УДУ імені Михайла Драгоманова

Факультет математики, інформатики та фізики

*Кафедра комп’ютерної та програмної інженерії*

Лабораторна робота №10

з курсу

«Автоматизація тестування»

Тема: Тестування безпеки

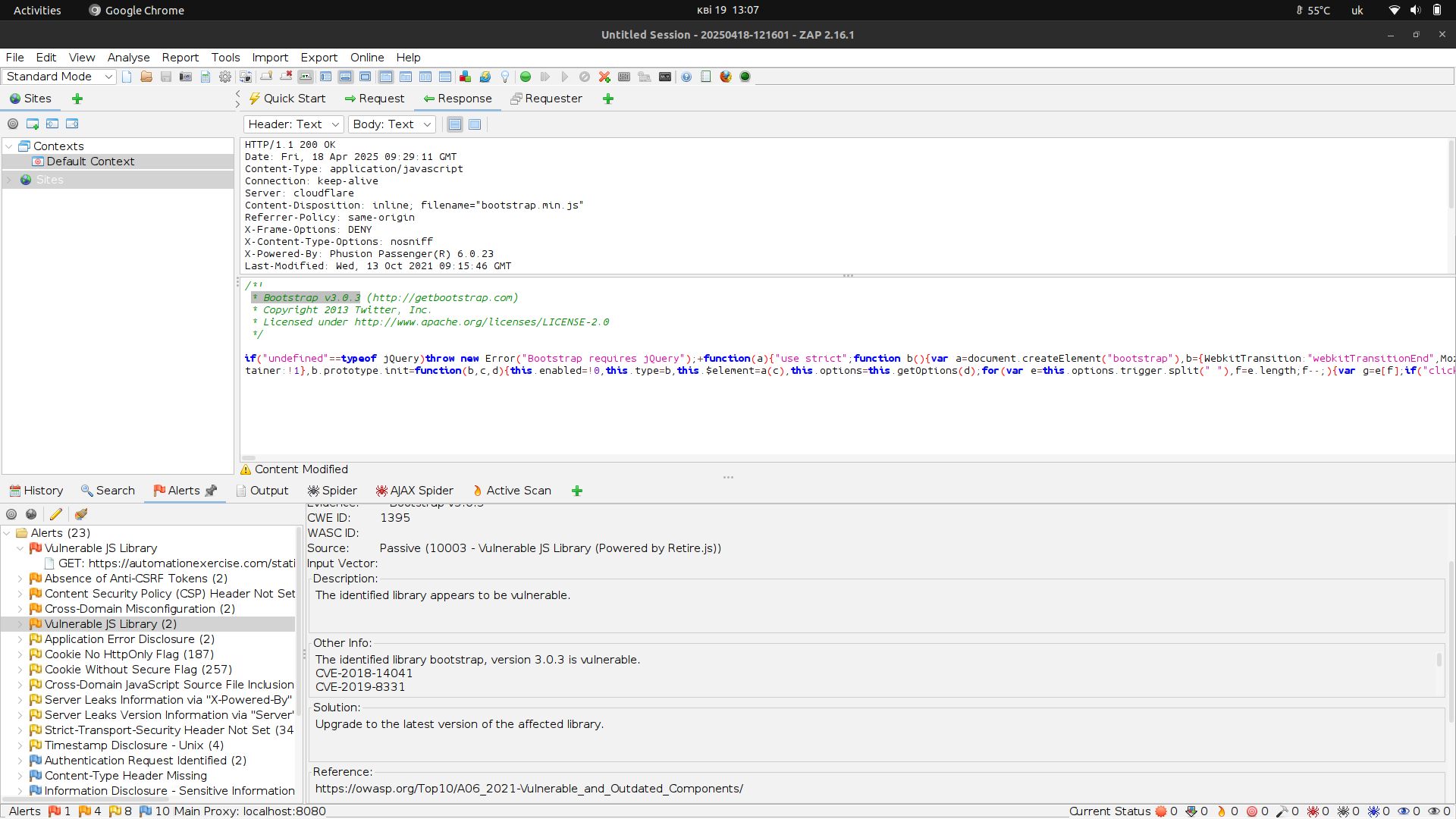
Студент: Власюк Роман Володимирович

Група: 41ІПЗ

Факультет: математики, інформатики та фізики

Викладач: Кархут В.Я.

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



Основні вразливості:

1. Використання вразливих js бібліотек: (prettyPhoto={version:"3.1.5"} та Bootstrap v3.0.3)

Рішення: оновіть бібліотеку до останньої версії.

1. Відсутність Anti-CSRF токена.

Рішення: використовуйте анти-CSRF пакети, такі як OWASP CSRFGuard; не використовуйте метод GET для запитів, які ініціюють зміну стану.

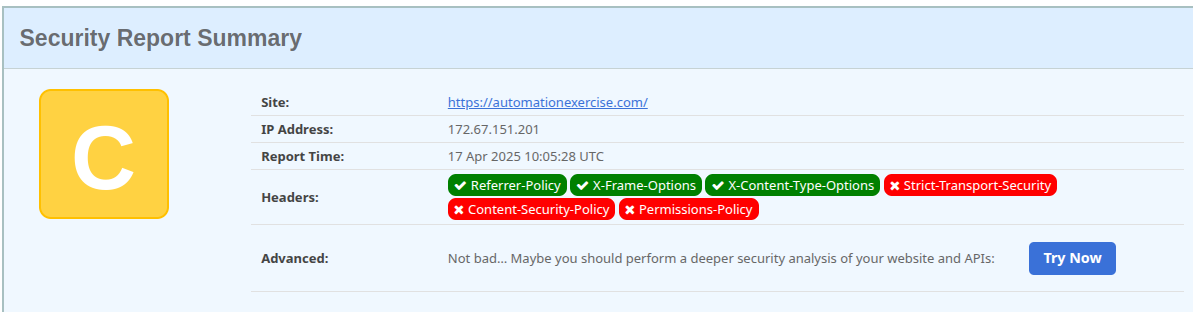
1. Заголовок Content Security Policy (CSP) не встановлений

Рішення: Переконайтеся, що ваш веб-сервер, сервер програм, балансувальник навантаження тощо має налаштований заголовок Content-Security-Policy.

1. Неправильна конфігурація Cross Origin Resource Sharing (CORS)

Рішення: Налаштуйте заголовок HTTP "Access-Control-Allow-Origin" на більш обмежувальний набір доменів або повністю видаліть усі заголовки CORS

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



Присутні заголовки - Referrer-Policy, X-Frame-Options, X-Content-Type-Options

Відсутні заголовки:

1. Strict-Transport-Security (Забезпечення з’єднання тільки через https). Рекомендоване значення - "Strict-Transport-Security: max-age=31536000; includeSubDomains".
2. Content-Security-Policy (Контроль завантажених файлів. Захист від Cross-site scripting) Рекомендоване значення - “Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self'; object-src 'none'; base-uri 'none'; frame-ancestors 'none';”
3. Permissions-Policy (Заборонити доступ до функцій пристрою, таких як камера, мікрофон і т.д. якщо вони не потрібні) Рекомендоване значення - “Permissions-Policy: camera=(), microphone=(), fullscreen=(), screen-wake-lock=()”