

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет науки і технологій**

Кафедра «Комп’ютерні інформаційні технології»

**Лабораторна робота №3  
з дисципліни «Безпека програм та даних»**

**на тему:**

**«**Визначення та аналіз вразливостей веб-додатків за допомогою OWASP ZAP.»

Виконав:

студент гр. ПЗ2011

Кулик С.В.

Прийняв:

доц. Жеваго О. О.

Дніпро, 2023

**Тема.** Визначення та аналіз вразливостей веб-додатків за допомогою OWASP ZAP.

**Мета.** Ознайомитись з інструментом пошуку вразливостей веб-додатків OWASP ZAP.

**Завдання**

1. Оберіть веб-додаток для сканування. Додаток повинен бути вами написаний

або взятий з github, та запущений на вашій машині.

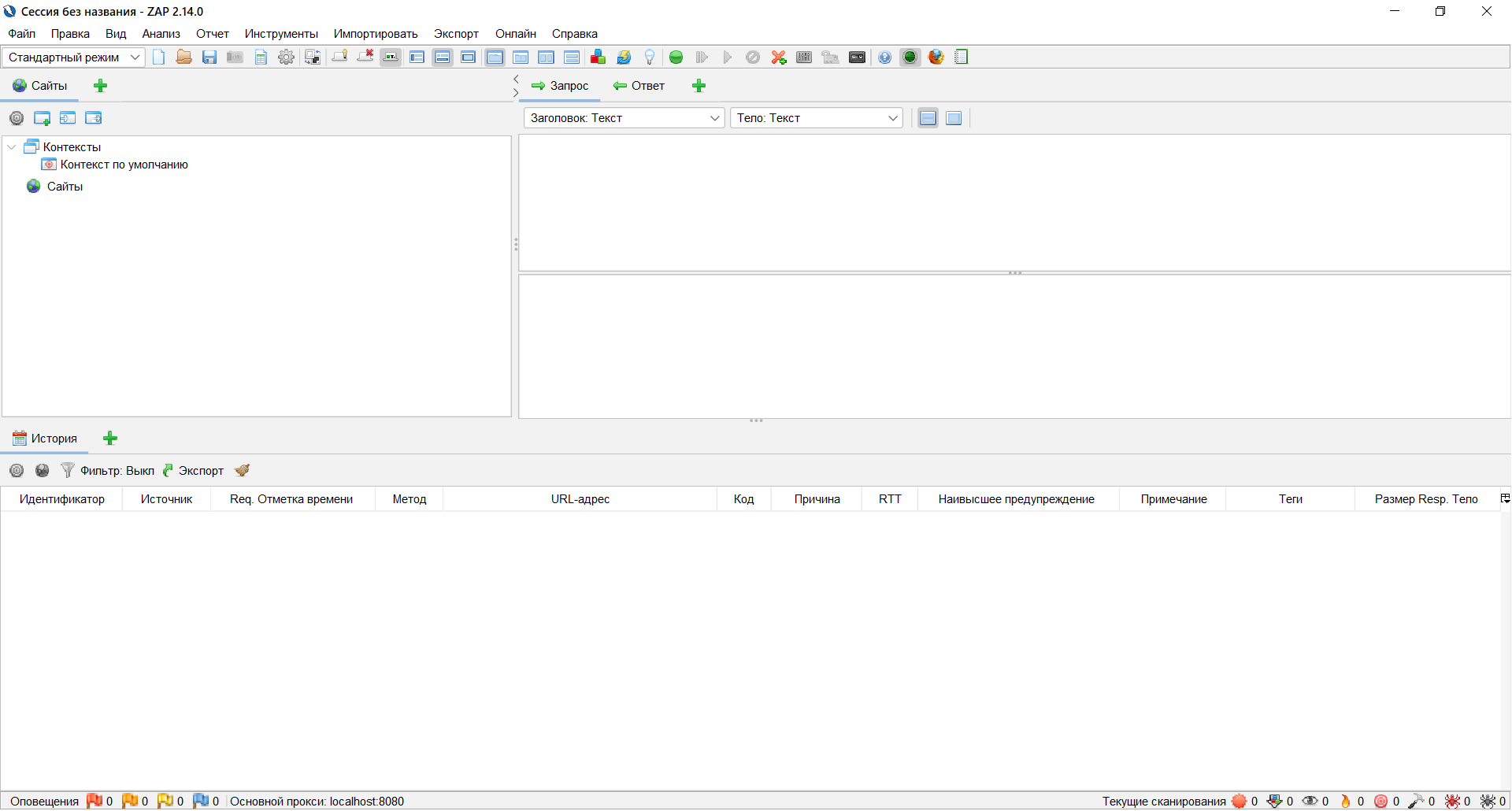
1. Виконайте перевірку веб-додатку за допомогою сканера OWASP ZAP.
2. Проаналізуйте результати сканування.
3. Надайте у звіті дані про найзначніші вразливості, що потрапили у звіт сканера.

**Індивідуальне завдання**

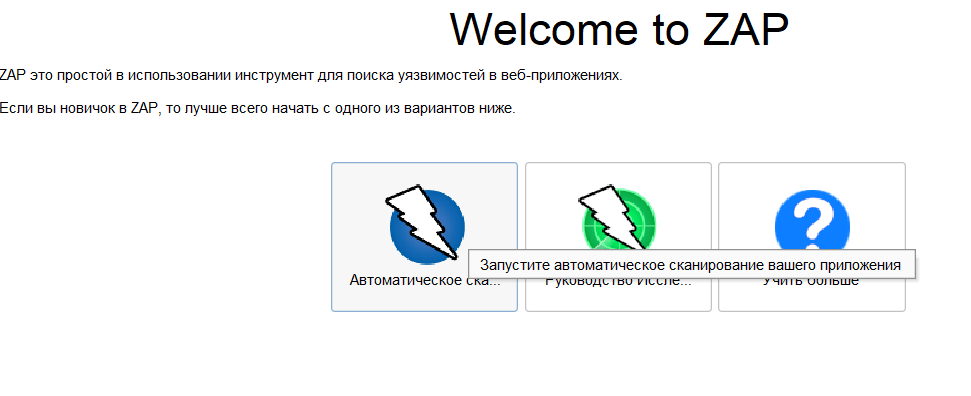
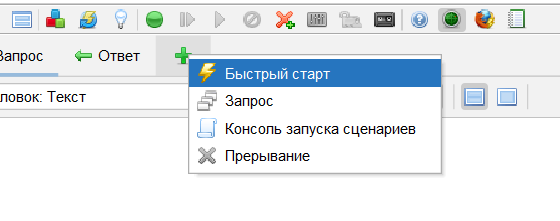
Для аналізу було обрано веб-додаток, який запускається на локальному сервері та придназначенний для створення та інтерактивної розробки програм на різних мовах програмування, найпопулярніша з яких – це Python.

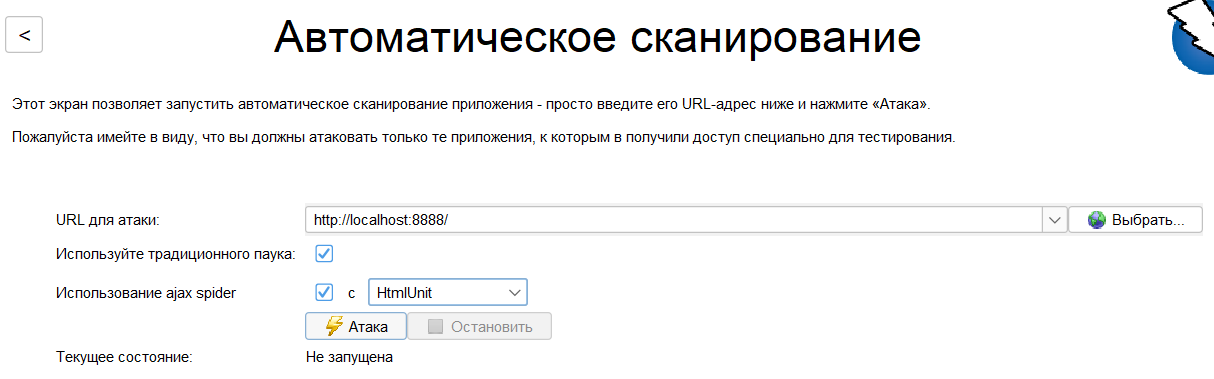
**Пошук вразливостей веб-додатку за допомогою OWASP ZAP**

1. Запускаємо наш веб-додаток для аналізу а також програму ZAP.

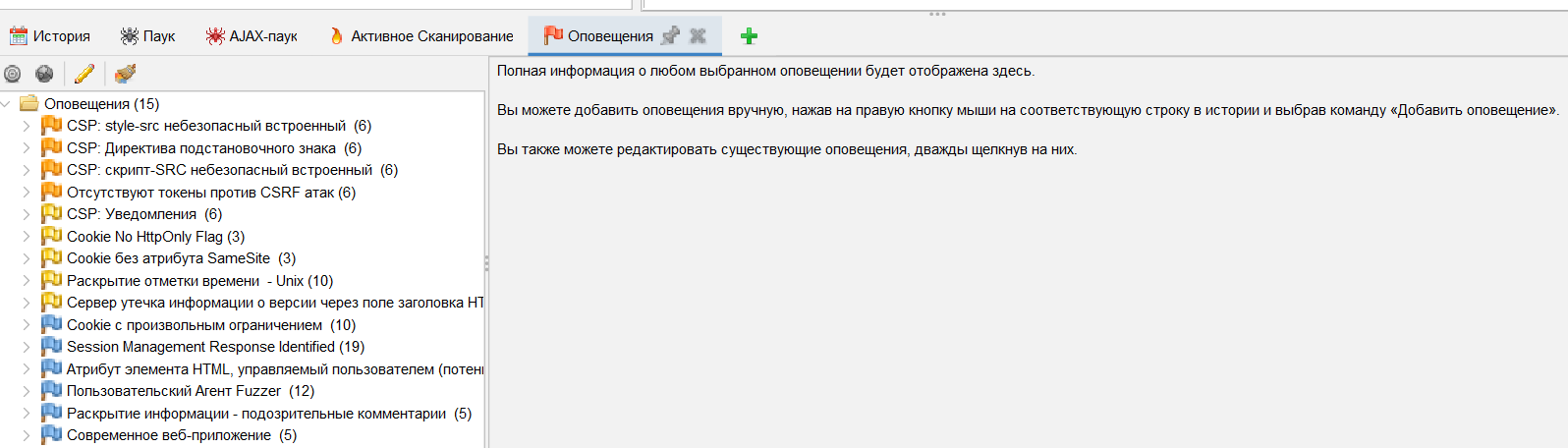


1. Жмемо на швидкий старт та вказуємо адресу на локалхості, де запущено наший додаток, а також деякі налаштування, зображені на скріні та тиснемо на кнопку атака.



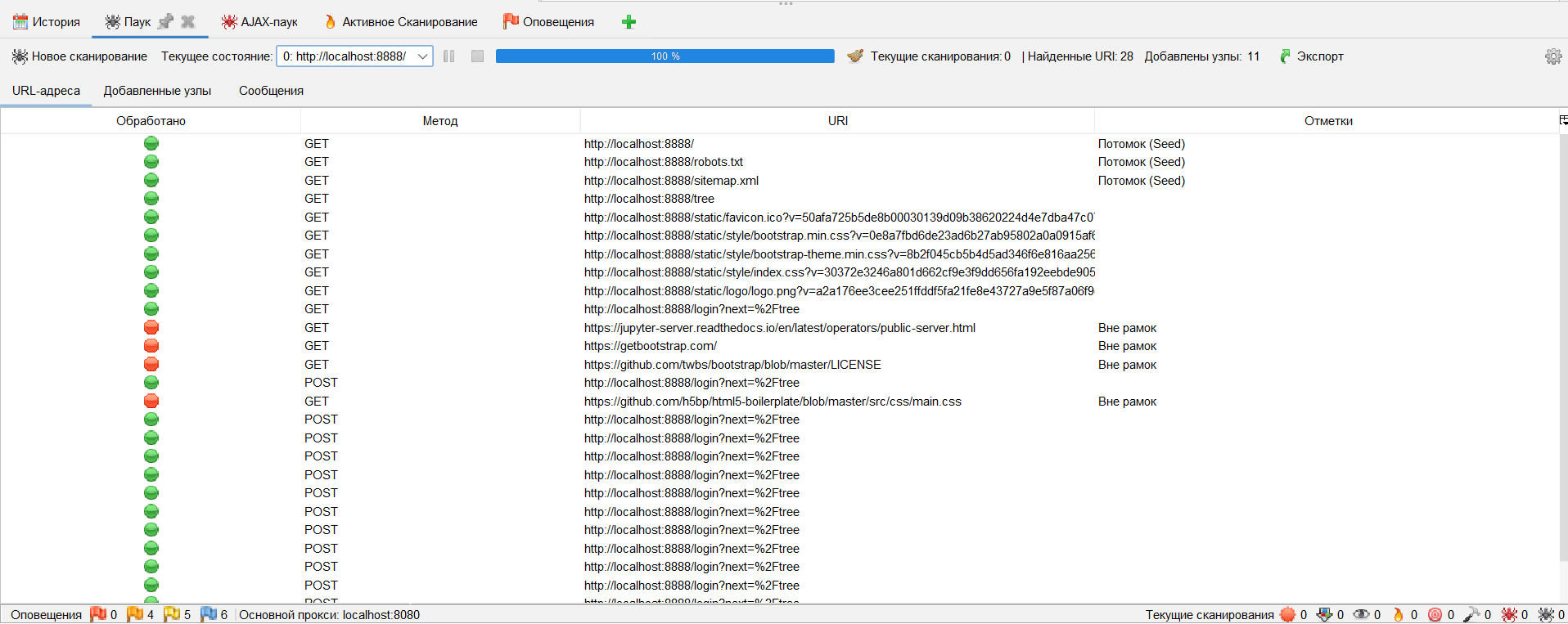


1. Після того як натиснуто кнопку атаки побачимо результати її.

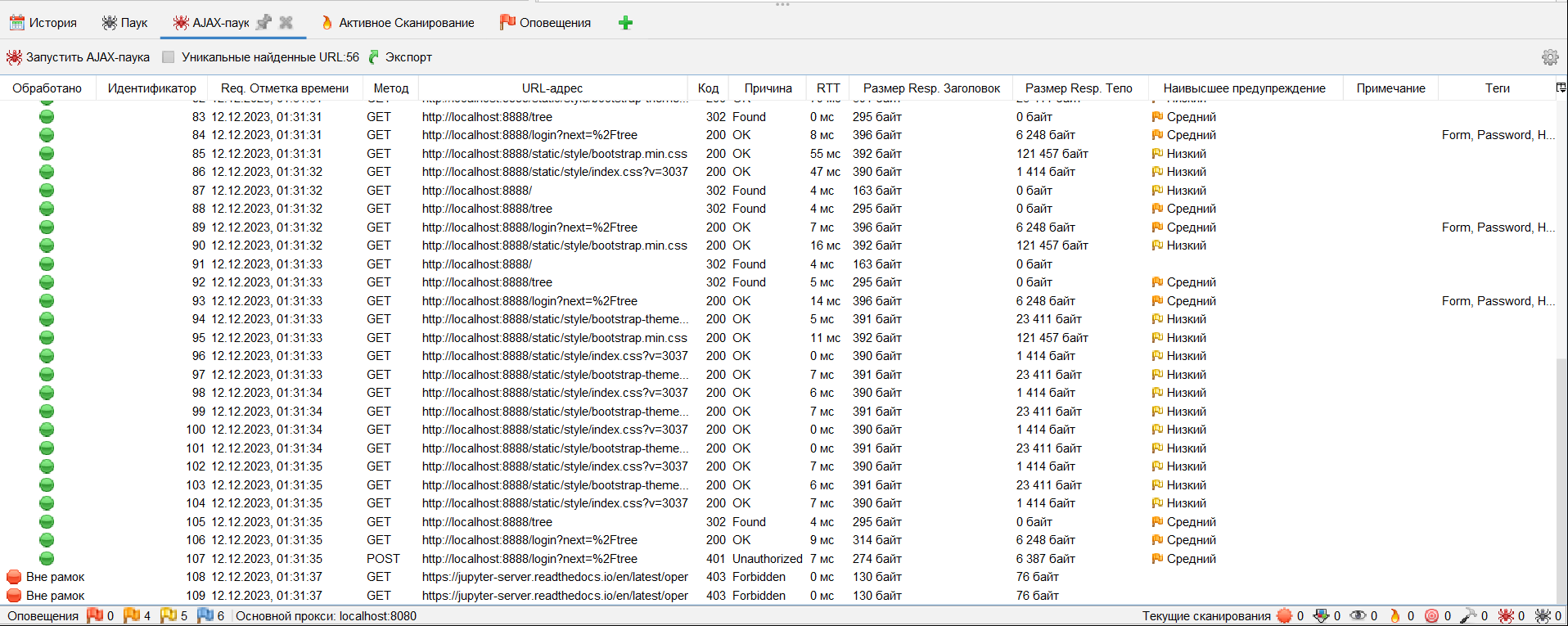


**Аналіз результатів сканування**

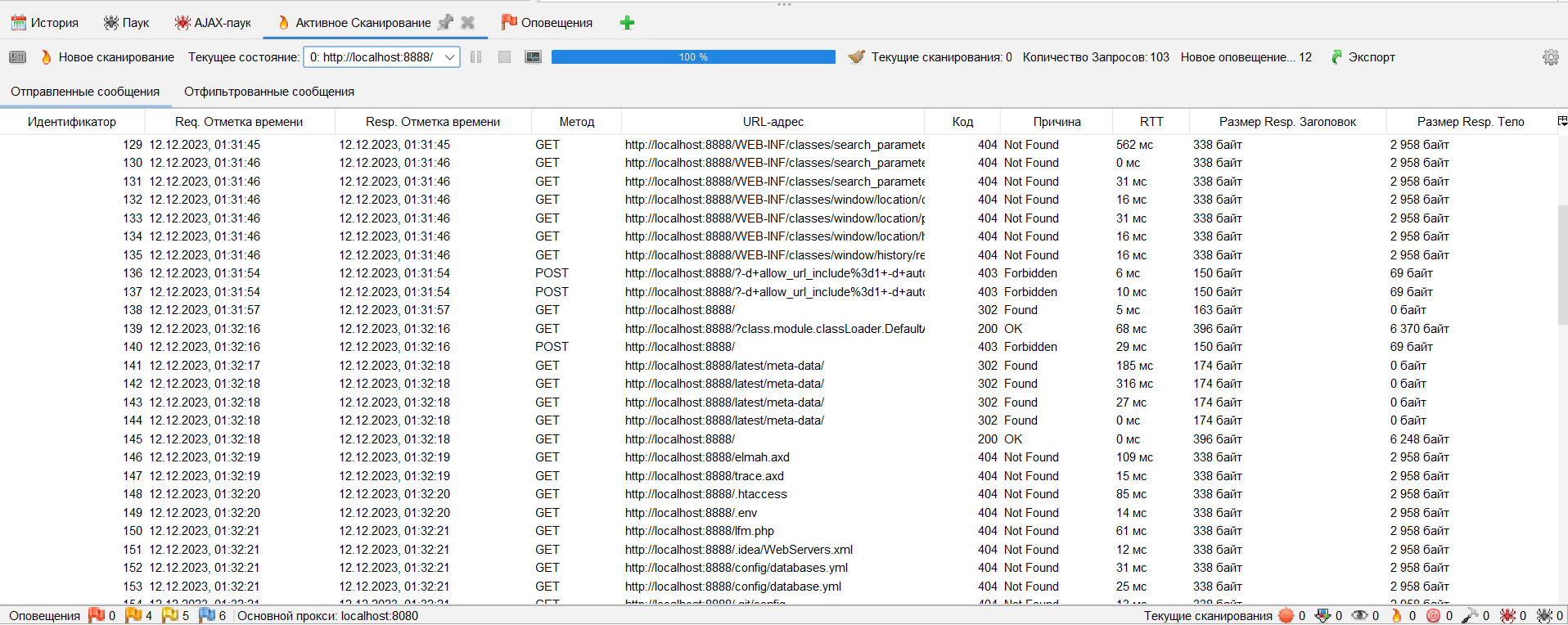
1. Результати сканування за допомогою павука методів GET та POST. Зеленим відмічені методи які повернули статус 200, а червоним відповідно 400 та 500.

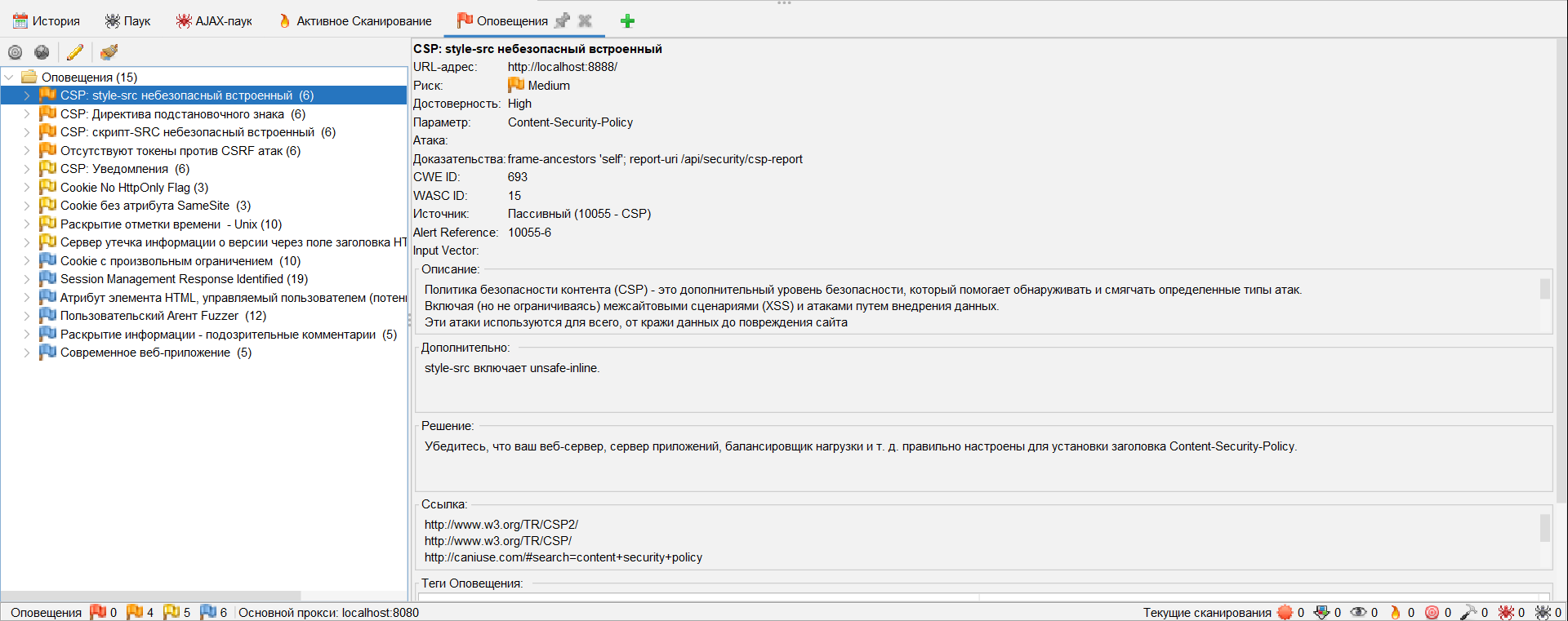


1. Результати сканування за допомогою AJAX павука. Зеленим відмічені методи які повернули статус 200, а червоним відповідно 400 та 500. Тут вже міститься більше інформації, час, що повернув метод, рівень попередження, розмір заголовку тип методу та теги.



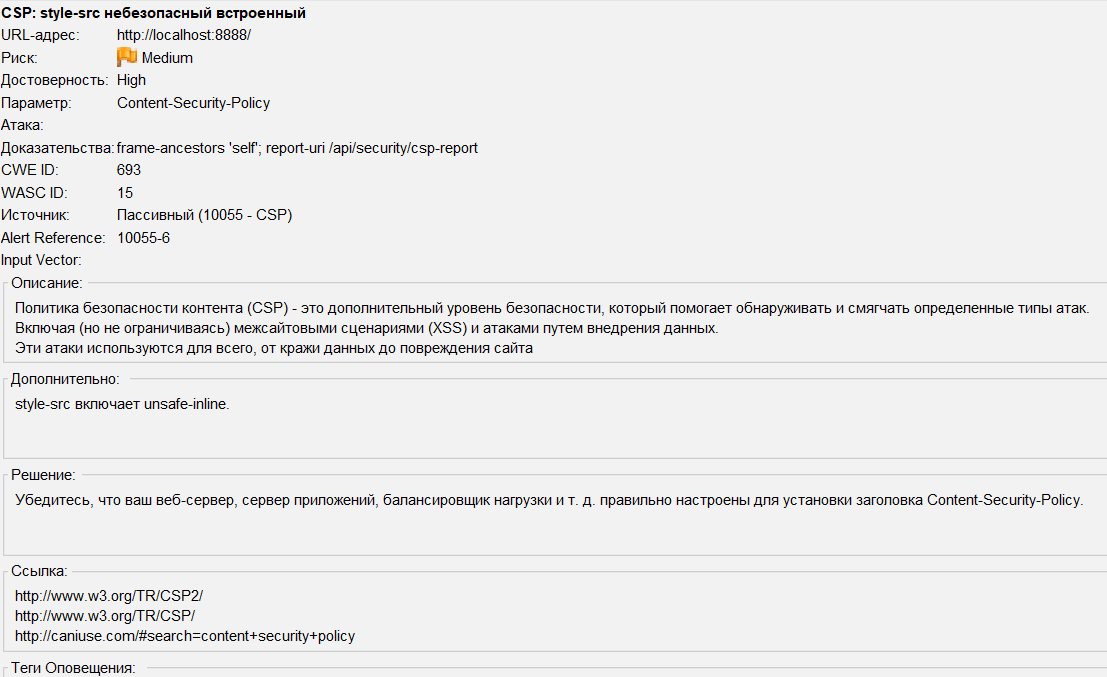
1. Активне сканування також вміщує в собі багато інформації, такої ж як і AJAX павук.

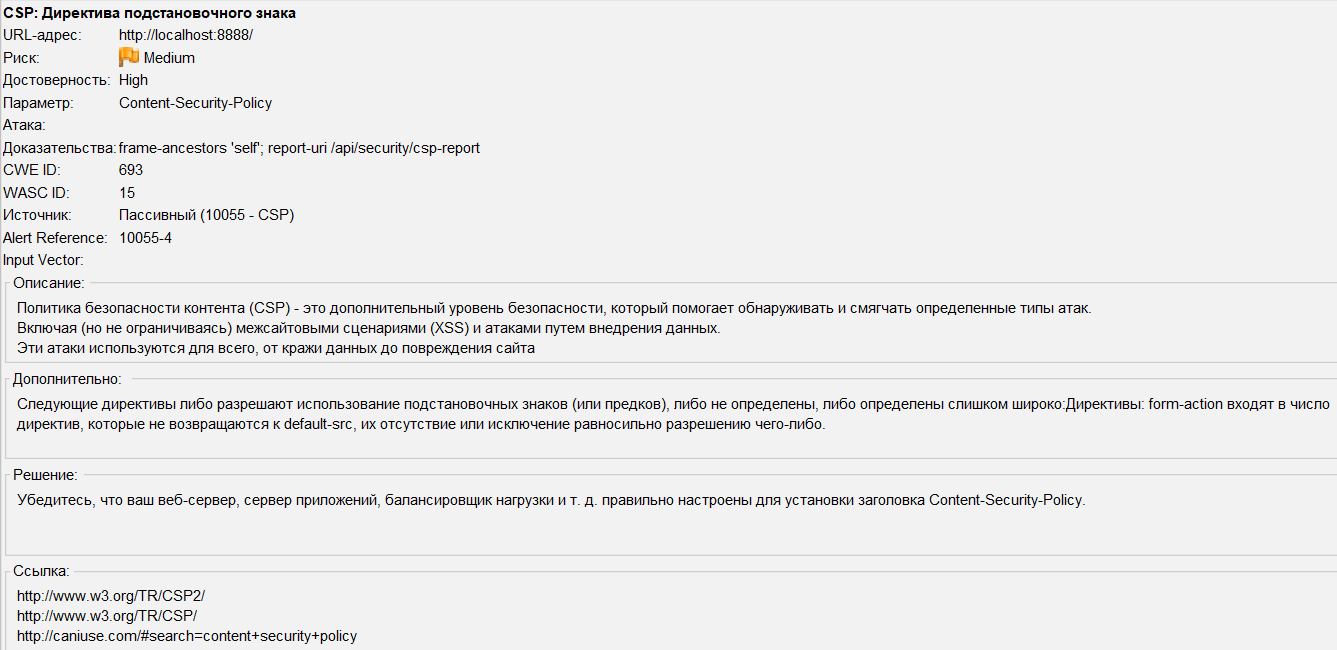


1. У сповіщеннях знаходяться всі попередження, а також детальна інформація про них.  
     
   

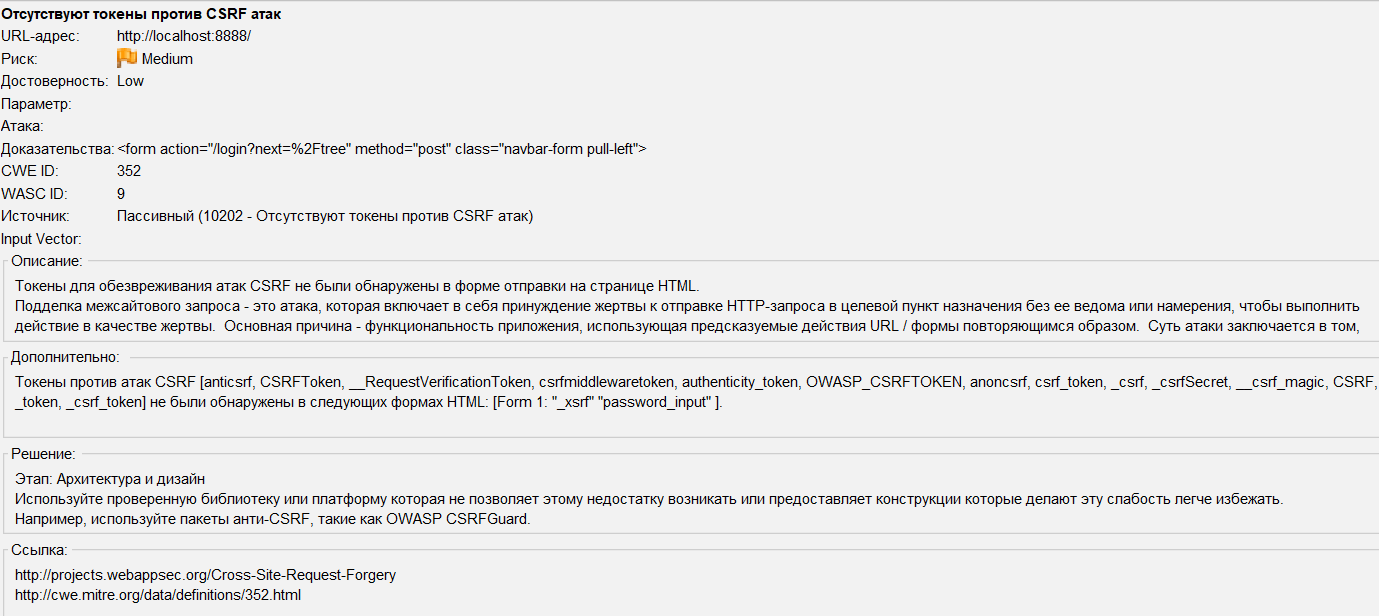
**Аналіз найзначніших знайдених вразливостей**

Під час дослідження додатку було виявленно 4 вразливості середнього рівня(medium). Детальна інформація про них виводиться у програмі, та вона є дуже вмістовною. Нижче наведені найзначніші вразливості:









**Висновки**

OWASP ZAP виявився ефективним інструментом для визначення та аналізу вразливостей веб-додатків. Зручний інтерфейс, висока ефективність виявлення ризиків, розширюваність та налаштування роблять його привабливим для користувачів. Детальна документація та активна спільнота сприяють швидкому вивченню та використанню. Система звітів надає докладну інформацію про вразливості, що допомагає забезпечити безпеку веб-додатків. OWASP ZAP - потужний інструмент для підвищення безпеки веб-проектів.