|  |  |
| --- | --- |
| Logo  Description automatically generated | THỰC HÀNH ATTT  Kiểm thử bảo mật Web&API bằng công cụ OWASP ZAP |

Họ và tên Sinh viên:

Mã Sinh viên: Nhóm:

[1. Giới thiệu 1](#_Toc177215174)

[2. Cài đặt Owasp ZAP 2](#_Toc177215175)

[3. Sử dụng Owasp ZAP để quét và kiểm tra bảo mật Website 2](#_Toc177215176)

[3.1 Tab Quick Start 2](#_Toc177215177)

[3.2 Tab Active Scan 3](#_Toc177215178)

[3.3 Tab Alerts 4](#_Toc177215179)

[3.4 Tab History 5](#_Toc177215180)

[3.5 Tab Sites 5](#_Toc177215181)

[3.6 Tab Statistics 5](#_Toc177215182)

[3.7 Menu Report 6](#_Toc177215183)

[3.7.1 Tạo báo cáo kết quả kiểm thử 6](#_Toc177215184)

[3.8 Menu Views 7](#_Toc177215185)

[3.9 Menu Tools 7](#_Toc177215186)

[4. Kiểm thử Website từ trình duyệt thông qua local proxy OWASP Zap 7](#_Toc177215187)

[4.1 Thiết lập Local Proxy 7](#_Toc177215188)

[4.2 Truy xuất Website từ trình duyệt Chrome 8](#_Toc177215189)

[5. BÀI TẬP 10](#_Toc177215190)

[6. Tham khảo 12](#_Toc177215191)

# Giới thiệu

Owasp Zap (OWASP Zed Attack Proxy) là một công cụ Tool Test Security giúp scan và tìm ra lỗ hổng trong hệ thống ứng dụng. ZAP đóng vai trò đứng giữa trình duyệt của người kiểm tra website, để có thể kiểm tra các thông tin được gửi đi cũng như sửa đổi.

Một số tính năng chính của OWASP ZAP :

* Hỗ trợ việc kết nối web (Web sockets support).
* Hỗ trợ nhiều loại ngôn ngữ scripting
* Hỗ trợ Plug-n-Hack (Plug-n-Hack support).
* Xác thực và hỗ trợ phiên (Authentication and session support).
* API dựa trên REST mạnh mẽ (Powerful REST based API).
* Tùy chọn cập nhật tự động (Automatic updating option).
* Integrated and growing marketplace of add-ons.
* Quét tự động (Automated scanner).
* Quét thụ động (Passive scanner).
* Duyệt bắt buộc (Forced browsing).

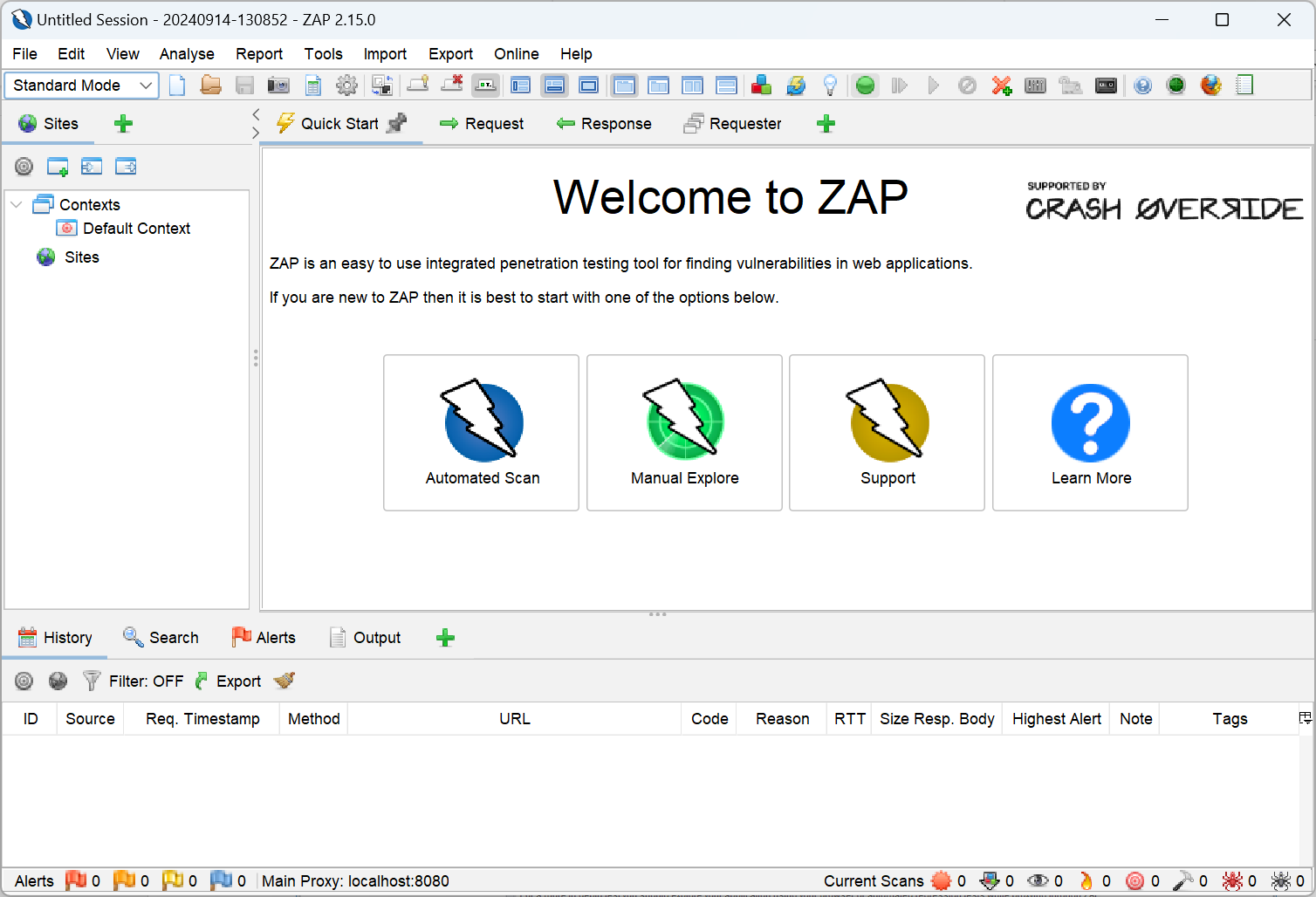
# Cài đặt Owasp ZAP

Cài đặt phiên bản JDK 11 trở lên.

Vào https://www.zaproxy.org và tải xuống phiên bản phù hợp

Khởi động Owasp ZAP: $zaproxy

Xuất hiện giao diện như hình bên dưới



# Sử dụng Owasp ZAP để quét và kiểm tra bảo mật Website

Lựa chọn Website kiểm thử và quét từ Owasp ZAP

## Tab Quick Start

* Trong OWASP ZAP, chọn tab [Quick Start]. Chọn Automated Scan.
* Trong mục URL to attack, nhập URL của Website cần kiểm thử bảo mật.

Ví dụ:

http://testphp.vulnweb.com

http://demo.testfire.net

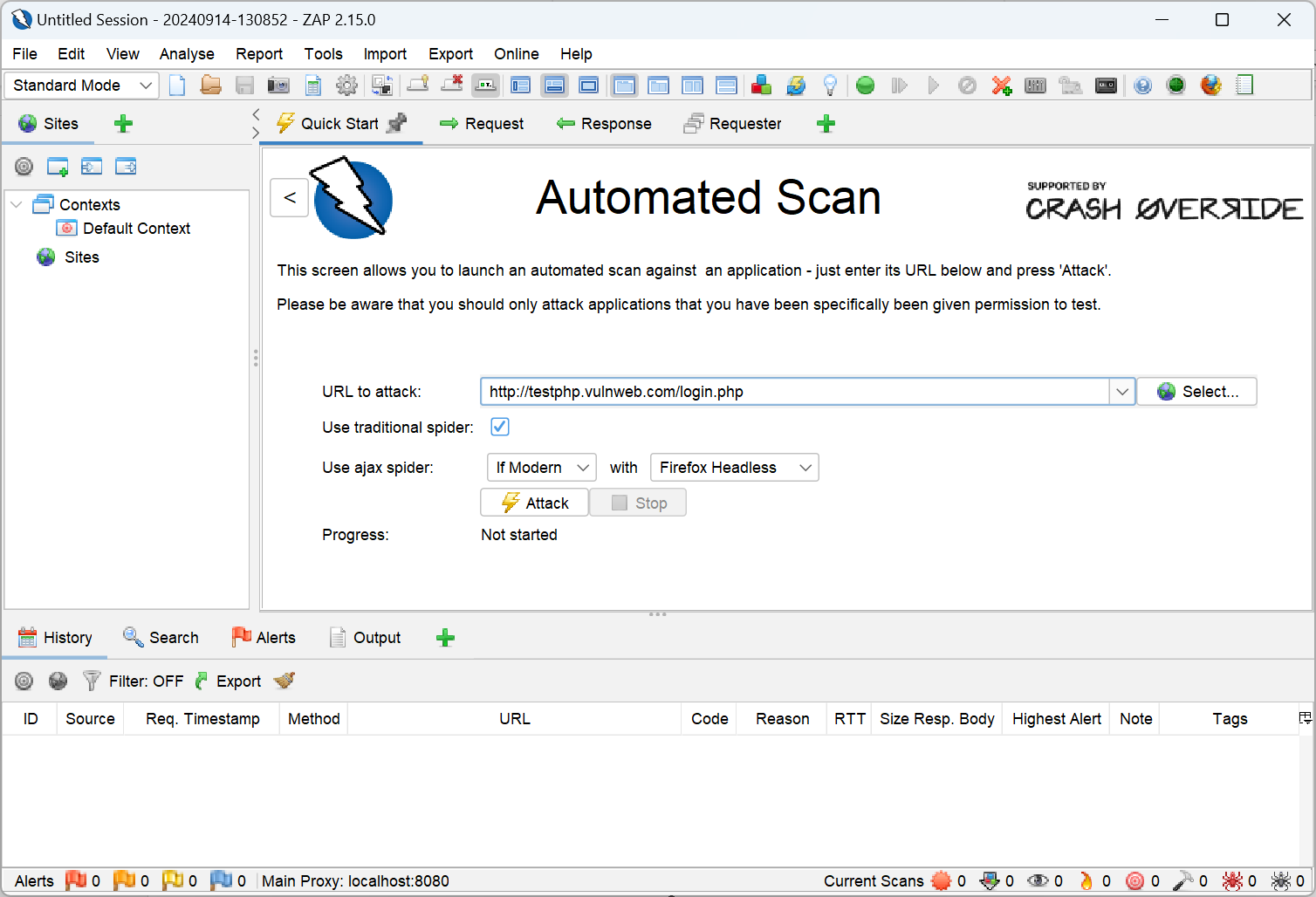
http://php.testsparker.com

http://testasp.vulnweb.com

http://zero.webappsecurity.com

http://testhtml5.vulnweb.com

http://aspnet.testsparker.com



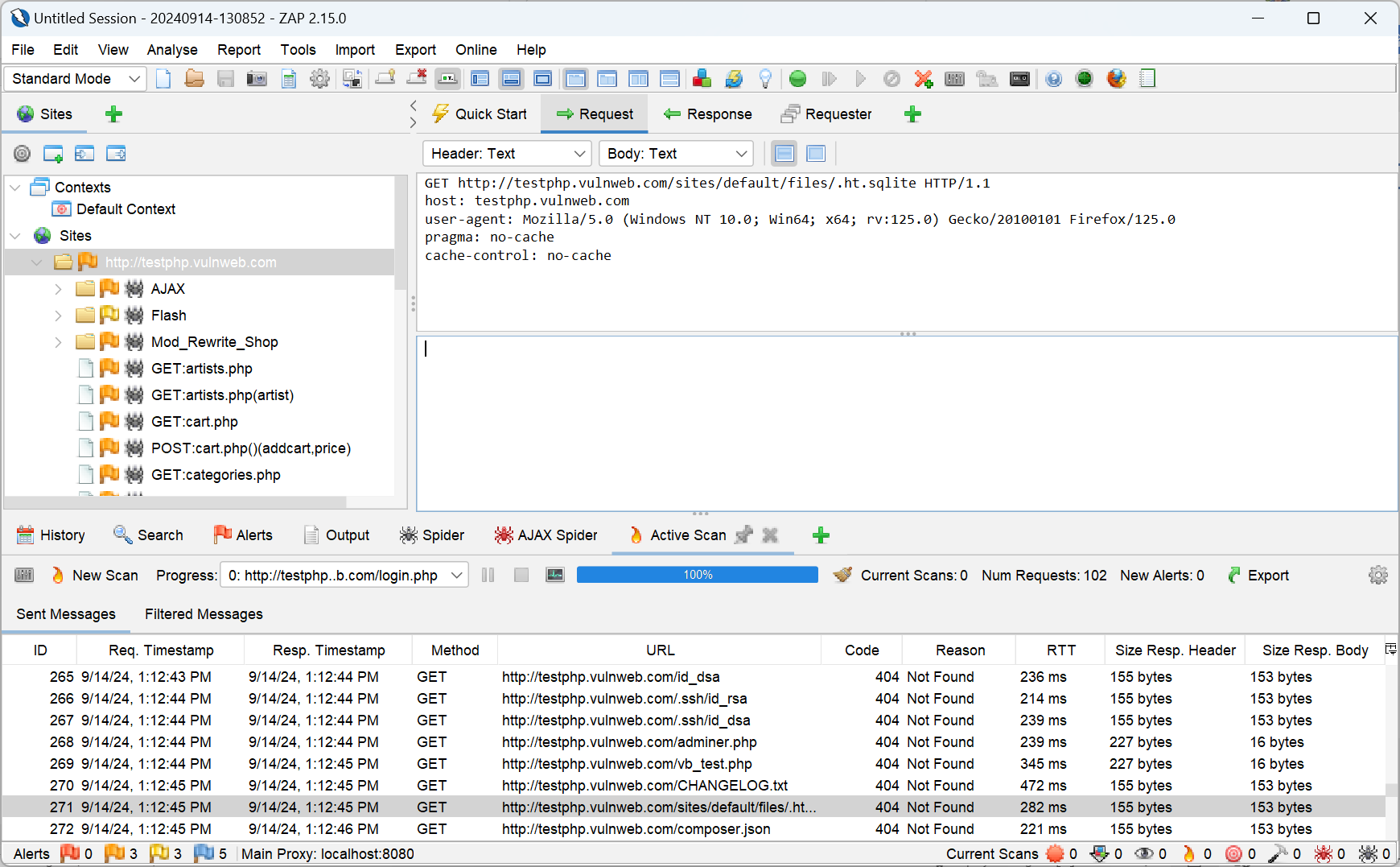
* Nhấn nút Attack để bắt đầu quét Website

>> Khuyến nghị test trên Website được phép test hoặc chạy trên local nếu có thể.

* OWASP ZAP sẽ bắt đầu quét ứng dụng web và tìm kiếm các lỗ hổng bảo mật phổ biến.
* Sau khi quét hoàn tất, NSD có thể xem kết quả quét trong các tab Alerts, Sites, History, …

## Tab Active Scan

* NSD có thể nhấp vào từng mục để xem chi tiết và thông tin liên quan.



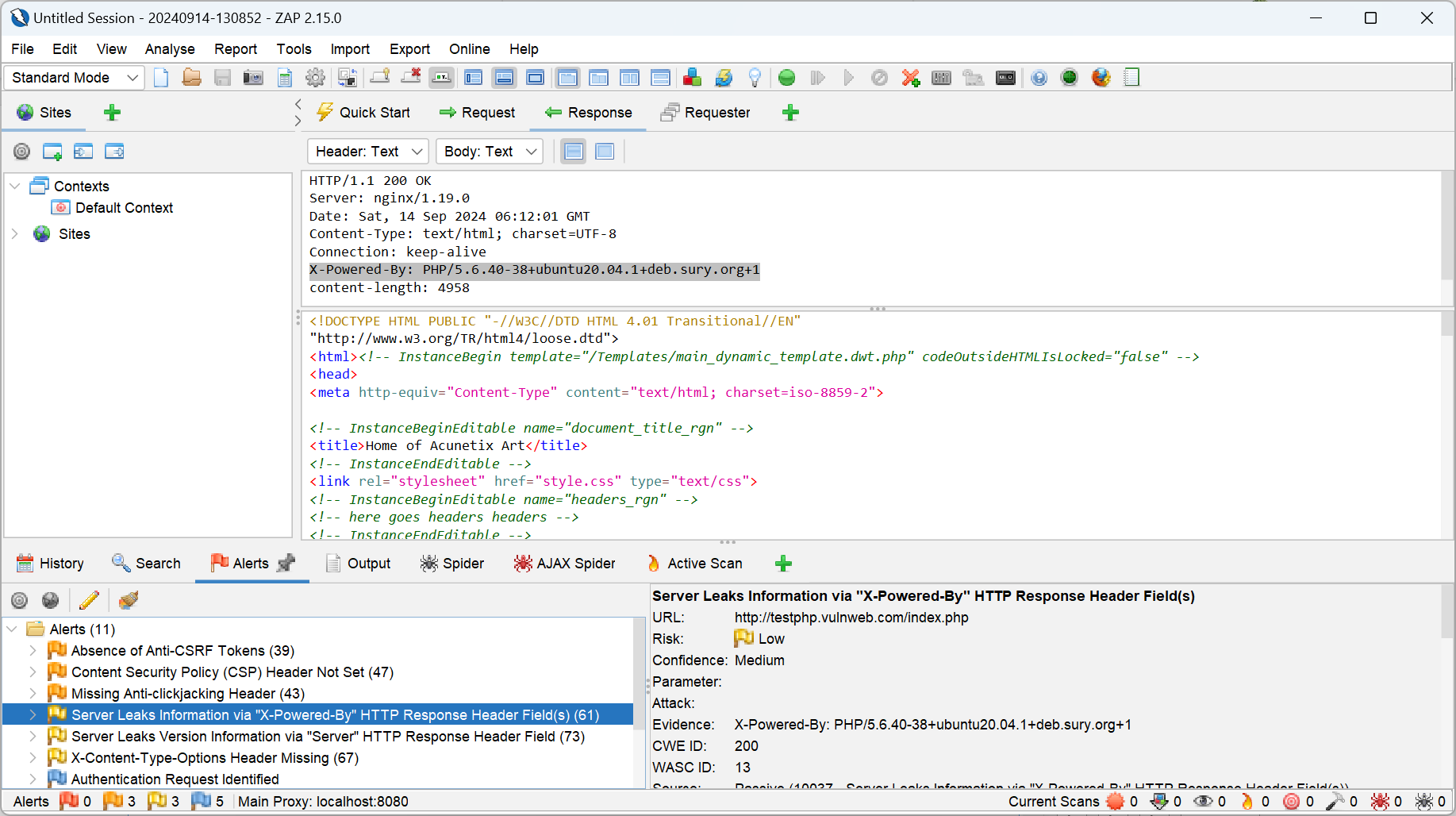
## Tab Alerts

Tab Alerts hiển thị các cảnh báo và lỗ hổng bảo mật tìm thấy trong quá trình quét.

Cung cấp các thông tin sau:

* Mức độ nghiêm trọng (Severity): Đánh giá mức độ nguy hiểm của lỗ hổng bảo mật: Critical, High, Medium, Low.
* Loại lỗ hổng (Vulnerability type): Mô tả loại lỗ hổng bảo mật đã được phát hiện, ví dụ: Cross-Site Scripting (XSS), SQL Injection, Insecure Direct Object References, và nhiều loại khác.
* URL liên quan: Liên kết đến trang web hoặc tài nguyên có chứa lỗ hổng bảo mật.
* Mô tả: Chi tiết về lỗ hổng bảo mật đã được phát hiện, bao gồm cách tấn công có thể được thực hiện và cách khắc phục.

Khi NSD kích chọn đường link và mở trình duyệt bằng OWASP, OWASP sẽ kiểm soát trình duyệt giống như một tool Automation Testing.



*>> SV liệt kê hình ảnh minh chứng, mô tả và nhận xét kết quả.*

## Tab History

Cung cấp các thông tin sau:

* Thời gian quét: Thời điểm và thời gian mà quá trình quét đã diễn ra.
* Số lỗ hổng: Tổng số lỗ hổng bảo mật đã được phát hiện trong quá trình quét.
* Thông tin liên quan: Các thông tin khác liên quan đến quá trình quét, ví dụ: thiết bị hoặc công cụ sử dụng.

*>> SV liệt kê hình ảnh minh chứng, mô tả và nhận xét kết quả.*

## Tab Sites

Cung cấp các thông tin sau:

* URL: Địa chỉ trang web đã được quét.
* Số lần quét: Số lần trang web đã được quét trong quá trình kiểm tra bảo mật.
* Số lỗ hổng: Số lỗ hổng bảo mật đã được phát hiện trong trang web.
* Trạng thái: Trạng thái hiện tại của trang web, ví dụ: hoạt động, không hoạt động, bị chặn.

*>> SV liệt kê hình ảnh minh chứng, mô tả và nhận xét kết quả.*

## Tab Statistics

Cung cấp các thông tin sau:

* Số lượng trang web: Tổng số trang web đã được quét.
* Số lỗ hổng: Tổng số lỗ hổng bảo mật đã được phát hiện trong tất cả các trang web.
* Mức độ nghiêm trọng: Thống kê về số lượng lỗ hổng theo mức độ nghiêm trọng.
* Các thông tin thống kê khác: Có thể bao gồm tỷ lệ lỗ hổng theo loại, biểu đồ thống kê, và thông tin liên quan khác.

*>> SV liệt kê hình ảnh minh chứng, mô tả và nhận xét kết quả.*

## Menu Report

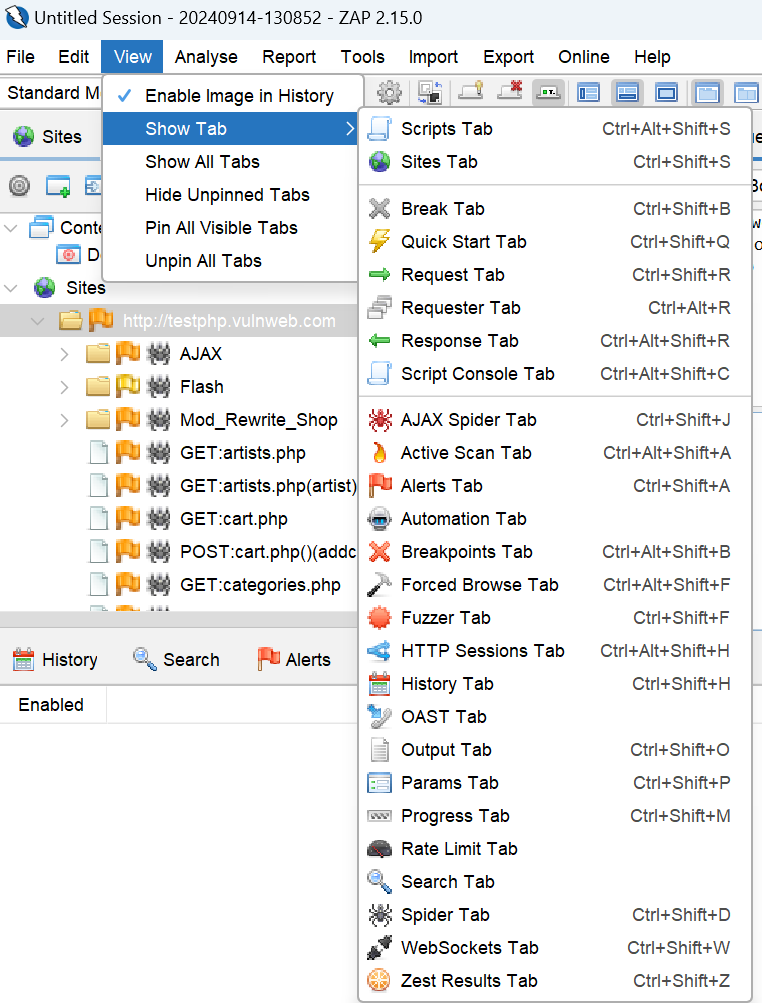
### Tạo báo cáo kết quả kiểm thử

* Có thể tạo báo cáo với tùy biến template của bản report, như định dạng HTML hay XML.
* Chọn menu [Report]/[General Report]



*>> SV liệt kê hình ảnh minh chứng, trích các nội dung quan trọng vào đây.*

## Menu Views



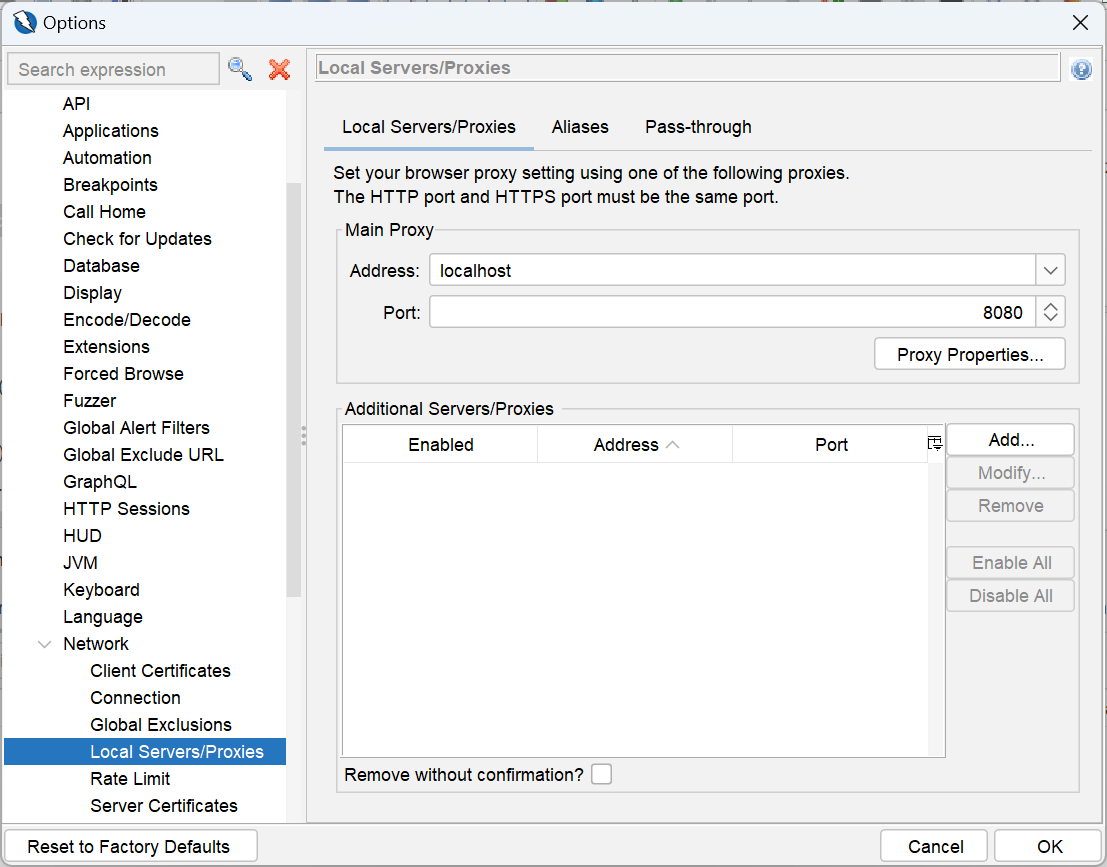
## Menu Tools

# Kiểm thử Website từ trình duyệt thông qua local proxy OWASP Zap

## Thiết lập Local Proxy

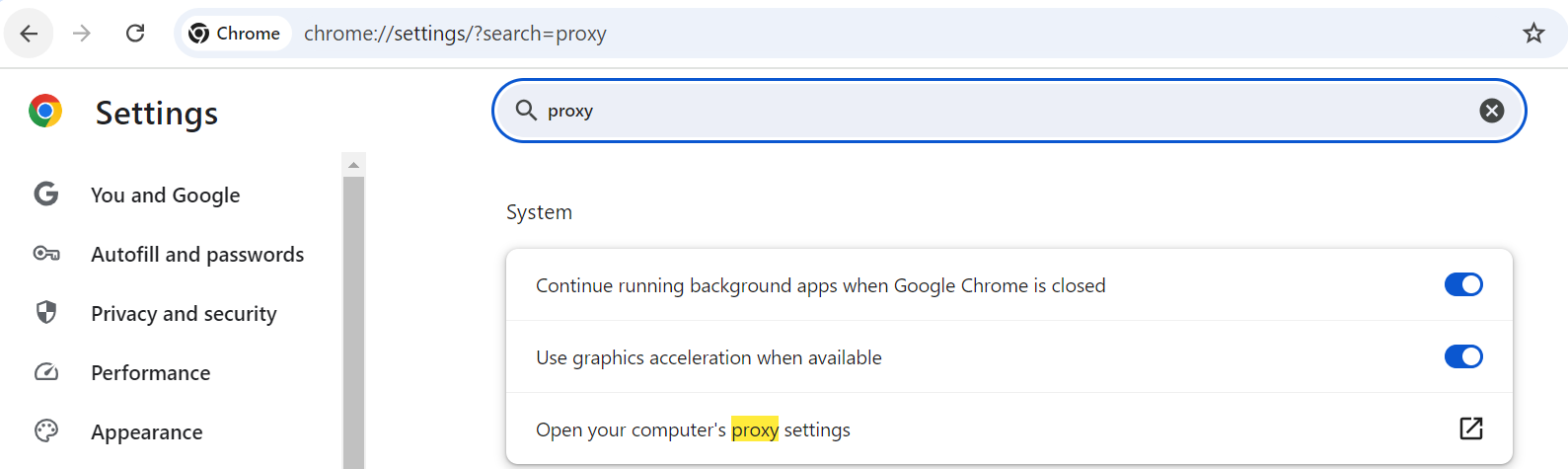
Để OWASP ZAP hoạt động như một proxy server, ta cần cấu hình trình duyệt web để sử dụng proxy này.

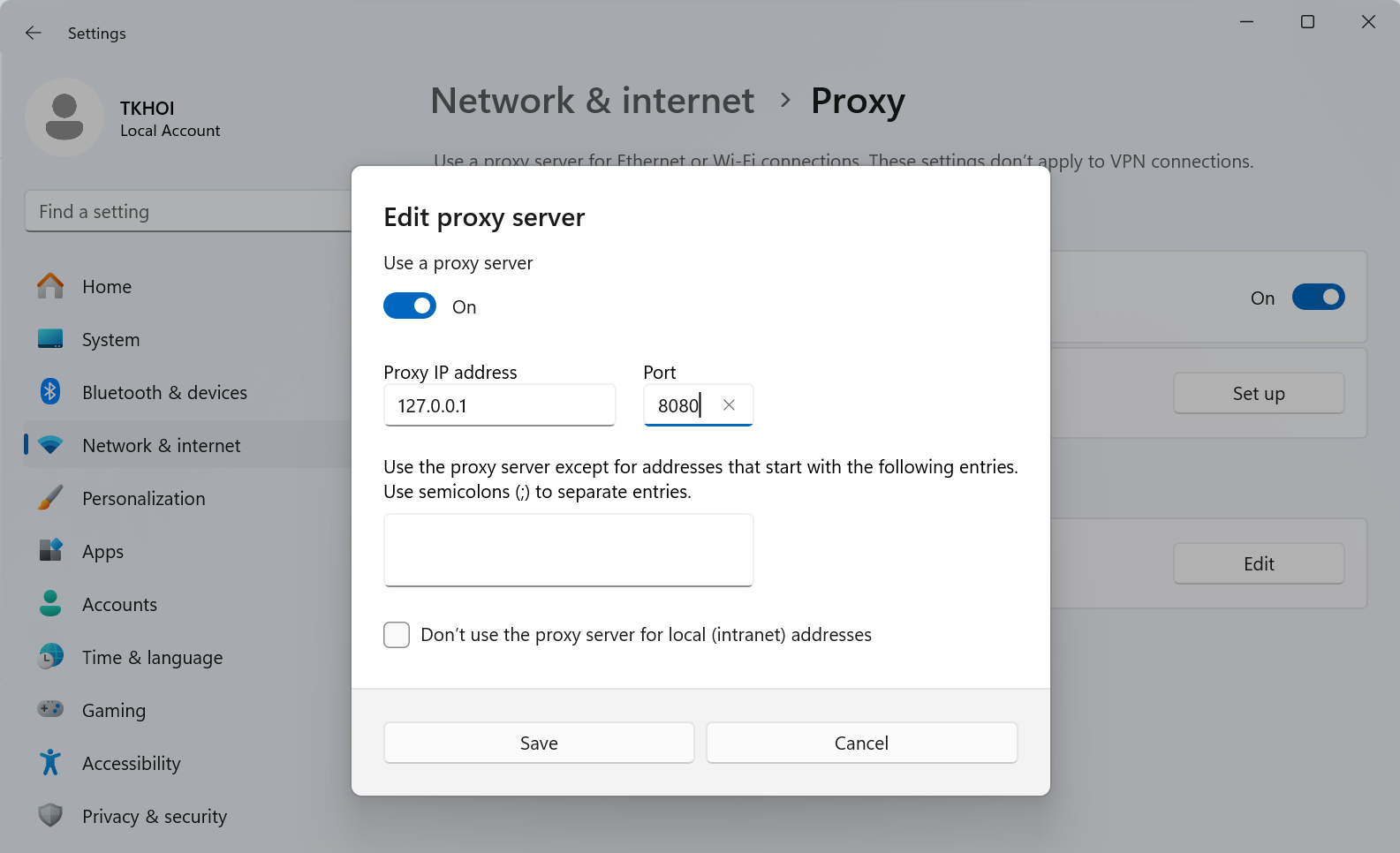
* Trong OWASP ZAP, chọn menu [Tools]/[Options]
* Trong Tab Options, chọn Local Servers/Proxies, mặc định port: 8080



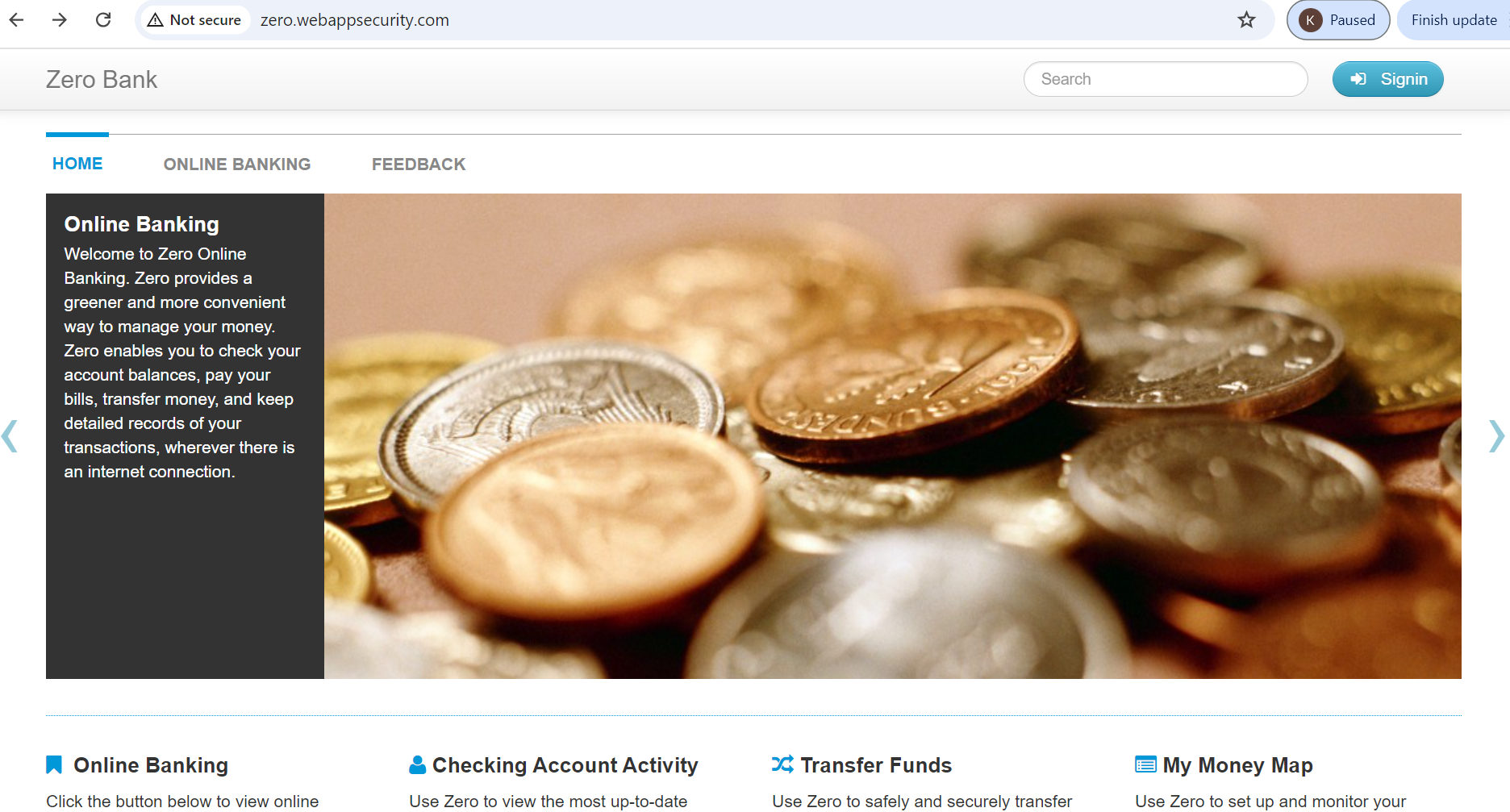
## Truy xuất Website từ trình duyệt Chrome

* Mở trình duyệt web (Ex: Chome), chọn mục **Settings**, gõ tìm proxy và thiết lập địa chỉ proxy thành localhost và cổng proxy là cổng OWASP ZAP đã chỉ định (8080).

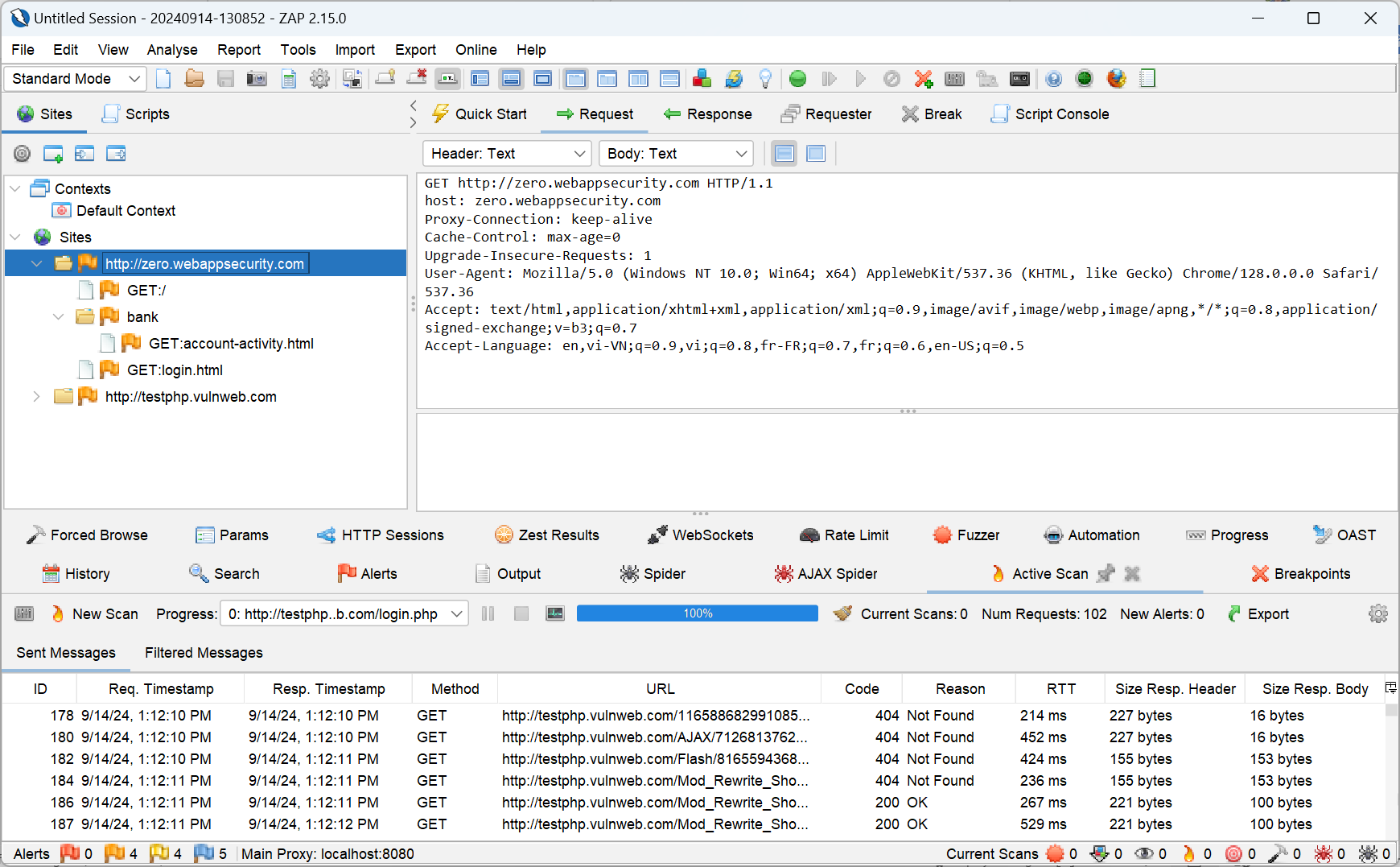




* Quay lại trình duyệt Chrome, nhập địa chỉ URL của WebSite kiểm thử bảo mật: http://....



* Quan sát kết quả trong các tab của cửa sổ OWASP như trên.



# BÀI TẬP

Phân tích và đánh giá kết quả kiểm thử bảo mật Website với Owasp Zap

Website cần kiểm thử: http://....

|  |  |  |
| --- | --- | --- |
| **TT** | **Nội dung cảnh báo** | **Giải thích** |
|  | Absence of Anti-CSRF Tokens | Cảnh báo (alert) của ZAP để chỉ một ứng dụng web bị thiếu các token Anti-CSRF. |
|  | Anti-CSRF tokens (hay CSRF tokens) | Cơ chế bảo vệ chống lại các cuộc tấn công CSRF (Cross-Site Request Forgery).  CSRF là một loại tấn công mà kẻ tấn công lừa một người dùng đăng nhập vào một trang web và sau đó sử dụng quyền truy cập của người dùng đó để thực hiện các hành động không mong muốn trên trang web đó.  NSD có thể edit các Alert bằng cách click vào chúng. |
|  | Missing Anti-clickjacking Header | Cảnh báo này xuất hiện khi ứng dụng web thiếu tiêu đề Anti-clickjacking (X-Frame-Options header) hoặc không đặt chính xác.  Tiêu đề này được sử dụng để ngăn chặn tấn công clickjacking, trong đó kẻ tấn công đưa nội dung độc hại vào một trang web khác và lừa người dùng nhấp chuột vào nó. |
|  | Cookie Poisoning | Cảnh báo cho thấy cookie trong ứng dụng web có thể bị tấn công bằng cách thay đổi nội dung của chúng.  Cookie là một thành phần quan trọng để duy trì trạng thái và xác thực trong các ứng dụng web, và khi bị nhiễm độc, nó có thể dẫn đến các hành vi không mong muốn hoặc vi phạm bảo mật. |
|  | Timestamp Disclosure | Cảnh báo này xuất hiện khi ứng dụng web tiết lộ thông tin về thời gian, chẳng hạn như thời gian tạo, sửa đổi hoặc xóa dữ liệu.  Thông tin về thời gian có thể cung cấp cho kẻ tấn công các gợi ý về cấu trúc hệ thống và thậm chí giúp tấn công theo thời gian (timing attacks). |
|  | Cookie without SameSite Attribute | Cảnh báo này khi cookie trong ứng dụng web không đặt thuộc tính SameSite hoặc không đặt chính xác.  Thuộc tính SameSite được sử dụng để xác định việc chia sẻ cookie giữa các trang web. Nếu không đặt đúng, có thể có nguy cơ tấn công CSRF hoặc thông tin đăng nhập bị rò rỉ. |
|  | Cookie Without Secure Flag | Cảnh báo này xuất hiện khi cookie không đặt cờ bảo mật (Secure flag) khi được truyền đi. Cờ bảo mật chỉ ra rằng cookie chỉ được gửi qua kết nối an toàn HTTPS, giúp ngăn chặn tấn công lắng nghe (eavesdropping) và đánh cắp thông tin đăng nhập. |
|  | Information Disclosure | Cảnh báo này xuất hiện khi ZAP phát hiện thông tin nhạy cảm hoặc thông tin quan trọng được tiết lộ trong phản hồi của ứng dụng web. Ví dụ, nó có thể là hiển thị thông tin về phiên làm việc, lỗi hệ thống, thông tin cấu trúc, hoặc thông tin đăng nhập không được bảo vệ. |
|  | Directory Listing | Cảnh báo này xuất hiện khi ZAP tìm thấy thư mục trên máy chủ web được cấu hình để hiển thị danh sách các tệp tin bên trong. Điều này có thể tiết lộ thông tin quan trọng về cấu trúc và nội dung hệ thống. |
|  | Open Redirect | Cảnh báo này xuất hiện khi ứng dụng web cho phép chuyển hướng không an toàn từ một URL đến một URL khác nằm ngoài tầm kiểm soát của ứng dụng. Kẻ tấn công có thể lợi dụng điều này để lừa người dùng truy cập vào các trang web độc hại hoặc nguy hiểm. |
|  | Server Misconfiguration | Cảnh báo này xuất hiện khi ZAP phát hiện các lỗ hổng bảo mật liên quan đến cấu hình không chính xác của máy chủ web. Điều này có thể bao gồm việc bật các tính năng không cần thiết, thiết lập quyền truy cập không đúng, hay cấu hình SSL/TLS không an toàn. |
|  | Unvalidated Redirects and Forwards | Cảnh báo này xuất hiện khi ứng dụng web cho phép chuyển hướng hoặc chuyển tiếp yêu cầu người dùng mà không thực hiện kiểm tra đúng đắn. Điều này có thể dẫn đến khả năng tấn công chuyển hướng không an toàn hoặc chuyển tiếp không mong muốn. |

Ngoài ra còn có nhiều cảnh báo có thể có, để NSD xem và phân tích tùy trường hợp.

*>> SV liệt kê các nhận xét, lỗ hổng, tình trạng của website tại đây….*

1. ..
2. ..

# Tham khảo

[1] https://viblo.asia/p/huong-dan-sercurity-testing-bang-tool-owasp-zap-cho-penetration-tester-kiem-thu-xam-nhap-PwlVmg8rJ5Z

-----------------------------------------------