

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ  
Кафедра кібербезпеки

**Звіт до лабораторної роботи № 11**  
**на тему “Використання сканера уразливостей OWASP ZAP для тестування веб-ресурсів”**

**Виконав студент(ка)**

Борщ Дмитро

**Група**

КБ-01

**Перевірила**

Лаврик Т.В.

**«Використання сканера уразливостей OWASP ZAP  
для тестування веб-ресурсів»**

**Завдання 1 (платформа Range Force).** Виконати модулі:

- OWASP ZAP: Basics
- Testing With OWASP ZAP
- OWASP Zed Attack Proxy Overview

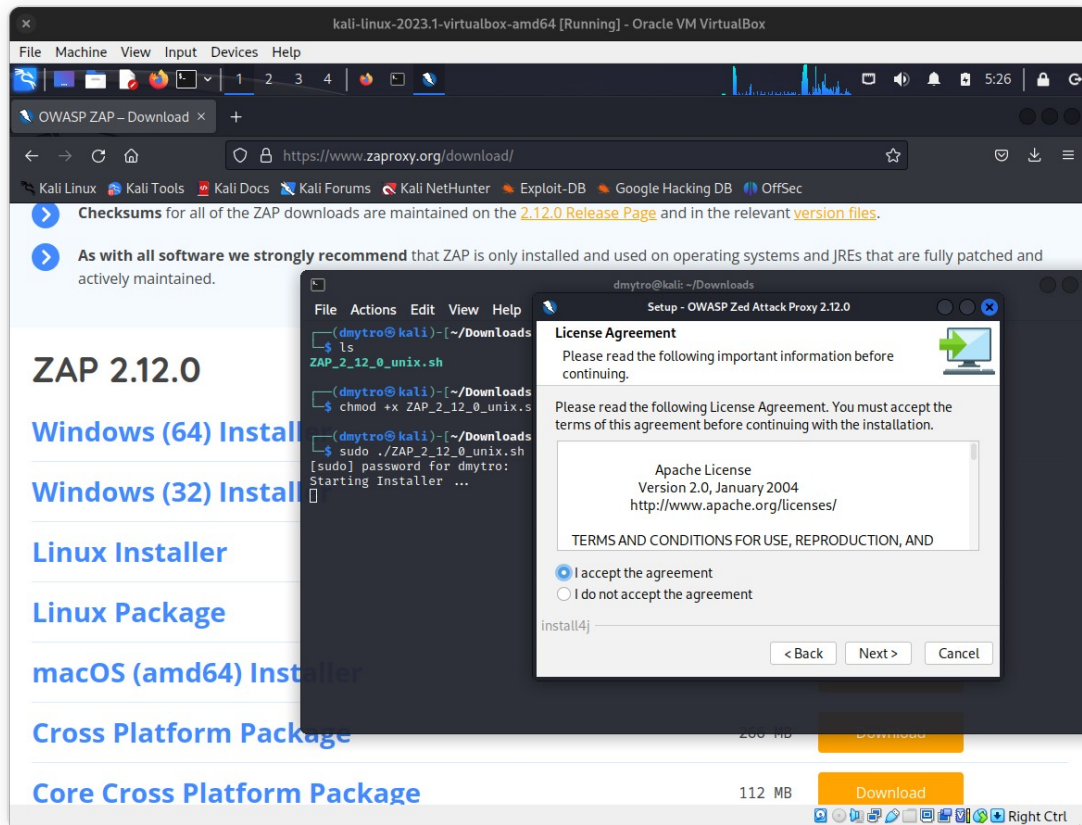
**Завдання 2. Встановлення OWASP ZAP**

1. Запустити віртуальну машину Kali Linux.

2. Завантажити OWASP ZAP з сайту <https://www.zaproxy.org/download/>. Обрати Linux Installer.

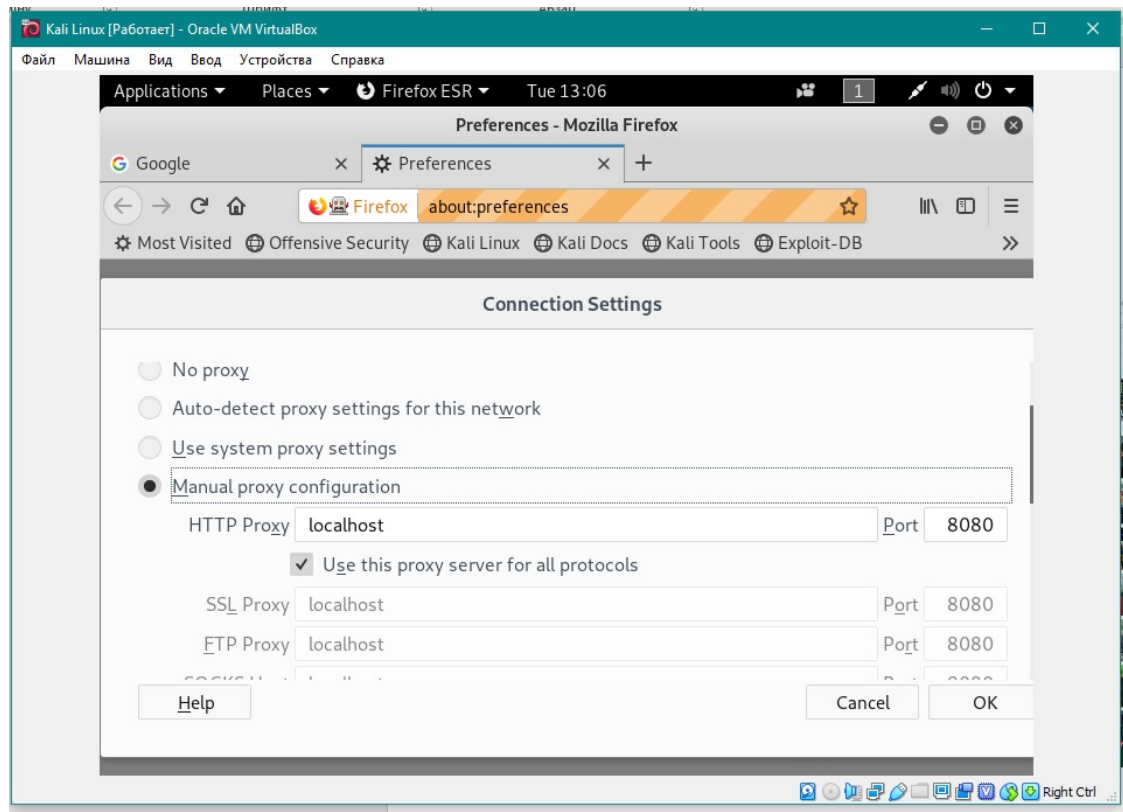
3. Встановити OWASP ZAP в Kali Linux. Один зі способів наведено нижче. Команди вводити від імені користувача з root правами. Послідовність команд наведена нижче.

- sudo bash (sudo su)
- cd Downloads
- ls
- chmod +x ZAP\_2\_11\_1\_unix.sh
- ./ZAP\_2\_11\_1\_unix.sh



4. OWASP ZAP не є повністю самостійними, так як для своєї роботи він взаємодіє з браузером. Тому необхідно налаштувати браузер (наприклад, Firefox) на використання проксі.

5. Відкрити Firefox, «Preferences» → Network Proxy. Встановити налаштування:



6. Через пошуковий рядок у списку додатків знайти OWASP ZAP і запустити.

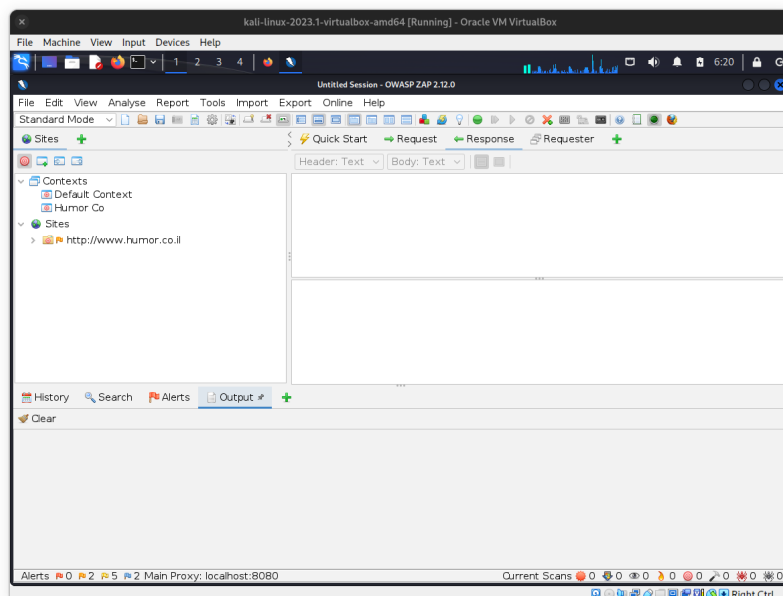
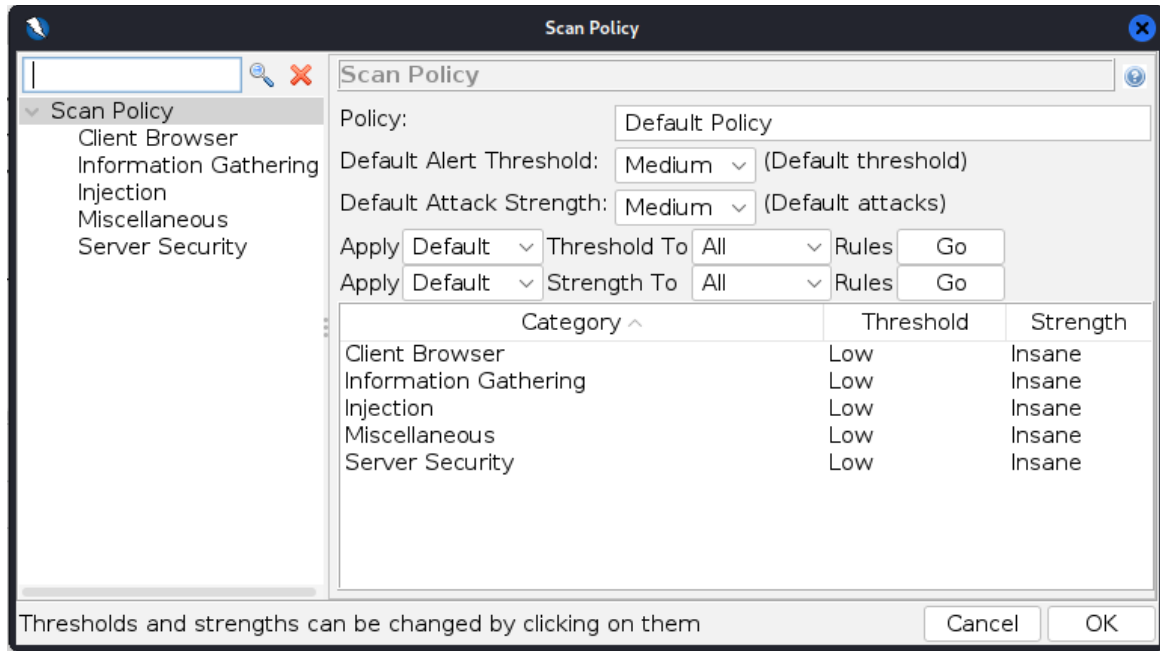


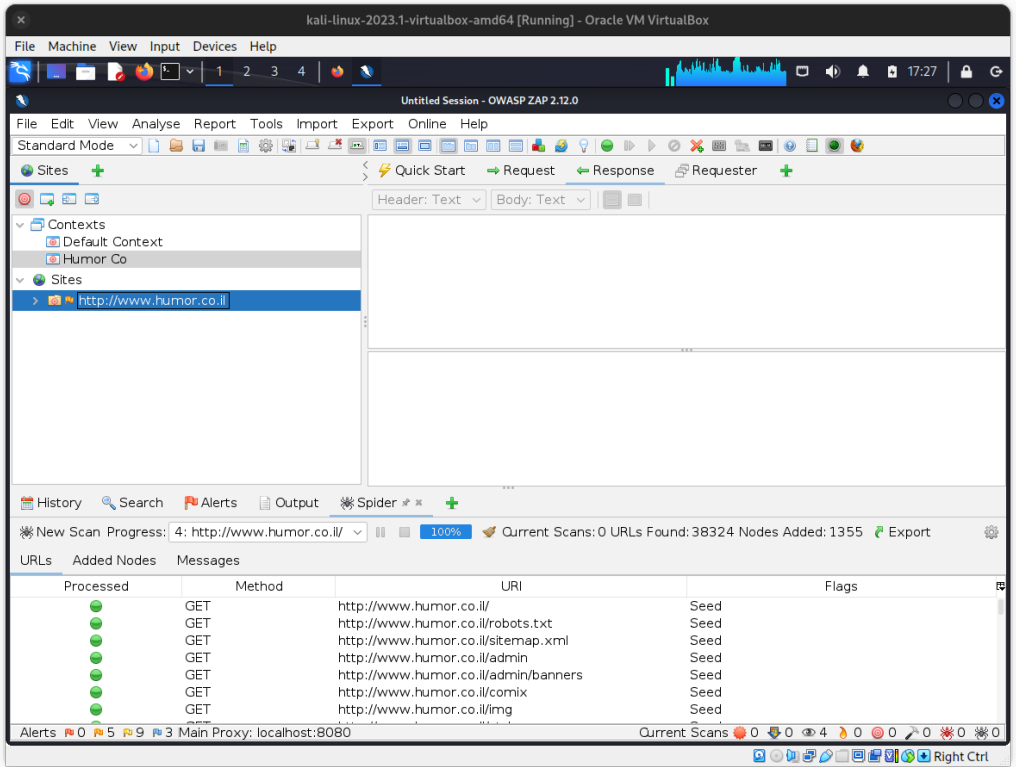
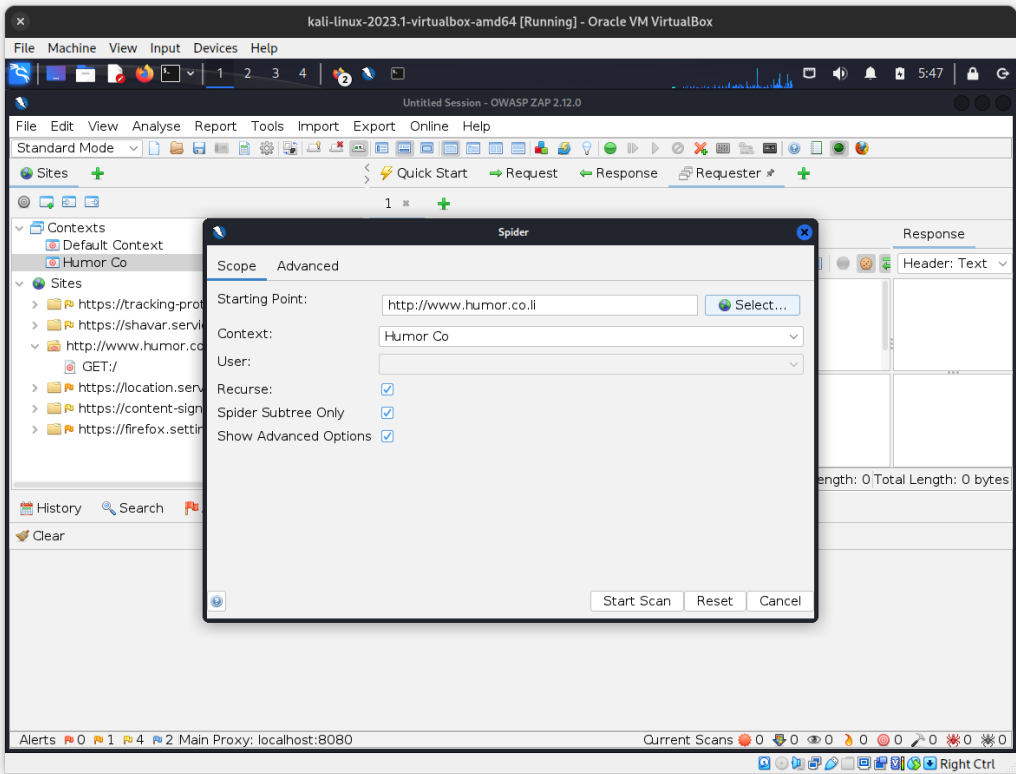
### Завдання 3. Проведення сканування з OWASP ZAP

7. У вікні додатку ZAP встановити стандартний режим (Standard Mode).

8. Для проведення сканування цільового сайту спочатку скористайтеся інструментом Spider.

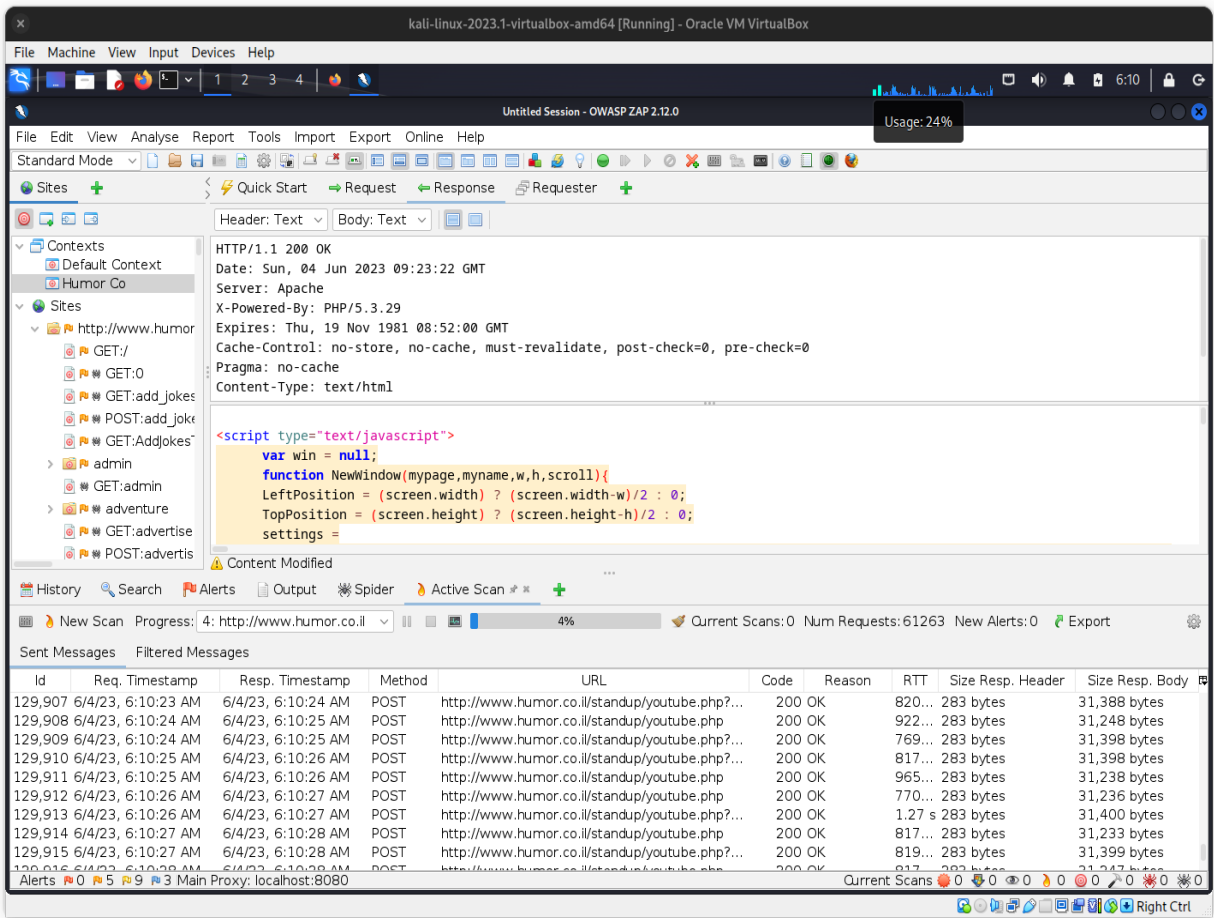
*Примітка: Для проведення сканування індивідуальний цільовий ресурс призначається викладачем.*



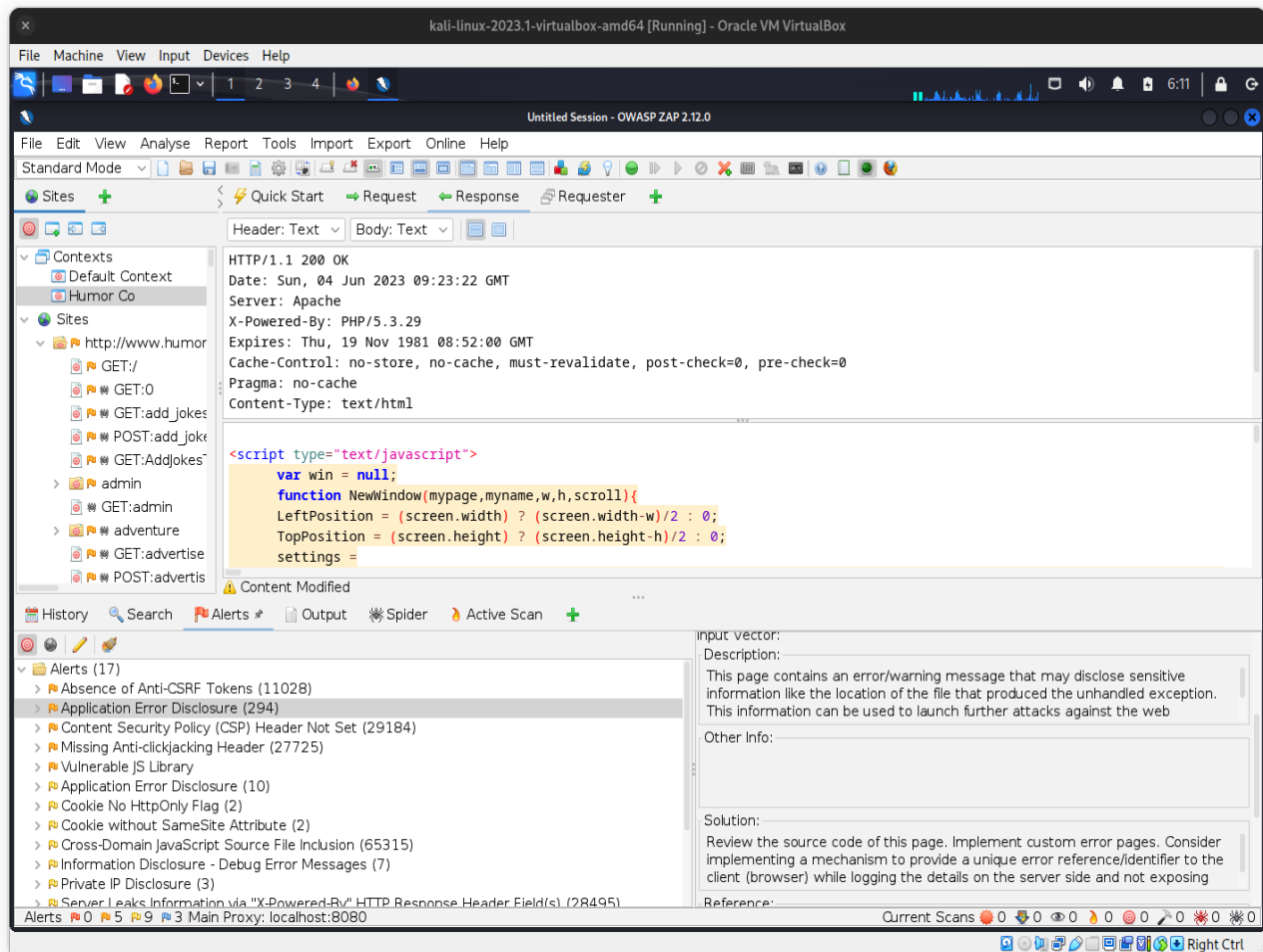


9. Проведіть сканування цільового сайту за допомогою Active Scan.

Через те, що сайт має дуже велику кількість сторінок, довелося зупинити сканування через 12 годин після початку на результаті в 61263 запити та лише 4% оброблених сторінок, що знайшов Spider.



10. Після проведеного тестування на вкладці «Alerts» проаналізуйте отримані оповіщення.





Таблиця 1. Попередження з високим пріоритетом

№	Назва уразливості	Кількість, знайдених вразливостей
-	-	-

Таблиця 2. Попередження із середнім пріоритетом

№	Назва уразливості	Кількість, знайдених вразливостей
1	Absence of Anti-CSRF Tokens	11028
2	Application Error Disclosure	294
3	Content Security Policy (CSP) Header Not Set	29184
4	Missing Anti-clickjacking Header	27725
5	Vulnerable JS Library	1

Таблиця 3. Попередження із низьким пріоритетом

№	Назва уразливості	Кількість, знайдених вразливостей
1	Application Error Disclosure	10
2	Cookie No HttpOnly Flag	2
3	Cookie without SameSite Attribute	2
4	Cross-Domain JavaScript Source File Inclusion	65315
5	Information Disclosure - Debug Error Messages	7
6	Private IP Disclosure	3
7	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	28495
8	Timestamp Disclosure - Unix	8
9	X-Content-Type-Options Header Missing	28707

Таблиця 4. Попередження з інформаційним пріоритетом

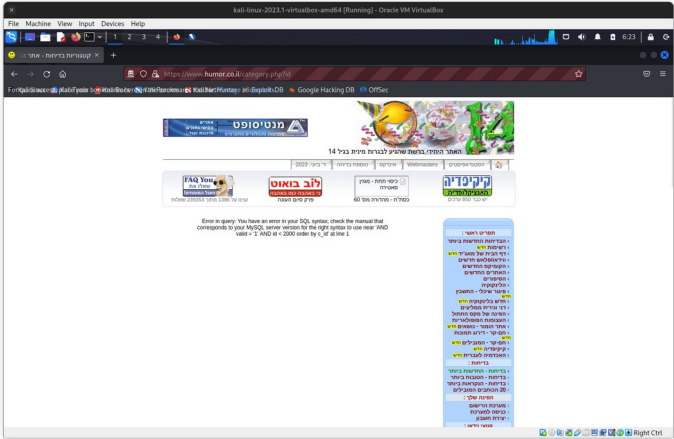
№	Назва уразливості	Кількість, знайдених вразливостей
1	Information Disclosure - Suspicious Comments	2709
2	Modern Web Application	25825
3	User Controllable HTML Element Attribute (Potential XSS)	18497

11. Оберіть по одній уразливості з високим та середнім пріоритетом та проведіть аналіз зібраної в OWASP ZAP інформації про уразливість за такими критеріями:

- фрагмент коду,
- URL-посилання,
- вразливий параметр,
- приклад атаки на параметр,
- короткий опис виявленої уразливості.

12. Заповніть таблиці:

Уразливість 1: **Application Error Disclosure**

Пріоритет	Medium
URL-адреса	http://www.humor.co.il/category.php?id
Уразливий параметр	-
Спосіб перевірки	Ця сторінка містить повідомлення про помилку/попередження, яке може розкривати конфіденційну інформацію, як-от розташування файлу, який створив необроблену виняткову ситуацію. Цю інформацію можна використовувати для подальших атак на веб-програму. Сповіщення може бути помилковим, якщо повідомлення про помилку знайдено на сторінці документації
Скріншот	

Уразливість 2: **Vulnerable JS Library**

Пріоритет	Medium
URL-адреса	http://www.humor.co.il/js/prototype.js
Уразливий параметр	-
Спосіб перевірки	Виявлена бібліотека prototypejs, версія 1.4.0 є вразливою.
Скріншот	