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"

Балицький Назар Сергійович
Група 41 КН
Факультет математики, інформатики та фізики
Викладач: Кархут В.Я.

Київ 2025

1. Завантажте ZAP сканнер https://www.zaproxy.org/download/ та проскануйте з його допомогою https://automationexercise.com/.

1. ***Вразлива бібліотека JavaScript***
   Було знайдено, що сайт використовує застарілі або потенційно небезпечні версії JavaScript-бібліотек, наприклад jquery.prettyPhoto.js і bootstrap.min.js. Це небезпечно тим, що такі бібліотеки можуть містити відомі вразливості, які легко використати для атак. Щоб цього уникнути, потрібно регулярно оновлювати сторонні бібліотеки та застосовувати інструменти на кшталт Retire.js або Snyk для виявлення проблемних компонентів.

2. ***Відсутність токенів Anti-CSRF***
   У формах, таких як /login, відсутні захисні токени від CSRF-атак. Через це існує ризик, що зловмисники можуть виконувати підставні запити від імені користувача. Для захисту потрібно додати CSRF-токени у всі форми і перевіряти їх дійсність на сервері при кожному запиті.

3. ***Відсутній заголовок Content-Security-Policy (CSP)***
   На сайті не налаштована політика безпечного завантаження контенту, що підвищує ризик XSS-атак. Щоб посилити безпеку, слід додати заголовок Content-Security-Policy і дозволити завантаження ресурсів тільки з перевірених джерел.

4. ***Server Leaks Information via "X-Powered-By" Header***
   Сервер у відповіді віддає заголовок X-Powered-By, що розкриває інформацію про використовувані технології. Це може допомогти хакерам при підготовці атак. Краще або повністю прибрати цей заголовок, або змінити його на щось нейтральне.

5. ***Strict-Transport-Security (HSTS) Header Not Set***
   На сайті не встановлено заголовок HSTS, через що браузер не змушується працювати виключно через HTTPS. Відсутність цього захисту робить сайт вразливим до атак "людина посередині". Щоб вирішити проблему, необхідно налаштувати Strict-Transport-Security для всіх відповідей через HTTPS.

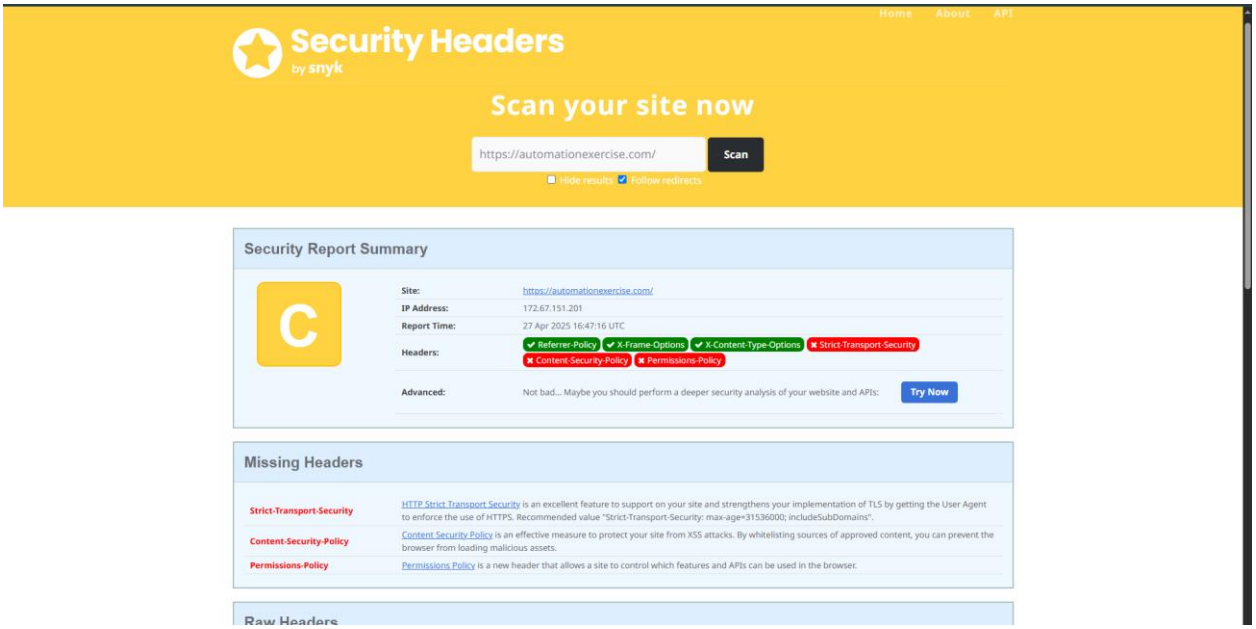
6. ***Файл cookie без прапорця HttpOnly або Secure***
   Деякі куки не мають атрибутів HttpOnly або Secure. Це дозволяє в разі атак XSS або на незахищених з'єднаннях викрасти або перехопити куки користувача. Для захисту їх потрібно завжди створювати з відповідними атрибутами.

7. ***Розкриття помилок програми***
   Під час помилок сервер виводить технічні подробиці, наприклад трасування помилок. Це може спростити зловмисникам аналіз внутрішньої структури

системи. Рекомендується замінити реальні повідомлення про помилки на загальні й логувати їх лише на сервері.

8. ***Інформаційні попередження (Info-level alerts)***
   Окремо були виявлені менш критичні рекомендації: відсутній заголовок Cache-Control, знайдені підозрілі HTML-коментарі, а також деякі особливості сучасних вебзастосунків. Їх варто врахувати для загального посилення безпеки сайту.

2. З допомогою https://securityheaders.com/ проскануйте https://automationexercise.com/ та визначте які загаловки доцільно змінити\додати щоб покращити безпеку додатку.



<u>Оцінка безпеки:</u> C

1. Немає заголовка Strict-Transport-Security.
Через це браузер не змушується використовувати HTTPS. Це може бути небезпечно, бо зловмисники можуть перехопити дані.
<u>Що потрібно зробити:</u> додати заголовок Strict-Transport-Security з параметром max-age=31536000; includeSubDomains.

2. Немає заголовка Content-Security-Policy.
Без цього заголовка сайт менш захищений від атак типу XSS (впровадження шкідливого коду).
<u>Що потрібно зробити:</u> налаштувати Content-Security-Policy для дозволу контенту тільки з довірених джерел.

3. Відсутній заголовок Permissions-Policy.
Це означає, що сайт не обмежує доступ браузера до функцій, таких як камера чи

геолокація.
Що потрібно зробити: встановити Permissions-Policy, щоб обмежити доступ до непотрібних функцій.

4. Невірно налаштовані cookies.
Файли cookies створюються без прапорців Secure і HttpOnly. Це може дати можливість викрасти дані користувачів.
Що потрібно зробити: додати прапорці Secure і HttpOnly для cookies.

5. Присутній заголовок X-Powered-By.
Сервер видає зайву інформацію про своє програмне забезпечення, що може допомогти зловмисникам у виборі способу атаки.
Що потрібно зробити: видалити або змінити цей заголовок.

Що налаштовано правильно:

- Використовується Referrer-Policy: same-origin (обмежує передачу реферера).
- Використовується X-Frame-Options: DENY (захист від підстановки фреймів).
- Використовується X-Content-Type-Options: nosniff (захист від неправильного визначення типу контенту).