УДУ імені Михайла Драгоманова

Факультету математики, інформатики та фізики

Кафедра комп’ютерної та програмної інженерії

ЛАБОРАТОРНА РОБОТА №10

з курсу

«Тестування програмного забезпечення»

Тема:" Розробка тест-кейсів на основі тест-плану та чек-листів"

Андрушко Антон Тарасович

Група 41 КН

Факультет математики, інформатики та фізики

Викладач: Кархут В.Я.

Київ 2025

Під час сканування сайту **automationexercise.com** інструментом ZAP було виявлено декілька типових вразливостей, які можуть створювати загрози для безпеки вебдодатку. Основні знайдені проблеми:

**1. Використання вразливих бібліотек JavaScript** (наприклад, jquery.prettyPhoto.js та bootstrap.min.js). Це може дозволити зловмисникам скористатися відомими уразливостями у застарілому коді. Щоб запобігти цьому, необхідно регулярно оновлювати сторонні бібліотеки до останніх стабільних версій.

**2. Відсутність заголовка політики безпеки вмісту (CSP)**. Без CSP браузер не обмежує можливе виконання шкідливого JavaScript, що підвищує ризик XSS-атак. Рекомендується налаштувати політику безпеки вмісту, щоб дозволяти завантаження тільки перевірених скриптів і ресурсів.

**3. Відсутність токенів Anti-CSRF** на формі входу. Це робить сайт вразливим до атак підміни запитів від імені користувача. Захистити додаток можна шляхом впровадження CSRF-токенів у форми та перевірки їх на сервері.

**4. Відсутність заголовка Strict-Transport-Security (HSTS)**. Це дозволяє здійснювати атаки типу "man-in-the-middle" при спробах переходу на сайт через незахищений HTTP. Для захисту варто увімкнути HSTS, щоб змусити браузери використовувати тільки HTTPS.

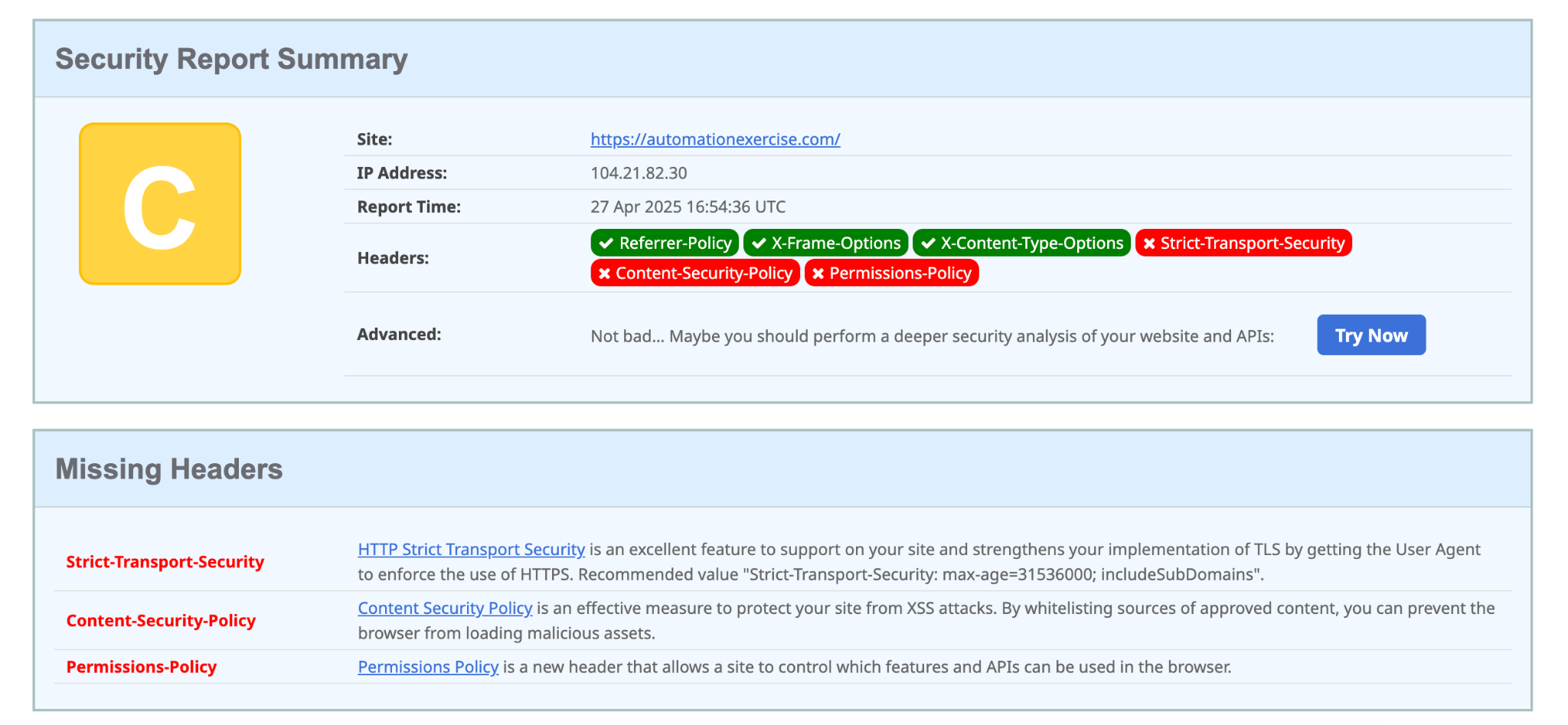
**5. Витік інформації через заголовок "X-Powered-By"**, наявність підозрілих коментарів у коді, помилки виведення, і розголошення сесійних відповідей. Ці моменти відкривають технічні деталі системи, які можуть бути використані атакуючими. Рекомендується мінімізувати інформацію в заголовках і прибирати коментарі перед релізом.

**6. Проблеми з атрибутами cookie**: відсутність прапорців HttpOnly і Secure, що може призвести до викрадення сесій. Для підвищення безпеки потрібно вказувати прапорці HttpOnly та Secure для всіх сесійних cookie.

**7. Інші інформаційні попередження**: відсутній заголовок Content-Type, некоректне керування кешем, а також наявність елементів, які можуть потенційно бути використані для XSS-атак. Рекомендується перевірити налаштування кешування, коректно встановлювати MIME-типи і здійснювати валідацію користувацьких даних.

**Загальний висновок**: сайт має набір класичних вразливостей, які часто зустрічаються в реальних проектах. Більшість проблем можна вирішити налаштуванням заголовків безпеки, оновленням компонентів і посиленням контролю введення та автентифікації. Рекомендується впровадити політики безпеки, налаштувати захист сесій та регулярно перевіряти сайт на наявність вразливостей.

2.

  
Під час сканування сайту [**https://automationexercise.com/**](https://automationexercise.com/) було виявлено декілька важливих моментів, які потребують уваги. Загальний рейтинг безпеки — **C**, що свідчить про середній рівень захищеності ресурсу.

Найбільшими проблемами є відсутність важливих HTTP-заголовків, таких як **Strict-Transport-Security**, **Content-Security-Policy** і **Permissions-Policy**. Відсутність Strict-Transport-Security знижує ефективність захисту трафіку через HTTPS і робить сайт вразливим до атак типу "man-in-the-middle". Налаштування цього заголовка з параметром max-age=31536000; includeSubDomains дозволило б змусити браузери завжди використовувати захищене з'єднання.

Також на сайті не налаштований Content-Security-Policy, що підвищує ризик XSS-атак. Встановлення CSP допомагає обмежити джерела, з яких завантажуються скрипти та інші ресурси. Відсутність Permissions-Policy позбавляє сайт можливості керувати використанням функцій браузера, таких як доступ до камери, мікрофона чи геолокації, що також впливає на загальну безпеку.

Аналіз заголовків показав, що деякі базові заходи безпеки все ж присутні: встановлені **Referrer-Policy** (same-origin), **X-Frame-Options** (DENY) і **X-Content-Type-Options** (nosniff). Однак є і негативні моменти: присутній заголовок **X-Powered-By** (Phusion Passenger 6.0.23), який розкриває інформацію про використовувані технології на сервері, що може бути використано для підготовки таргетованих атак. Рекомендується або прибрати цей заголовок, або замінити його на менш інформативний.

Щодо cookies, було виявлено, що встановлений cookie (csrftoken) не має встановлених флагів **HttpOnly** і **Secure**, що робить його потенційно вразливим для викрадення через JavaScript або перехоплення в незашифрованих сесіях. Для підвищення безпеки необхідно обов'язково додавати обидва ці прапорці до всіх cookies, що стосуються автентифікації або збереження сесій.

Крім того, в майбутньому рекомендується впровадити нові захисні заголовки, такі як **Cross-Origin-Embedder-Policy**, **Cross-Origin-Opener-Policy** та **Cross-Origin-Resource-Policy**, які посилюють захист контенту від небезпечних операцій через різні домени.

**Загальний висновок**: сайт має базові механізми безпеки, але відсутність важливих заголовків і некоректні налаштування cookies суттєво послаблюють загальний рівень захисту. Рекомендується виправити ці недоліки для підвищення стійкості сайту до сучасних типів атак і переходу до вищого класу безпеки.