**УДУ імені Михайла Драгоманова**

**Факультет математики, інформатики та фізики**

***Кафедра комп’ютерної та програмної інженерії***

**Лабораторна робота № 10**

з дисципліни **«Автоматизація тестування»**

Виконав: Болілий Р.О.

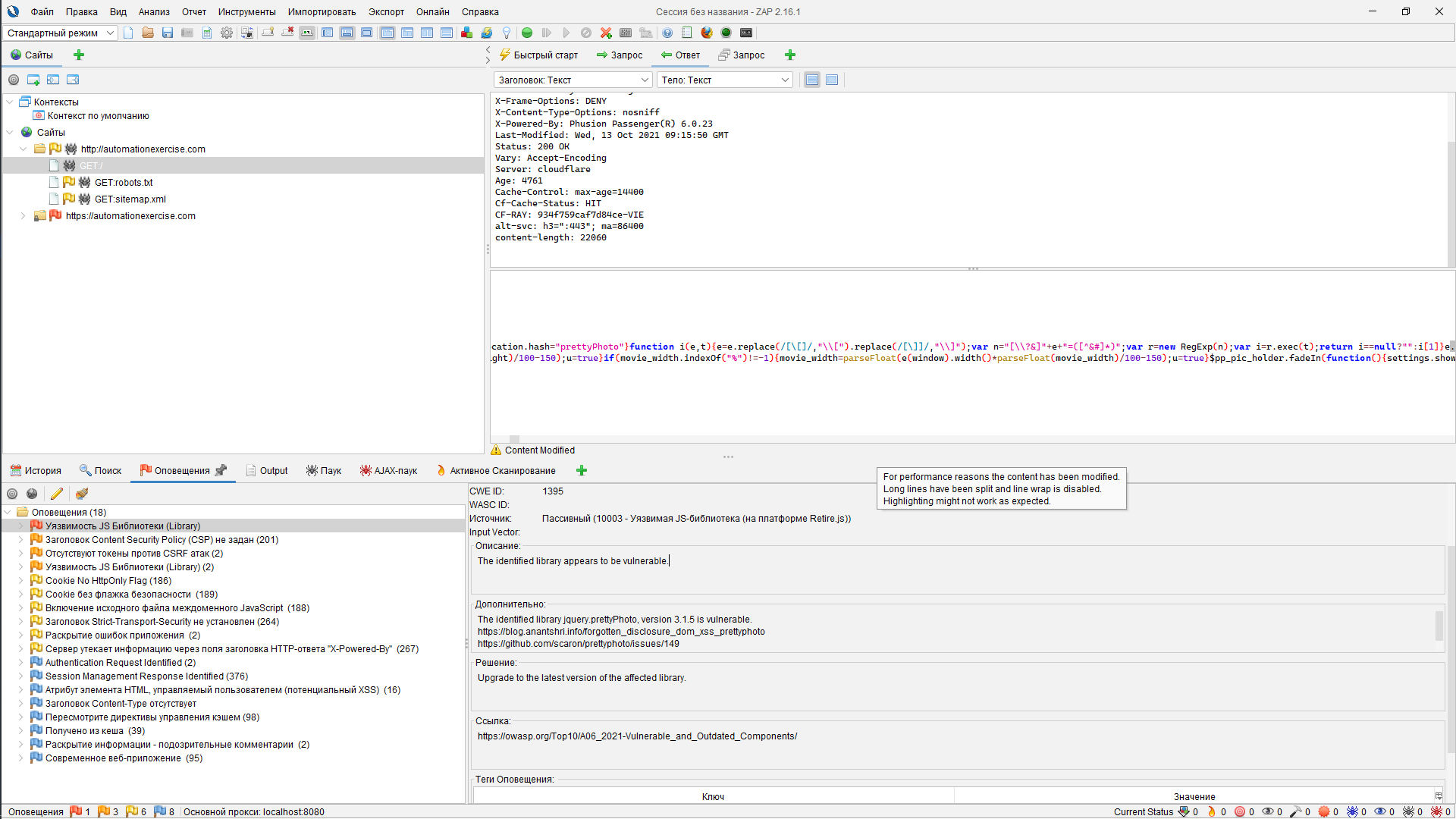
Група: 41ІПЗ

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/.**

Після проведення тестування за допомогою Zaproxy було знайдено 18 помилок, які показані на скріншоті. 

Шляхи вирішення цих вразливостей пишуться в самому додатку, але якщо все підсумувати, то основна порада це використовувати найновіші утиліти\програми\бібліотеки.

**2. З допомогою https://securityheaders.com/ проскануйте https://automationexercise.com/ та**

**визначте які загаловки доцільно змінити\додати щоб покращити безпеку додатку.**

Після сканування вдалося визначити наступні заголовки які потрібно додати чи змінити:

**Strict-Transport-Security**

HTTP Strict Transport Security — це чудова функція для підтримки на вашому сайті, яка покращує впровадження TLS, заставляючи агента користувача примусово використовувати HTTPS. Рекомендоване значення "Strict-Transport-Security: max-age=31536000; includeSubDomains".

**Content-Security-Policy**

Content-Security-Policy Content Security Policy – ​​це ефективний засіб захисту вашого сайту від атак XSS. Додавши джерела схваленого вмісту в білий список, ви можете запобігти завантаженню шкідливих ресурсів браузером.

**Permissions-Policy**

Permissions Policy — це новий заголовок, який дозволяє сайту контролювати, які функції та API можна використовувати у браузері.

