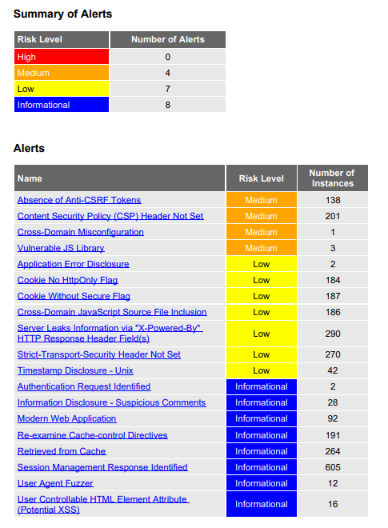
***Сканування за допомогою ZAP cканера***

***Основні знайдені типи вразливостей:***



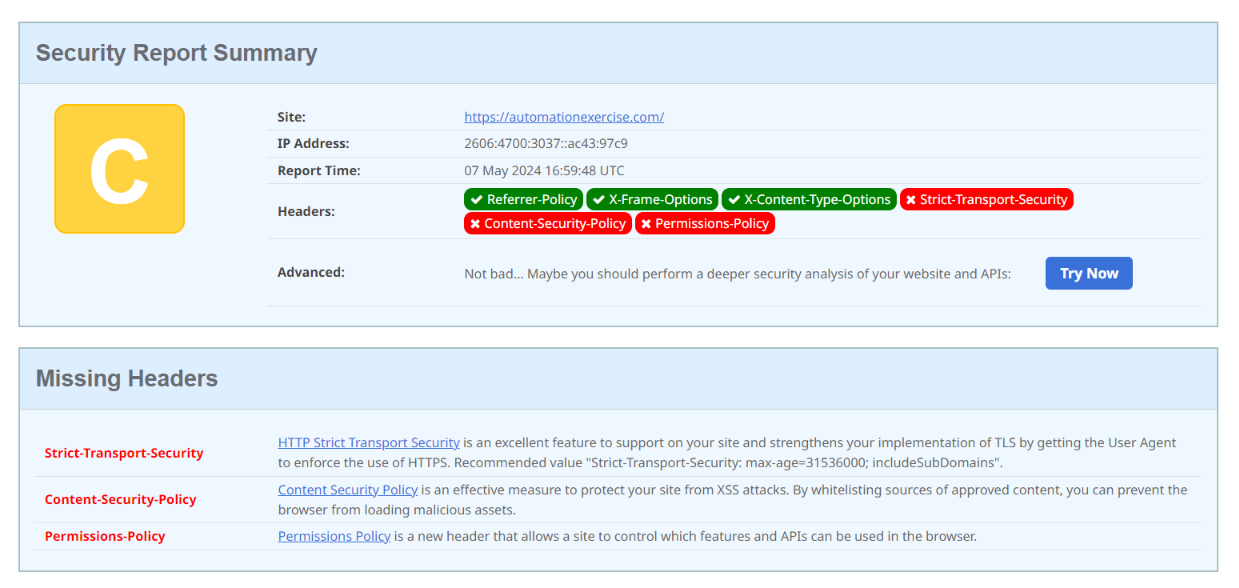
1. Absence of Anti-CSRF Tokens – Відсутність токенів Anti-CSRF.
2. Content Security Policy (CSP) Header Not Set – Відсутність заголовка Content Security Policy (CSP).
3. Cross-Domain Misconfiguration – Крос-доменна некоректна конфігурація.
4. Vulnerable JS Library – Вразлива бібліотека JavaScript.
5. Application Error Disclosure – Розкриття інформації про помилки сайту.
6. Cookie No HttpOnly Flag – Кукі без атрибута HttpOnly.
7. Cookie Without Secure Flag – Кукі без атрибута Secure.
8. Cross-Domain JavaScript Source File Inclusion – Крос-доменне включення джерел JavaScript.
9. Server Leaks Information via “X-Powered-By” HTTP Response Header Field(s) – Витік інформації через заголовок відповіді HTTP “X-Powered-By”.
10. Strict-Transport-Security Header Not Set – Відсутність заголовка Strict-Transport-Security.
11. Timestamp Disclosure - Unix – Розкриття часової мітки Unix.

* **Відсутність токенів Anti-CSRF.** Це може призвести до атак типу Cross-Site Request Forgery (CSRF), де зловмисник може використати авторизовану сесію користувача для виконання небажаних дій.
* **Відсутність заголовка Content Security Policy (CSP).** Це може зробити сайт вразливим до атак Cross-Site Scripting (XSS), де зловмисник внедрює та виконує власний код JavaScript на сторінках сайту.
* **Крос-доменна некоректна конфігурація.** Це може призвести до можливості атак на безпеку, які використовують інформацію з інших доменів для атак на основний сайт.
* **Вразливі бібліотеки JavaScript.** Це може дозволити зловмиснику використовувати вразливості в сторонніх бібліотеках для атак на сайт.
* **Відкриття інформації про помилки додатку.** Це може розкрити чутливу інформацію про сайт, що може бути використано для атак або недозволених дій.
* **Недостатність захисту кукі.** Це може призвести до можливості отримання доступу до авторизованих сесій користувача з боку зловмисника.
* **Виток інформації через заголовок HTTP “X–Powered–By”.** Це може розкривати непотрібну інформацію про сервер, що може бути використано для атак.
* **Недостатня конфігурація заголовка Strict-Transport-Security.** Це може зробити сайт вразливим до атак Man-in-the-Middle (MITM), де зловмисник може перехопити комунікацію між клієнтом і сервером.
* **Розкриття часової мітки Unix.** Це може надати зловмиснику зайву інформацію про сервер або додаток, яка може бути використана для аналізу та виконання атак.
* **Інформаційні вразливості**. Це може надати зловмисникам інформацію, яка може бути використана для пошуку вразливостей або атак на сайт.

Щоб запобігти цим вразливостям, важливо вжити наступні заходи безпеки:

* Використання токенів Anti-CSRF для захисту форм від атак CSRF.
* Встановлення правильної політики Content Security Policy (CSP), щоб обмежити виконання вразливого коду JavaScript.
* Правильна конфігурація CORS (Cross-Origin Resource Sharing) для запобігання крос-доменним атакам.
* Регулярне оновлення та моніторинг використання вразливих бібліотек JavaScript.
* Вимкнення відображення детальних повідомлень про помилки на виробничих серверах.
* Встановлення атрибутів HttpOnly та Secure для кукі для підвищення їх безпеки.
* Видалення або приховання інформації про сервер з заголовка HTTP “X-Powered-By”.
* Встановлення заголовка Strict-Transport-Security для забезпечення безпечного з’єднання через HTTPS.
* Відключення розкриття часової мітки Unix та інших зайвих даних з відповідей сервера.
* Ретельна перевірка та видалення будь-якої чутливої інформації або коментарів у вихідному коді додатка.

***Скан сайту https://automationexercise.com/ за допомогою https://securityheaders.com/***



Для того щоб покращити безпеку додатку, рекомендується додати заголовки, які відображені нижче. Це допоможе убезпечити сайт від різних видів атак, таких як атаки на мережевий рівень, XSS-атаки та несанкціонований доступ до функцій браузера.

* Strict-Transport-Security (STS): цей заголовок вказує браузерам відвідувачів сайту, що вони повинні завжди використовувати HTTPS для з’єднання з сайтом. Це допомагає запобігти атакам, пов'язаним з перехопленням мережевого трафіку. Рекомендоване значення max-age вказує, на який час браузер повинен запам'ятовувати це правило.
* **Content-Security-Policy (CSP):** цей заголовок дозволяє встановлювати правила для завантаження ресурсів на сайті, що допомагає уникнути атак XSS (міжсайтового скриптінгу). Можна вказати, з яких джерел можна завантажувати скрипти, стилі, медіа-файли та інші ресурси.
* **Permissions-Policy:** Цей заголовок дозволяє контролювати доступ до різних функцій та API в браузері. Можна обмежити доступ до геолокації, камери, мікрофону та інших API, що допомагає зменшити ризики витоку даних та збільшити приватність користувачів.