УДК 004.7:004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.066

# ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВІД ВИТОКІВ ІНФОРМАЦІЇ ЧЕРЕЗ МЕТАДАНІ РЕСУРСІВ WEB-ДОДАТКІВ

Качан В.Є.
Науковий керівник – к.т.н., ст. викл. каф. Марчук А.В.
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Науки, 14, кафедра ІКІ імені В.В. Поповського, тел. +38(050) 702-55-92)
email: vadym.kachan@nure.ua, artem.marchuk@nure.ua

The work is aimed at considering the criticality of information leakage in files metadata. A vulnerable web application OWASP Juice Shop has been analyzed and a possible solution has been developed that removes this critical vulnerability.

У сучасному світі безпека веб-додатків постає одним з найвизначніших викликів безпеки, адже вони обслуговують значну кількість користувачів, що зростає щодня. Організація OWASP визначає 10 найрозповсюдженіших вразливостей веб-безпеки, що наявні в сучасних веб-додатках (OWASP Top 10) [1]. Ресурси OWASP, що пов’язані із OWASP Top 10 надають чіткий опис того, як використовується вразливість, із наданням прикладів та рекомендацій по її усуненню.

Однією із вразливостей, що впливають на конфіденційність у веб-додатках є витік інформації з метаданих файлів, особливо файлів, що завантажуються користувачами. Для проведення дослідження, яке показало б чіткий приклад та наслідки такого витоку, використовується тренувальний вразливий додаток OWASP Juice Shop, метою якого є навчання спеціалістів з кібербезпеки на прикладі різних вразливостей, що впроваджені в цей веб-додаток. Як зазначається на офіційній сторінці OWASP [2], даний вразливий додаток має в сумі 106 завдань, що стосується наступних категорій вразливостей:

- порушений контроль доступу;
- порушена автоматизація;
- порушена аутентифікація;
- вразливості в криптографії;
- неправильна обробка вхідних даних;
- ін’єкції;
- ненадійна десеріалізація;
- різні некласифіковані помилки (miscellaneous);
- неправильні налаштування безпеки;
- безпека за допомогою «затьмарення» (obscurity);
- розкриття конфіденційних даних;
- неперевірені переадресації;
- вразливі компоненти;

−міжсайтовий скриптинг;

−атака на зовнішню сутність XML.

В ході роботи було проаналізовано кожну вразливість в додатку, окрім тих, що визначені як жартівливі та тих, що стосуються розвідки OSINT. В категорії що стосується розкриття конфіденційних даних було виявлено вразливість, яка стосується витоку інформації через картинки, що завантажені користувачами. В конкретному прикладі додатка картинка користувача містила GPS-дані щодо місця, де було зроблено фото і це місце являло собою відповідь на секретне питання користувача, що дозволило отримати доступ до його акаунту шляхом скидання його паролю. Далі, за допомогою документації OWASP Top 10 та суміжних ресурсів OWASP, було визначено, що така документація не надає жодних пояснень або згадувань того, як виявляти та захищатись від подібного роду атак. Окремим чином було визначено, що документація інструменту OWASP ZAP [3], який є проксі-додатком для роботи з запитами, надає список оповіщень безпеки, до якого входить оповіщення «Зображення викриває локацію або приватні дані». Опис даного оповіщення визначає, що перед завантаженням або передачею картинок необхідно видалити з них критичну інформацію, що міститься в метаданих. Це передбачає повне видалення метаданих або лише GPS компоненти, та інших даних, таких як серійні номери.

Як було визначено, опис захисту від витоку інформації з метаданих ресурсів, що завантажуються в додаток, не чітко визначений в основних ресурсах, що надаються OWASP, лише наявний в документації їхнього програмного продукту. Незважаючи на це, такий витік становить критичну необхідність його усунення, адже зловмисник таким чином може без значних затрат скомпрометувати обліковий запис користувача. Через це, в рамках даної роботи запропоновано програмне рішення, яке є прикладом можливого впровадження відповідного функціоналу в реальний веб-додаток, в тому числі Juice Shop, який, однак, є комплексним та динамічним, і був створений командою OWASP та їхньою спільнотою, через що зазначений механізм обробки метаданих впроваджено локально в окремому вигляді.

Спочатку було створено локально сайт тільки із функціоналом завантаження файлів формату jpg/png та pdf, файли того ж формату можна завантажити і у додаток OWASP Juice Shop. На рисунку 1 зображено видалення метаданих картинки, після того як вона була завантажена. Було видалено конфіденційні дані GPS, а також переіменовано картинку випадковим чином, щоб у випадку, якщо зловмисник отримає до неї доступ, він не міг зробити висновок про те, чия це картинка/фотографія і ким вона була завантажена.

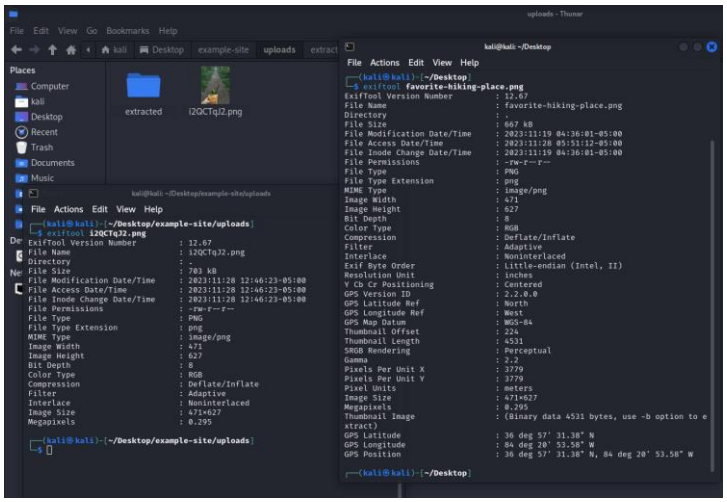

Рисунок 1 - Результат видалення метаданих картинки

Аналогічним чином виконується обробка файлу pdf – усі критичні метадані (наприклад, автор файлу і програма, де було створено файл) видаляються і файл зберігається із випадковим іменем.

**Висновок**.

В роботі виконано аналіз загальнодоступних ресурсів OWASP та вразливостей в OWASP Juice Shop і запропоновано впровадження можливого рішення для усунення витоку інформації користувача з веб-додатку із використанням метаданих файлів.

Критичність атаки, що досліджувалась, за шкалою оцінки CVSS [4] становить 7.3 і визначається як «висока» («high»). Таким чином, впровадження запропонованого рішення усуває високо критичну атаку.

Список використаних джерел:

1. Top 10 Web Application Security Risks. URL: https://owasp.org/www-project-top-ten/ (дата звернення 03.03.2024).

2. OWASP Juice Shop. URL: https://owasp.org/www-project-juice-shop/mage Expo.ses Location or Privacy (дата звернення 03.03.2024).

3 ZAP. Image Exposes Location or Privacy Data. URL: https://www.zaproxy.org/docs/alerts/10103/ (дата звернення 03.03.2024).

4. NIST. Common Vulnerability Scoring System Calculator. URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (дата звернення 03.03.2024).