Під час сканування сайту [**https://automationexercise.com/**](https://automationexercise.com/) за допомогою ZAP було виявлено наступні проблеми:

1. Відсутність Content Security Policy (CSP): через це сайт уразливий до атак із вставкою шкідливого JavaScript-коду. Необхідно обмежити джерела контенту через політику безпеки.
2. Cross-Site Request Forgery (CSRF): сайт не має захисту від підроблених запитів. Для усунення потрібно впровадити CSRF-токени у форми та обмежити дію cookies.
3. Використання застарілих JavaScript-бібліотек: існує ризик експлуатації відомих вразливостей. Рекомендується регулярно оновлювати сторонні бібліотеки.
4. Cookies без прапору HttpOnly: відкриває доступ до cookies стороннім скриптам. Для захисту слід додавати атрибут HttpOnly.
5. Відсутній заголовок Strict-Transport-Security (HSTS): це дозволяє браузеру підключатися через незахищений HTTP. Потрібно примусово вмикати HTTPS через HSTS.
6. Витік технологічної інформації через X-Powered-By: сервер відкриває дані про свою платформу, що полегшує роботу зловмисників. Рекомендується приховати цей заголовок.
7. Недостатній контроль за сесіями: сесії можуть залишатися активними без обмеження часу або бути легко вкраденими. Потрібно встановити таймаути і використовувати безпечні ідентифікатори.
8. Вразливість до XSS-атак (Cross-Site Scripting): зловмисники можуть вставляти шкідливі скрипти. Всі введені дані потрібно ретельно перевіряти і екранувати.
9. Відсутній або некоректний заголовок Content-Type: без правильного вказання типу вмісту браузер може некоректно обробити відповідь, що підвищує ризики атак.

Під час сканування сайту [**https://automationexercise.com/**](https://automationexercise.com/) за допомогою [**https://securityheaders.com/**](https://securityheaders.com/)було виявлено які загаловки доцільно змінити\додати щоб покращити безпеку додатку.

1. Content-Security-Policy — захищає від XSS-атак і небезпечних ресурсів.
2. Strict-Transport-Security — примушує використовувати HTTPS.
3. Referrer-Policy — контролює, яку інформацію посилає браузер у реферері.
4. Permissions-Policy — обмежує доступ до апаратних можливостей браузера.



