Під час аналізу сайту<https://automationexercise.com/> за допомогою ZAP були виявлені такі недоліки:

* **Відсутність Content Security Policy (CSP):** сайт не має політики обмеження джерел контенту, що робить його вразливим до впровадження шкідливих JavaScript-скриптів.
* **Нестача захисту від CSRF:** на сайті не застосовані токени CSRF у формах, а cookies не обмежені за призначенням, через що можливі підроблені запити.
* **Застарілі JS-бібліотеки:** використання непоновлених сторонніх скриптів може призвести до експлуатації відомих вразливостей.
* **Cookies без атрибуту HttpOnly:** відкритий доступ стороннім скриптам підвищує ризик викрадення сесій.
* **Відсутність заголовка HSTS:** без Strict-Transport-Security браузери можуть переходити на незахищений HTTP.
* **Розкриття технологічних деталей через X-Powered-By:** цей заголовок видає інформацію про платформу сервера, полегшуючи підготовку атак.
* **Неналежне керування сесіями:** відсутність обмежень за тривалістю сесій і використання ненадійних ідентифікаторів збільшує шанс їх викрадення.
* **Уразливість до XSS:** без належної валідації та екранування вводу зловмисники можуть ін’єктувати шкідливі скрипти.
* **Відсутній або некоректний Content-Type:** браузер може неправильно інтерпретувати відповідь сервера, що створює додаткові ризики.