**УДУ імені М.П.Драгоманова**

Факультет математики, інформатики та фізики

*Кафедра комп’ютерної інженерії*

ЛАБОРАТОРНА РОБОТА №10

з курсу

***«Тестування програмного забезпечення»***

**Тема: "Тестування безпеки"**

Павлій Олександра Геннадіївна

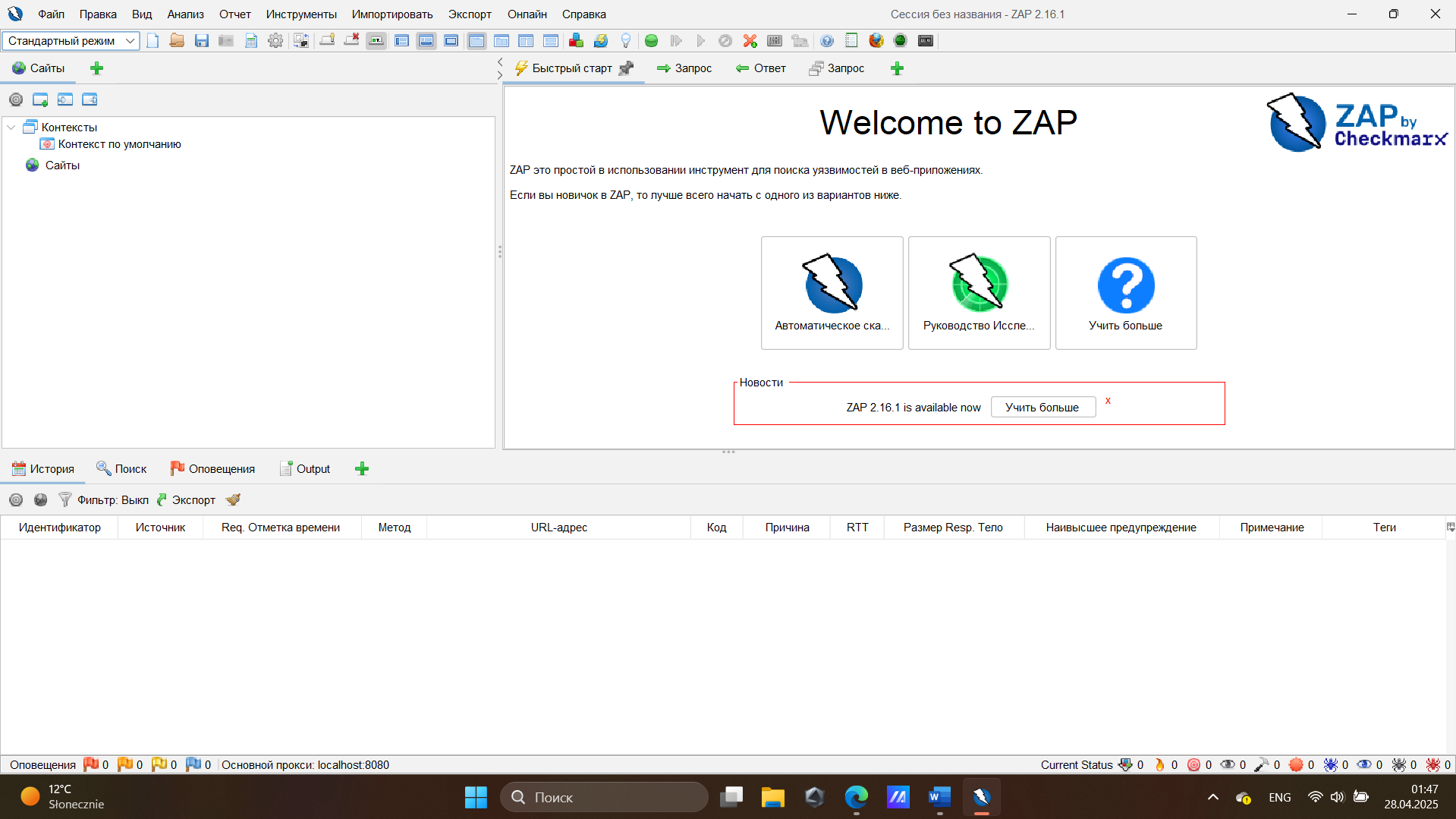
Група   41 КН

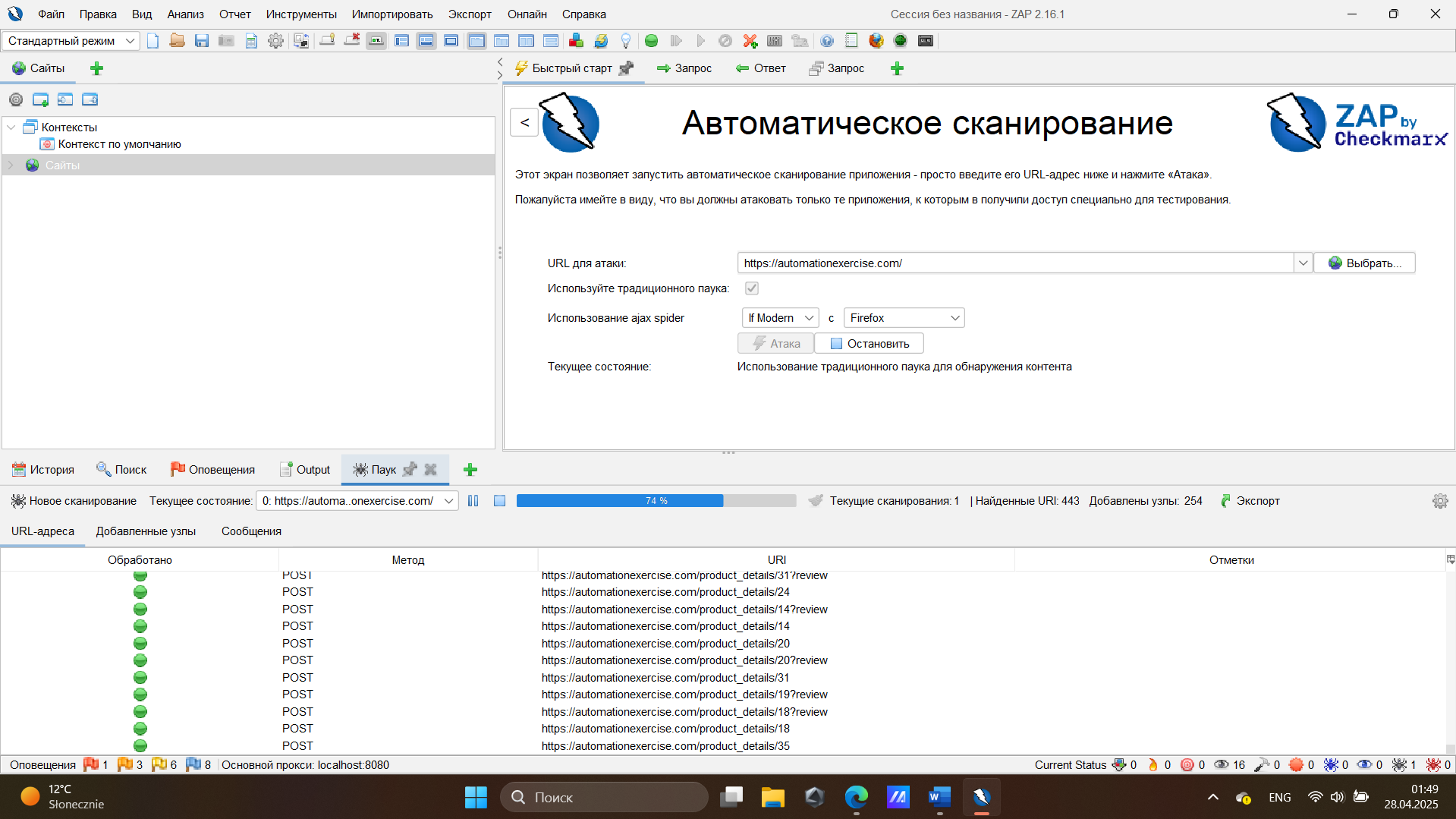
Факультет математики, інформатики та фізики

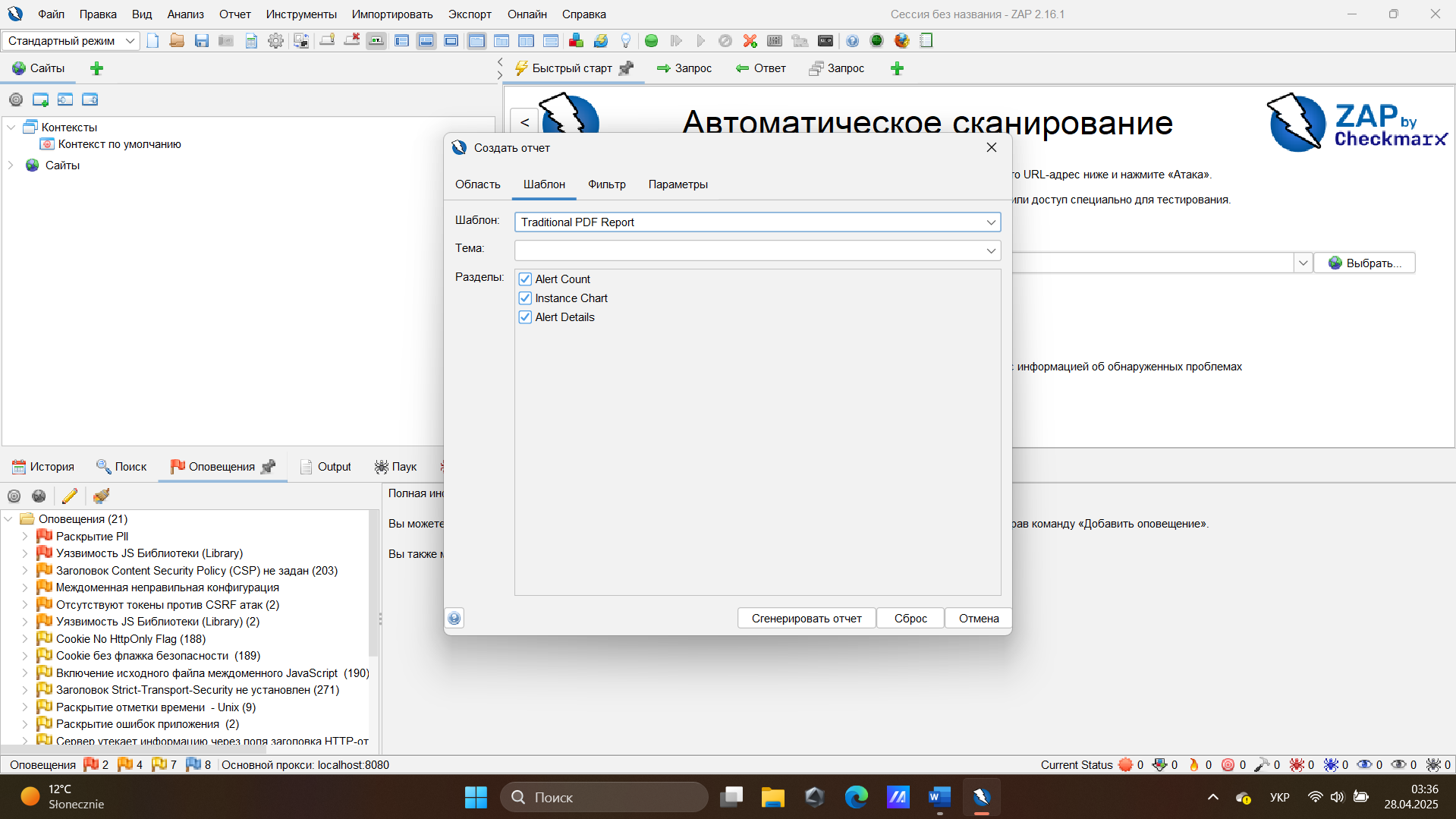
икладач: Кархут В.Я.

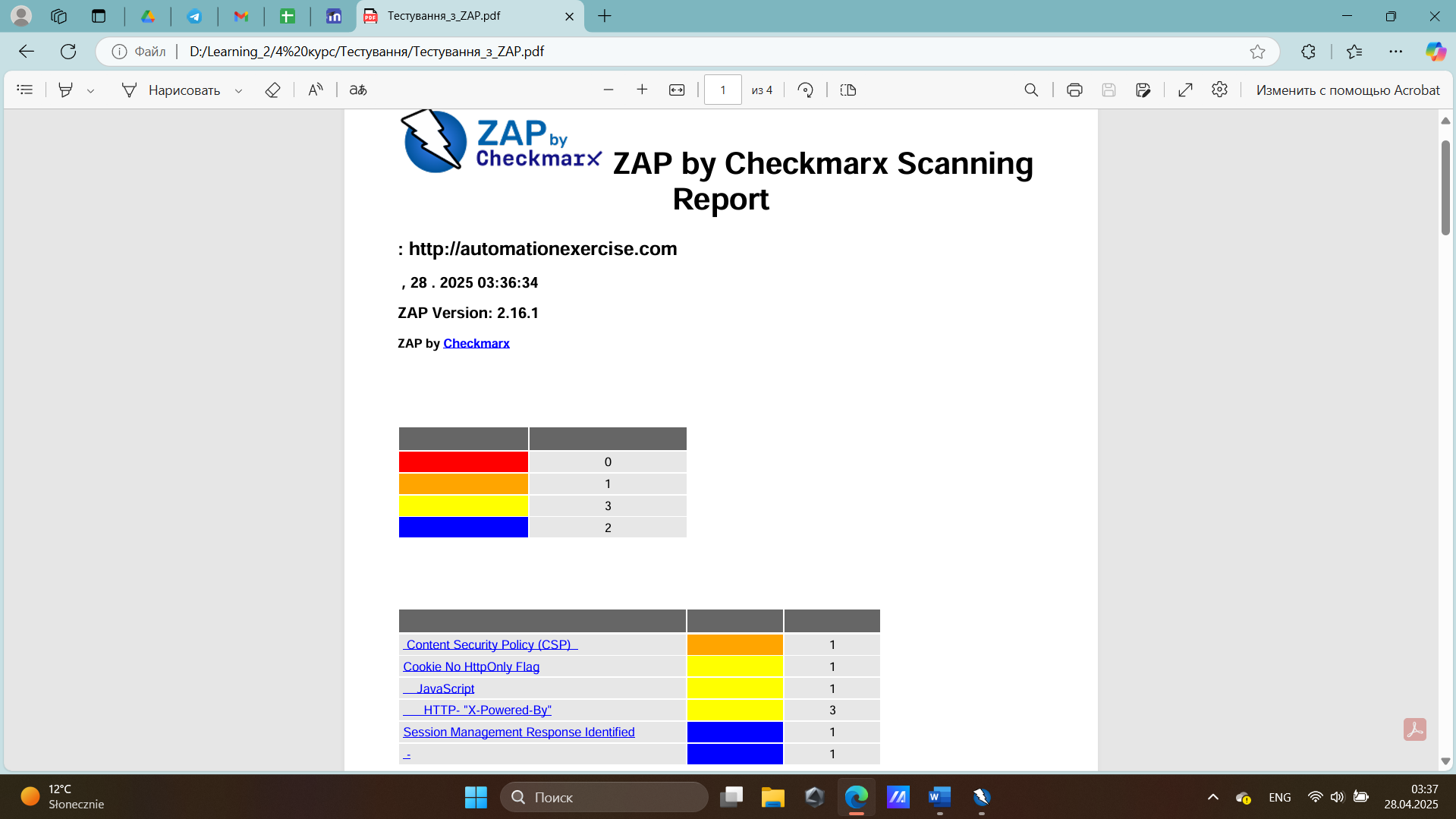
Київ 2024

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









Вразливості:

**Відсутність Content Security Policy (CSP) -** сайт не використовує CSP, що робить його вразливим до міжсайтового скриптингу (XSS) та інших атак, пов'язаних з виконанням зловмисного коду. Можливість ін'єкції шкідливого JavaScript, CSS або HTML. Щоб запобігти додайте заголовок Content-Security-Policy для обмеження джерел завантаження скриптів, стилів та інших ресурсів і використовуйте директиву default-src 'self' для заборони завантаження ресурсів із зовнішніх джерел, якщо це не потрібно.

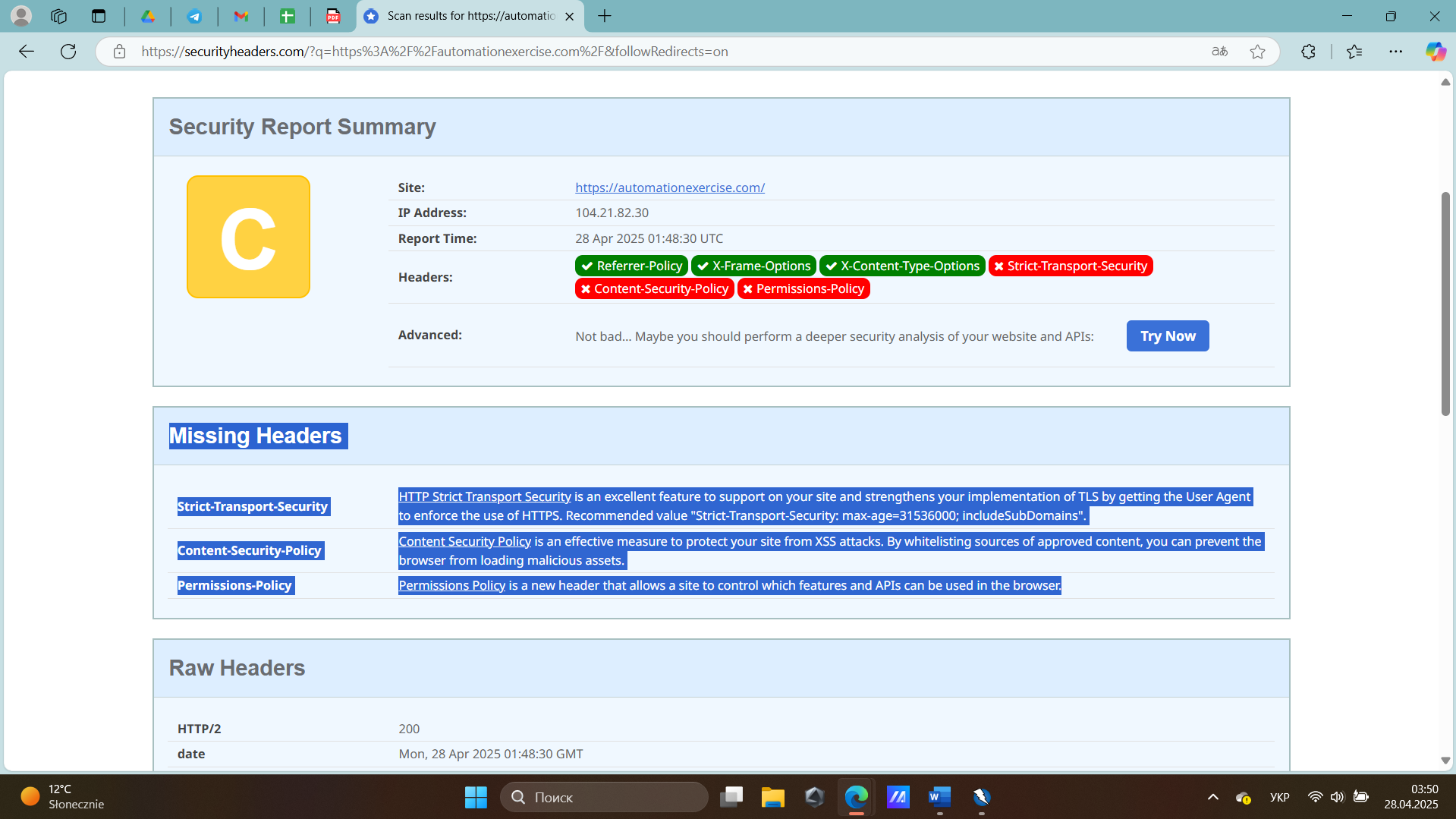
**Відсутність атрибуту HttpOnly для кукі –** кукі не позначені атрибутом HttpOnly, що дозволяє JavaScript отримувати до них доступ. Можливість крадіжки кукі через XSS-атаки. Додайте атрибут HttpOnly до всіх кукі, які містять конфіденційні дані (наприклад, токени сесій).

**Розкриття PII (Персональних даних) -** це будь-яка інформація, яка може ідентифікувати користувача (ім'я, email, телефон, адреса, дані карток тощо). Якщо такі дані передаються або зберігаються неналежним чином, зловмисники можуть їх перехопити та використати для шахрайства. Запобігання: мінімізація збору PII; шифрування даних; захист даних у rest api; регулярний аудит.

**Використання зовнішніх JavaScript-бібліотек -** завантажує JavaScript з зовнішнього джерела (googlesyndication.com), що може становити ризик, якщо джерело буде скомпрометоване. Якщо можливо, завантажуйте JavaScript-бібліотеки локально або використовуйте субресурсні хеші (SRI) для перевірки цілісності.

**Ідентифікація токенів сесії у відповідях -** відповідях сервера виявлено токени сесії, що може призвести до несанкціонованого доступу, якщо токени будуть перехоплені. Використовуйте HTTPS для шифрування передачі даних. Встановіть атрибути Secure та SameSite для кукі. Обмежте час дії токенів сесій та реалізуйте механізми їх повторної генерації.

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



**Змінити:**

**Strict-Transport-Security**

Примусово переводить всі з’єднання на HTTPS, запобігаючи атакам через HTTP (наприклад, downgrade-атаки).

Рекомендоване значення: Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

max-age=31536000 — термін дії (1 рік).

includeSubDomains — застосовується до всіх піддоменів.

preload — включення до списку HSTS прелоаду (для браузерів).

**Content-Security-Policy**

Блокує виконання підозрілих скриптів, запобігаючи XSS-атакам.

Рекомендовано:

Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' https://trusted.cdn.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self'; connect-src 'self'; frame-src 'none'; object-src 'none'

default-src 'self' — забороняє всі зовнішні ресурси, окрім поточного домену.

script-src — дозволяє скрипти лише з довірених джерел.

frame-src 'none' — блокує iframe (захист від клікіджекінгу).

**Permissions-Policy**

Контролює, які API браузера може використовувати сайт (наприклад, камера, мікрофон, геолокація).

Рекомендовано:

Permissions-Policy: geolocation=(), camera=(), microphone=(), payment=(), fullscreen=(self)

Забороняє доступ до геолокації, камери та мікрофона.

Дозволяє повноекранний режим лише для поточного домену.

**x-powered-by: Phusion Passenger(R) 6.0.23**

Розкриває інформацію про сервер. Рекомендація: видалити або замінити на фіктивне значення (наприклад, x-powered-by: PHP/8.1).

**set-cookie**

Відсутній HttpOnly (захист від XSS). Відсутній Secure (передача лише по HTTPS). SameSite=Lax — досить добре, але для критичних дій краще Strict.

**Додати:**

**Cross-Origin-Embedder-Policy.** Ізоляція контексту для захисту від Spectre.

**Cross-Origin-Opener-Policy.** Блокує спільний доступ до вікна з іншими доменами.

**Cross-Origin-Resource-Policy.** Контроль завантаження ресурсів.