**Міністерство освіти і науки України**

**УДУ імені М.П.Драгоманова**

Факультет математики, інформатики та фізики

*Кафедра комп’ютерної та програмної інженерії*

ЛАБОРАТОРНА РОБОТА № 12

з курсу

*«Автоматизація тестування»*

## *Тема роботи: «*Тестування безпеки»

Студент:

Невмержицький Д. Ю.

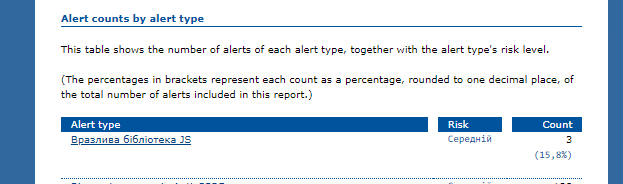
Група   41 ІПЗ

Факультет   інформатики

Викладач: Кархут В.Я.

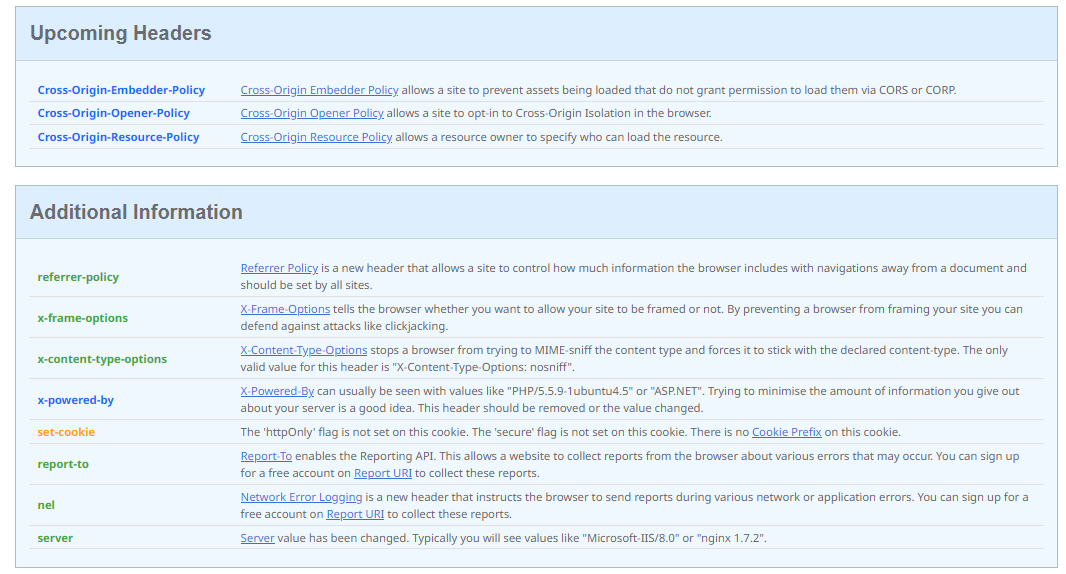
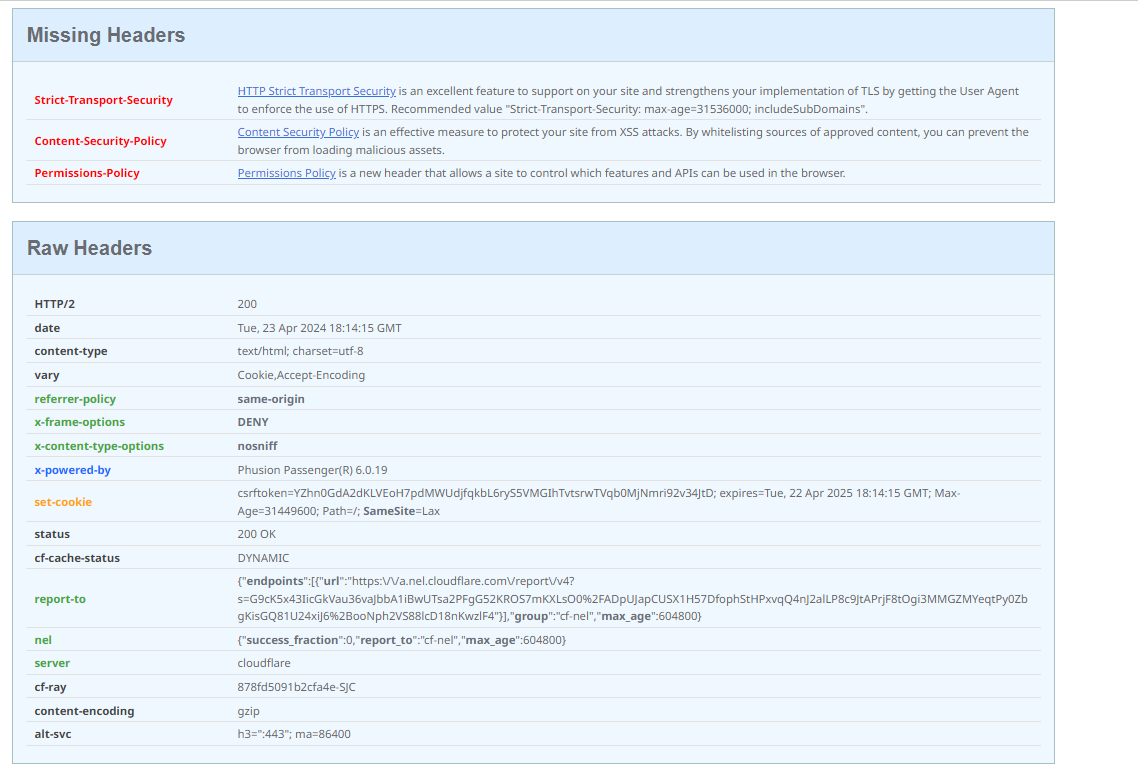
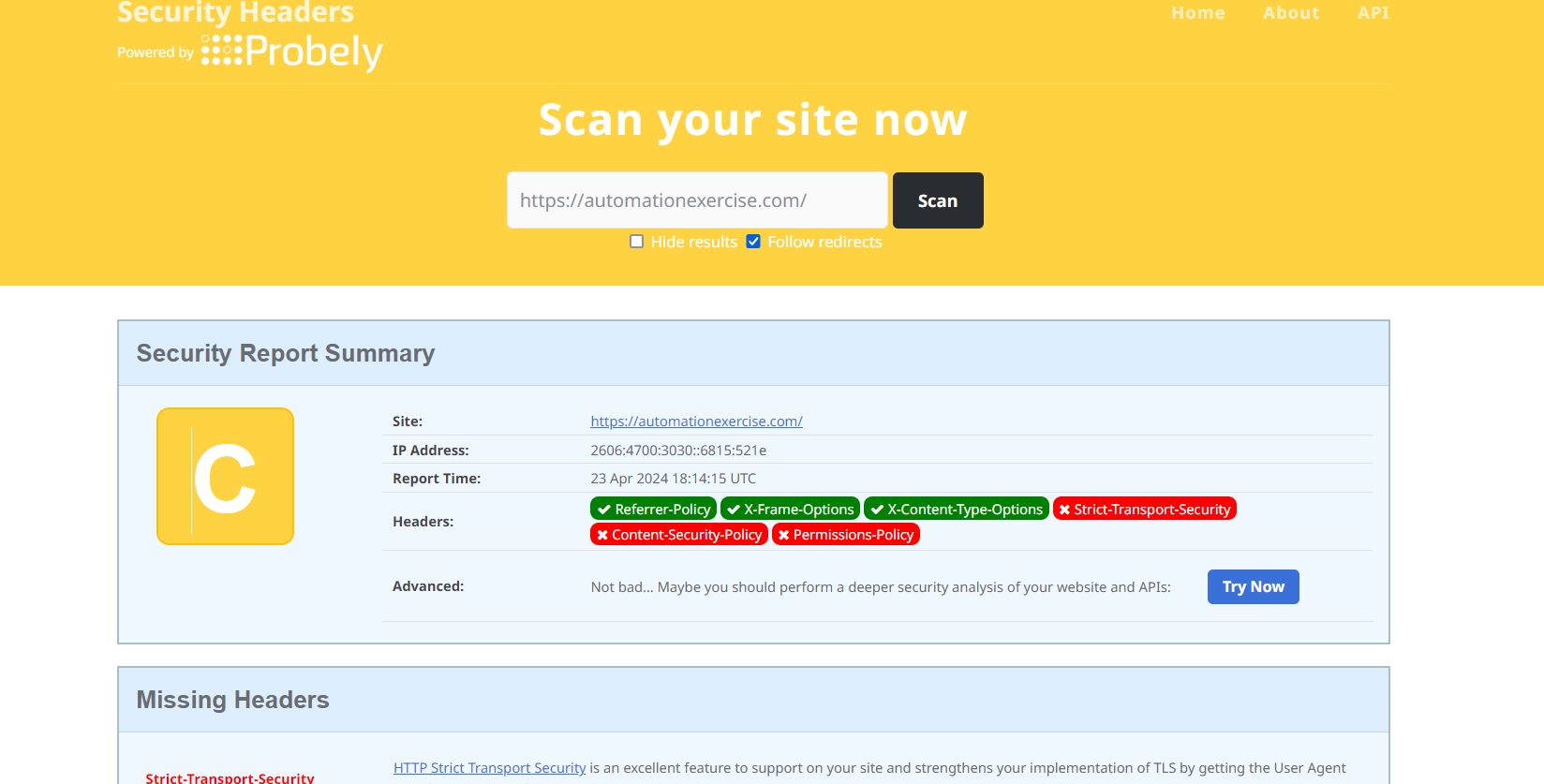
1. Завантажте ZAP сканнер https://www.zaproxy.org/download/ та проскануйте з його допомогоюhttps://automationexercise.com/.

Згенеруйте репорт та опишіть основні типи знайдених вразливостей та потенційні способи їх запобігання.





Основні вразливості, виявлені під час сканування:

1. **Відсутність заголовка Content Security Policy (CSP)**: Це збільшує ризик атак XSS. Запобігання полягає у введенні CSP для обмеження завантаження ресурсів.
2. **Міждоменна неправильна конфігурація (CORS)**: Неправильні налаштування CORS можуть дозволити несанкціонований доступ до даних користувачів. Запобігання полягає у правильному налаштуванні політик CORS.
3. **Відсутні токени проти CSRF атак**: Це може дозволити зловмисникам виконувати шкідливі запити від імені користувача. Введення токенів CSRF може запобігти таким атакам.
4. **Уразливості JavaScript бібліотек**: Використання застарілих JS бібліотек може викликати ризик XSS та інших атак. Рекомендується регулярне оновлення бібліотек.
5. **Cookie без флажків HttpOnly або Secure**: Відсутність цих флажків дозволяє зловмисникам отримувати доступ до cookies через скрипти або в незахищених умовах. Запобігання полягає в установці цих флажків для забезпечення безпеки cookies.
6. **Відсутність заголовка Strict-Transport-Security (HSTS)**: Невикористання HSTS може призвести до атак типу "man-in-the-middle". Рекомендується впровадити HSTS для гарантії використання HTTPS.
7. З допомогою https://securityheaders.com/ проскануйте https://automationexercise.com/ та визначте які загаловки доцільно змінити\додати щоб покращити безпеку додатку.
8. **Додавання заголовка Strict-Transport-Security (HSTS)**:
   * **Рекомендація**: Додати **Strict-Transport-Security: max-age=31536000; includeSubDomains** для зміцнення TLS, вимушуючи використання HTTPS.
   * **Користь**: Запобігає атакам типу "man-in-the-middle" шляхом примусу браузерів користувачів до виключно захищених з'єднань.
9. **Впровадження заголовка Content-Security-Policy (CSP)**:
   * **Рекомендація**: Встановити CSP, який би обмежував джерела контенту та запобігав завантаженню шкідливих асетів. Наприклад: **Content-Security-Policy: default-src 'self'; script-src 'self' https://trusted.cdn.com; object-src 'none'**.
   * **Користь**: Захист від атак типу cross-site scripting (XSS) і інших веб-загроз.
10. **Додавання заголовка Permissions-Policy**:
    * **Рекомендація**: Використовувати Permissions Policy для контролю доступу до певних API та функцій у браузері. Наприклад: **Permissions-Policy: geolocation=(self), microphone=()**.
    * **Користь**: Дозволяє адміністраторам сайтів визначати, які функції та API дозволені для використання на сайті.