УДК 004.056

М. Б. Дидяк
О. В. Войцеховська

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ БЕЗПЕЦІ ДАНИХ ПРИ ПЕРЕХОДІ ЗА URL-ПОСИЛАННЯМ

Вінницький національний технічний університет

Анотація

В роботі проведено аналіз видів загроз, таких як SQL-ін'єкція, міжсайтовий скриптинг, викрадення сесії, які можуть виникати при переході за URL-посиланням. Надано пропозиції щодо заходів захисту, які можуть бути вжиті для зменшення ризику та забезпечення безпеки в Інтернеті.

Ключові слова: загроза, SQL-ін'єкція, міжсайтовий скриптинг, викрадення сесії, URL-посилання.

Abstract

An analysis of the types of threats, such as SQL injection, cross-site scripting, and session hijacking, which may occur when navigating through URL links, was conducted in work. Suggestions are provided for protective measures that can be taken to reduce risk and ensure online safety.

Keywords: threat, SQL-injection, cross-site scripting, session hijacking, URL link.

Вступ

У сучасному світі Інтернет є невід'ємною частиною повсякденного життя, зокрема він надає можливості для комунікації, пошуку інформації, навчання, розваг, отримання та надання послуг, здійснення комерційних операцій, інтернет-банкінгу тощо. Але разом з цим приходить і ризик для безпеки користувачів. Постійне збільшення кількості web-продуктів приводить до зростання кількість наявних вразливостей. Одним з шляхів поширення кіберзагроз є використання URL-посилань, які можуть приховувати різноманітні загрози безпеці.

Метою даного дослідження є аналіз потенційних загроз, а також визначення шляхів їх виявлення та підвищення рівня захисту особистої інформації під час переходу за URL-посиланням. Розуміння цих загроз та прийняття відповідних заходів захисту є актуальним для забезпечення безпеки та конфіденційності у цифровому середовищі.

Результати дослідження

Зазвичай, загрози, що виникають при переході за посиланням, приховані як від користувача так і від адміністратора веб-ресурсу. При цьому будь-яка потенційна загроза може привести до втрати працездатності або порушення цілісності web-ресурсу, викрадення даних, втрати конфіденційності або доступності інформації тощо. Тому важливо ще на етапі розробки та технічної підтримки web-ресурсу дотримуватись базових заходів безпеки.

Розглянемо основні види загроз, які можуть виникати при переході за URL-посиланням.

1. SQL-ін'єкція – виникає, коли зловмисник вставляє SQL-код у введені дані, які передаються через GET або POST запити. Може призвести до витоку конфіденційної інформації або пошкодження бази даних. Можливими найпростішими методами захисту є використання параметризованих запитів, обмеження прав доступу до бази даних, валідація та екранування введених даних [1].
2. Міжсайтовий скриптинг (XSS) – дозволяє зловмисникам вставляти на сторінки безпечного веб-сайту скрипти, які виконуються у браузері користувача, оскільки браузер вважає, що сценарій надійшов із надійного джерела. Зловмисний скрипт може отримати доступ, наприклад, до файлів cookie або конфіденційної інформації, яка зберігається браузером і використовується на цьому сайті. Методами захисту є екранування та валідація введених даних, використання Content Security Policy, обмеження виконання JavaScript на сторінках [2].
3. Викрадення сесії (cookie poisoning) – дозволяє зловмисникам отримувати доступ до сесійних ідентифікаторів користувачів та підроблювати або змінювати їх сесії з метою отримання доступу до

облікового запису користувача або викрадення його ідентифікаційних даних. Методами захисту можуть бути використання HTTPS, валідація сесійних даних, використання механізму перевірки цілісності даних [3].

У підсумку, визначимо методи, необхідні для запобігання або мінімізації зловмисним загрозам.

Розробникам web-ресурсів обов'язково потрібно перевіряти та очищати введені дані перед їх використанням, щоб уникнути атак типу SQL-ін'єкція. Також потрібно використовувати безпечний код, тобто важливо регулярно оновлювати та перевіряти код програмного забезпечення, щоб виявляти та виправляти потенційні вразливості. Крім того, необхідно виконувати захист сесій, зокрема користуватися надійними механізмами керування сесіями, такими як токени аутентифікації, механізми перевірки цілісності даних тощо.

Висновки

Проведений аналіз показав, що перехід за URL-посиланням може приховувати різні загрози для безпеки користувачів в Інтернеті. Типові атаки, такі як SQL-ін'єкція, міжсайтовий скриптинг та викрадення сесії, можуть легко мати успіх при недостатньому захисті веб-додатків та неправильному використанні URL-посилань.

Для ефективного захисту від цих загроз необхідно вживати комплекс заходів безпеки як з боку користувачів, так і з боку розробників веб-продуктів. Важливо вдосконалювати процеси розробки, включаючи валідацію та екранування введених даних, регулярне оновлення програмного забезпечення та використання безпечних механізмів аутентифікації та авторизації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Тестування безпеки: SQL-ін'єкції [Електронний ресурс] – Режим доступу до ресурсу: https://training.qatestlab.com/blog/technical-articles/security-testing-sql-injection/.

2. Cross Site Scripting (XSS) [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-community/attacks/xss/.

3. Cookie poisoning [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/cookie-poisoning.

Дидяк Максим Богданович — студент групи 1КІ-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: maksimdidyak234@gmail.com

Войцеховська Олена Валеріївна – кандидат технічних наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця.

Maksym Bogdanovych Dydiak — student of group 1KI-20b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, email: maksimdidyak234@gmail.com

Voytsekhovska Olena V. – PhD, Assistant Professor of the Computer Techniques Department, Vinnytsia National Technical University, Vinnytsia.