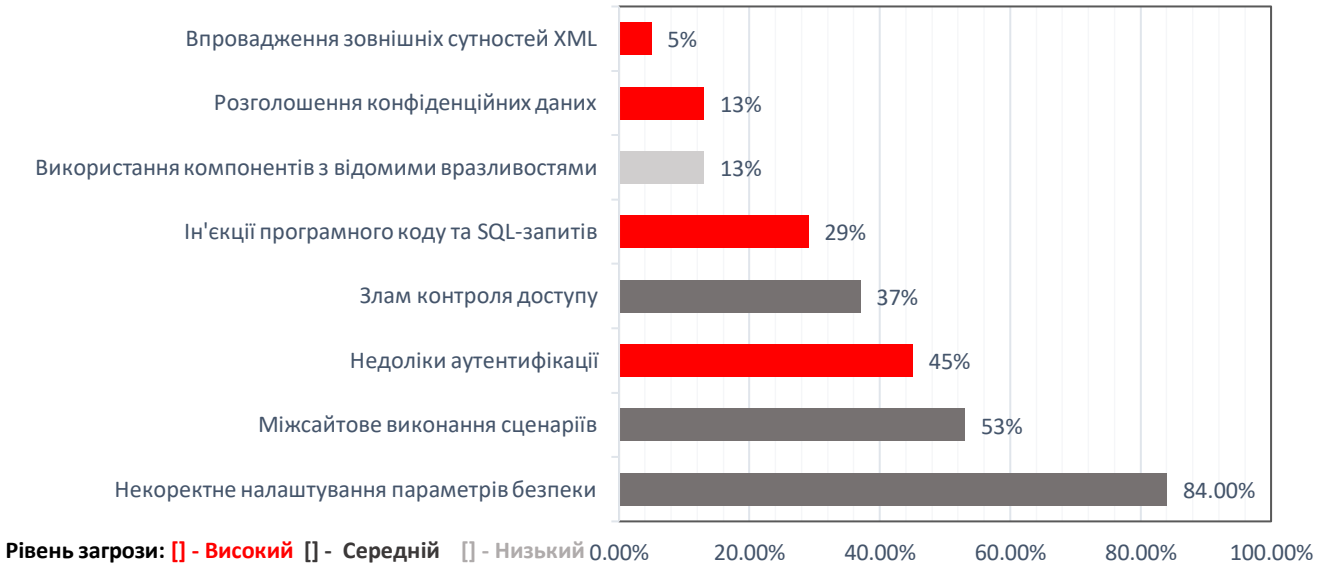

Рисунок 2 – Атаки зі списку OWASP Top 10 – 2019

Ін’єкція програмного коду та SQL-запитів(SQL and code injection) – складається з вставки або впровадження SQL-запита через вхідні дані від клієнта до додатка. Успішний SQL-експлойт може зчитувати конфіденційні дані та змінювати їх, виконувати операції адміністрування базі даних. Є дуже поширеними в додатках PHP і ASP через наявних старих функціональних інтерфейсів[4].

Необхідність реалізації захисту від даної загрози полягає у тому, щоб уникнути втрати важливих даних що зберігаються у базі даних та попередити виконання вставленого програмного коду.

Недоліки аунтентифікації (Broken Authentication) – трапляється в основному через погану реалізацію функцій додатків, пов’язаних з аутентифікацією та керуванням сеансом, що дозволяє зловмисникам компрометувати паролі, ключі або маркери сеансу, навіть заходячи так далеко, щоб використовувати інші недоліки впровадження, щоб припустити особистість користувачів тимчасово або назавжди. Цей вид атаки досить легко здійснити, оскільки хакери можуть використовувати декілька прийомів, таких як варіанти перебору паролів грубої сили, включаючи атаки на основі словника або навіть заповнення даних (автоматизована ін'єкція раніше порушених/ загальнодоступних пар імені користувача / пароля, не обов'язково пов'язані з поточною ціллю, щоб шахрайським шляхом отримати доступ до облікових записів користувачів).[2, 5]

Необхідність реалізації захисту від даної загрози полягає у тому, щоб уникнути можливості отримання доступу до чужого облікового запису.

Використання незахищених протоколів (Sensitive Data Exposure) – багато додатків не використовують механізм для захисту переданих даних, таких, як використання протоколу HTTPS. Наприклад додаток шифрує номери кредитних карт у базі даних за допомогою автоматичного шифрування бази даних. Однак ці дані автоматично розшифровуються при

отриманні, що дозволяє хакерові при використанні SQL ін’єкції отримати ці дані у розшифрованому вигляді.[2, 5]

Необхідність реалізації захисту від даної загроз полягає у тому, щоб уникнути отримання важливих та конфіденційних даних зловмисником.

Впровадження зовнішніх сутностей XML (XML External Entity Injection) - вид ін'єкції, заснований на впровадженні в XML-запит до сервера атрибутів і сутностей, що дозволяють отримати неавторизований доступ до даних. Наприклад, коли в XML запит вказують зовнішній файл, який знаходиться на сервері.

Необхідність реалізації захисту від даної загрози полягає у тому, щоб уникнути отримання серверних файлів зловмисником.

Злам контролю доступу (Broken Access Control) – вразливість в методах авторизації, яка дозволяє порушнику отримати підвищені привілеї у додаткові. Один конкретний тип проблеми контролю доступу - це адміністративні інтерфейси, які дозволяють адміністраторам сайтів керувати сайтом через Інтернет. Такі функції часто використовуються, щоб дозволити адміністраторам сайтів ефективно керувати користувачами, даними та вмістом на своєму сайті.[2, 5]

Необхідність реалазації захисту від даної загрози полягає у тому, щоб уникнути отримання прав вищого рівня у ВЕБ-додаткові.

Некоректне налаштування параметрів безпеки (Security Misconfiguration) - WEB-додаток - це складна система, що складається з багатьох компонентів, таких як WEB-сервер, СУБД та ін. Невірна конфігурація одного з компонентів може призвести до серйозних проблем з безпекою всього додатку [2]. Необхідність реалізації захисту від даної загрози полягає у тому, щоб уникнути втрати важливих даних.

Міжсайтове виконання сценаріїв (XSS) - ін'єкція шкідливого коду в HTTP-відповідь, що отримується клієнтом і виконується на стороні клієнта. Існує два типи XSS атак - пасивна та активна. Активна атак має більшу небезпеку, з точки зору зловмисника немає необхідності заманити жертву за спеціальним посиланням, йому достатньо вставити шкідливий код в базу даних або у якийсь файл, що знаходиться на сервері. Таким чином, всі, хто відвідує сайт автоматично стають жертвами [2].

Необхідність реалізації захисту від даної загрози полягає у тому, щоб уникнути отримання захищених даних зловмисником.

Відсутність валідації даних (Insecure Deserialization) – десеріалізація перетворює послідовність біт в структуровані дані, найчастіше на даному етапі не приділяється достатньо уваги безпеці, наприклад, відсутня валідація типів даних, що призводить до їх підміні.[2, 5]

Необхідність реалізації захисту від даної загрози полягає у тому, щоб уникнути отримання некоректних даних та збереження некоректних сутностей у базі даних.

Розголошення конфіденційних даних призводить до отримання зловмисником секретних даних, таких як пароль та логін адміна, інформації про присутні баги у додаткові.

Необхідність реалізаціях захисту від даної загрози, щоб уникнути розголошення конфіденційної, секретної інформації про розробку додатку.

Висновки

В даній роботі було досліджено та проаналізовано найпопулярніші вразливості та загрози ВЕБ-додатків. Наведено статистику даних на які найчастіше спрямовані атаки, відсоткове співвідношення частоти атак та загроз у ВЕБ-додатків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Web Applications vulnerabilities and threats: statistics for 2019 [Електронний ресурс] – Режим доступу: https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/

2. OWASP Top 10 Security Risks & Vulnerabilities [Електронний ресурс]. Режим доступу: https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/

3. Cybersecurity threatscape: Q3 2019 [Електронний ресурс] – Режим доступу: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q3/

4. Voitovych, O. P., O. S. Yuvkovetskyi, and L. M. Kupershtein. "SQL injection prevention system." 2016 International Conference Radio Electronics & Info Communications (UkrMiCo). IEEE, 2016 [Електронний ресурс] – Режим доступу: https://ir.lib.vntu.edu.ua/bitstream/handle/ 123456789/ 27968/45nigxju2tpe63tv5iy6aa8jor5pguaiic.pdf?sequence=1&isAllowed=y

5. Securing web applications: top OWASP threats and what to do about them [Електронний ресурс]- Режим доступу: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/securing-web-applications-top-owasp-threats-and-what-to-do-about-them/

6. Rich Cannings, Himanshu Dwivedi, Zane Lackey., Hacking Exposed Web 2.0: Web 2.0 Security Secrets and Solutions/ Rich Cannings, Himanshu Dwivedi, Zane Lackey // McGraw-Hill Education; December 2007

Бондарчук Вячеслав Костянтинович – студент групи 1БС-18мс, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: slava.777.bondarchuk@outlook.com

Куперштейн Леонід Михайлович – доцент кафедри захисту інформації, Вінницький національний технічний університет, м.Вінниця

Bondarchuk Viacheslav K. - student of group 1CS-18 junior specialist, Faculty of Information Technologies and Computer Engineering, National University of Ukraine, Vinnitsa, e-mail: slava.777.bondarchuk@outlook.com

Supervisor: **Kuperstein Leonid M**. - Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia