1. **Використання сканеру ZAP**

Перевіривши сайт <https://automationexercise.com/> за допомогою застосунку ZAP було виявлено наступні основні вразливості:

1. **Cross-Site Scripting (XSS)**

Сайт дозволяє вставляти чужий JavaScript-код у сторінку. Це означає, що зловмисник може запустити свій скрипт у браузері жертви — наприклад, вкрасти кукі чи перенаправити на підробний ресурс.

1. **Cross-Site Request Forgery (CSRF)**

Інша сторінка може «попросити» браузер користувача виконати якусь дію на сайті, де користувач вже авторизований (наприклад, змінити настройки акаунта), навіть без його згоди.

1. **Небезпечні налаштування кукі**

Кукі з сесією можуть бути доступні з JavaScript або передаватися незашифрованими. Тобто крадіжка сесії стає простішою, бо зловмисник може їх прочитати чи перехопити.

1. **Завантаження будь-яких файлів**

Форма приймає файли без перевірки. Це дає змогу завантажити на сервер шкідливий файл (наприклад, веб-шелл), який потім можна виконати.

1. **Витік інформації в коментарях і mailto-посиланнях**

В коді залишилися коментарі з внутрішніми шляхами, секретами чи електронними адресами. Це допомагає зловмисникам краще зрозуміти, як влаштований сайт, і підготувати атаки.

1. **Clickjacking**

Сайт можна «вкласти» в чужий фрейм, завдяки чому користувач може неуважно натиснути на приховану кнопку або посилання й зробити небажану дію.

1. **Нестійка обробка форм**

Приховані поля або поля пароля можна змінити на клієнті — наприклад, підмінити дані перед відправкою. Поле для вводу паролю може автозаповнюватися або бути вкраденим через скрипти.

1. **Використання сканеру Security Headers**

Після сканування сайту <https://automationexercise.com/> за допомогою сервісу <https://securityheaders.com/> було виявлено наступні незахищені заголовки:

* **Strict-Transport-Security**

Говорить браузеру: «З цього моменту завжди заходь на сайт по HTTPS, ніколи не використовуй незахищене HTTP».

* **Content-Security-Policy**

Дає змогу вказати, звідки сайт може брати скрипти, стилі, зображення тощо, щоб випадково або навмисно не запустити чужий шкідливий код.

* **Permissions-Policy**

Обмежує доступ сайту до різних функцій браузера (наприклад, камери, мікрофона, геолокації), якщо вони не потрібні для роботи.