|  |  |
| --- | --- |
| Logo  Description automatically generated | THỰC HÀNH ATTT  Kiểm thử bảo mật Web bằng công cụ Burp Suite |

Họ và tên Sinh viên:

Mã Sinh viên: Nhóm:

[1. Giới thiệu 1](#_Toc177303640)

[2. Chuẩn bị và cài đặt 1](#_Toc177303641)

[3. Khởi động và cấu hình 2](#_Toc177303642)

[4. Sử dụng BurpSuite để quét thông tin Website 4](#_Toc177303643)

[4.1 Tab Dashboard 4](#_Toc177303644)

[4.2 Tab Target 6](#_Toc177303645)

[4.3 Tab Proxy 8](#_Toc177303646)

[4.4 Tab Intruder 11](#_Toc177303647)

[4.4.1 Sniper 11](#_Toc177303648)

[4.4.2 Battering ram 12](#_Toc177303649)

[4.4.3 Pitchfork 12](#_Toc177303650)

[4.4.4 Cluster Bomb 13](#_Toc177303651)

[4.5 Tab Repeater 13](#_Toc177303652)

[5. Phân tích và đánh giá kết quả kiểm thử bảo mật Website 14](#_Toc177303653)

[6. Tham khảo 14](#_Toc177303654)

# Giới thiệu

Burp Suite là một công cụ dùng kiểm thử bảo mật Web, có các chức năng chính sau:

*1. Quét lỗ hổng và phân tích ứng dụng web:* Tìm lỗ hổng bảo mật như SQL injection, cross-site scripting (XSS), CSRF, và các lỗi khác. Giúp NSD xác định các điểm yếu trong hệ thống và có giải pháp khắc phục.

*2. Khai thác lỗ hổng:* BurpSuite cung cấp nhiều chức năng như Repeater, Intruder và Sequencer để thử nghiệm, tìm và khai thác lỗ hổng.

*3. Thực hiện tấn công từ đơn giản đến phức tạp:* Cung cấp các kỹ thuật tấn công như Brute Force, parameter tampering, và bypassing authentication. NSD có thể tận dụng các công cụ trong Burpsite để áp dụng các chiến thuật tấn công khác nhau và xem các kết quả.

*4. Kiểm tra tích hợp:* giữa các ứng dụng web và các dịch vụ khác như CSDL, phần mềm máy chủ và ứng dụng di động. Dùng để kiểm tra và xác minh tính bảo mật của hệ thống toàn diện hơn.

# Chuẩn bị và cài đặt

* Cài đặt Java JDK.
* Tải và giải nén file burpsuiteprov2022.7.1.rar trong LINK03.

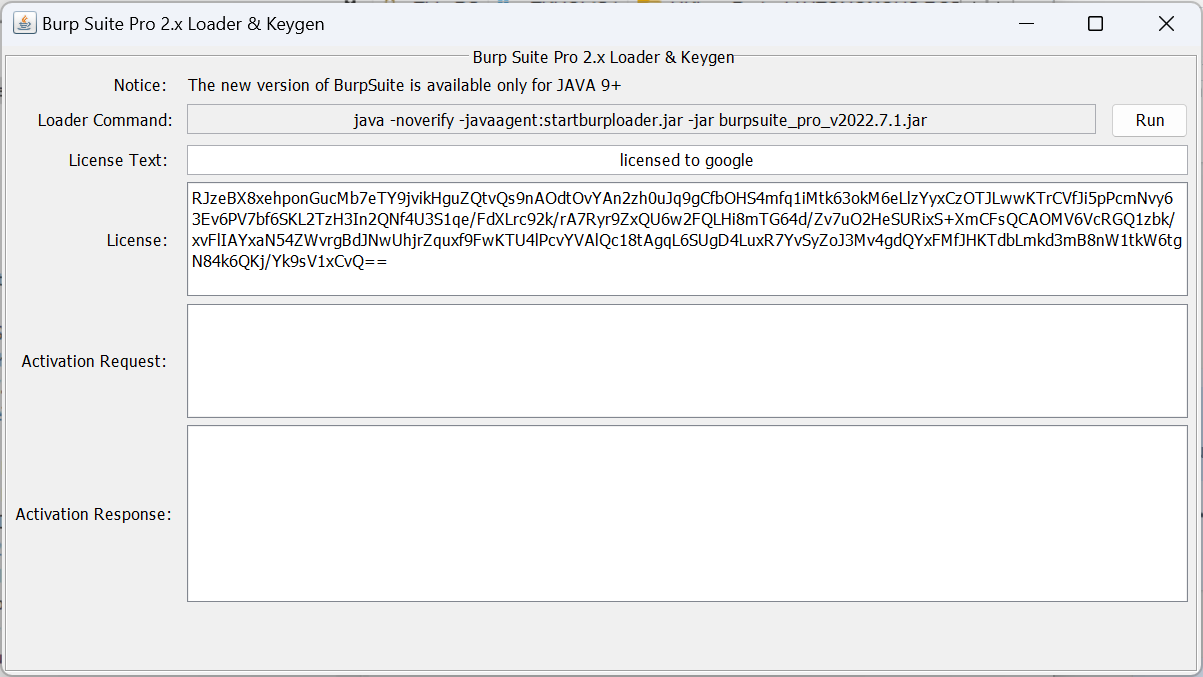
Chọn website URL thực hiện kiểm thử bảo mật: http://abc.com

*Ví dụ: http://testphp.vulnweb.com/login.php*. Username: test, password: test

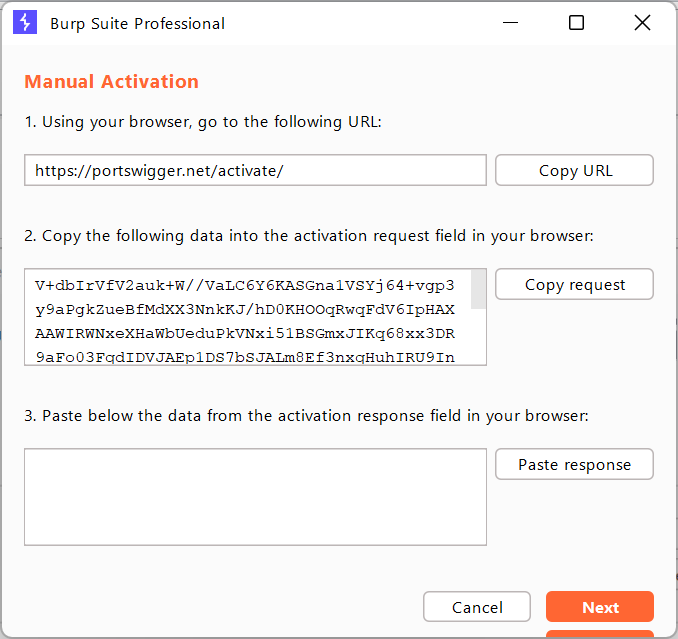
# Khởi động và cấu hình

Burp Suite được thiết kế để sử dụng cùng với trình duyệt. Công cụ này hoạt động giống như một HTTP proxy server, và tất cả HTTP(S) traffic đều sẽ đi qua Burp.

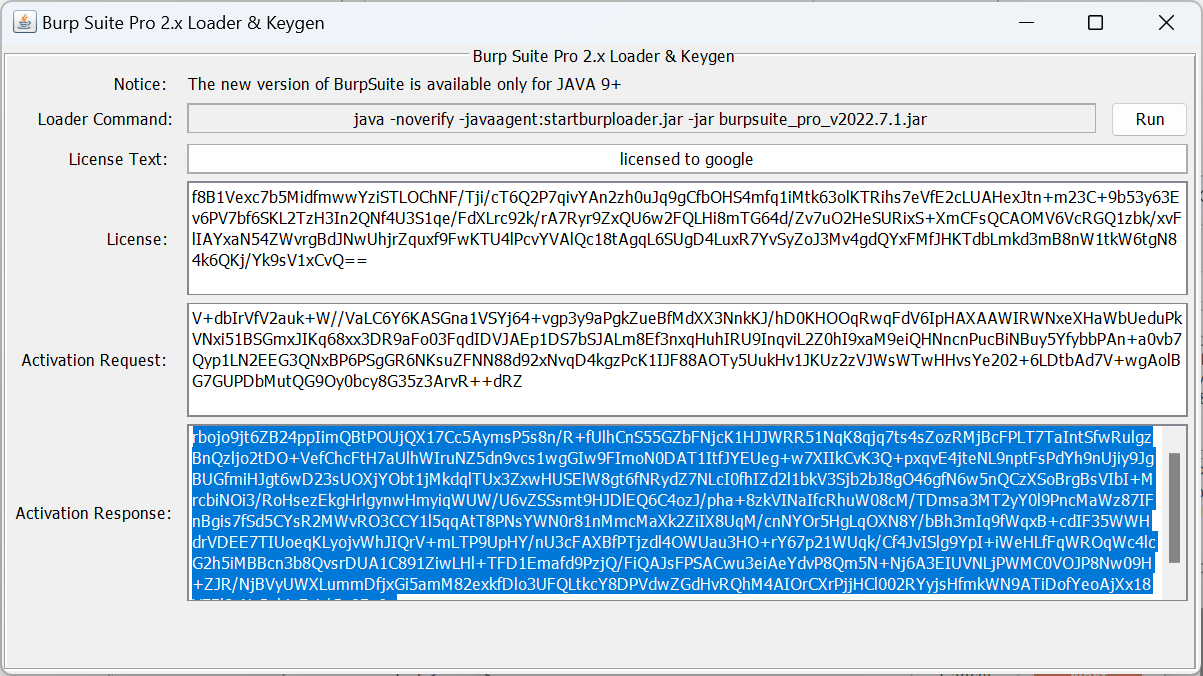
* Chạy file .JAR lên để mở chương trình.
* Chọn *Temporary project ® Next ® Dashboard*

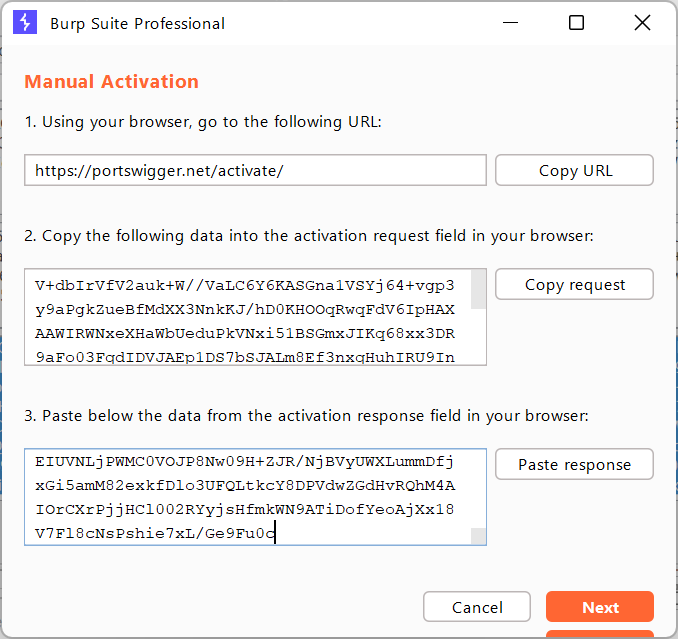


* Chọn mục Run
* Chọn Manual activation



* Chọn Copy request





A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

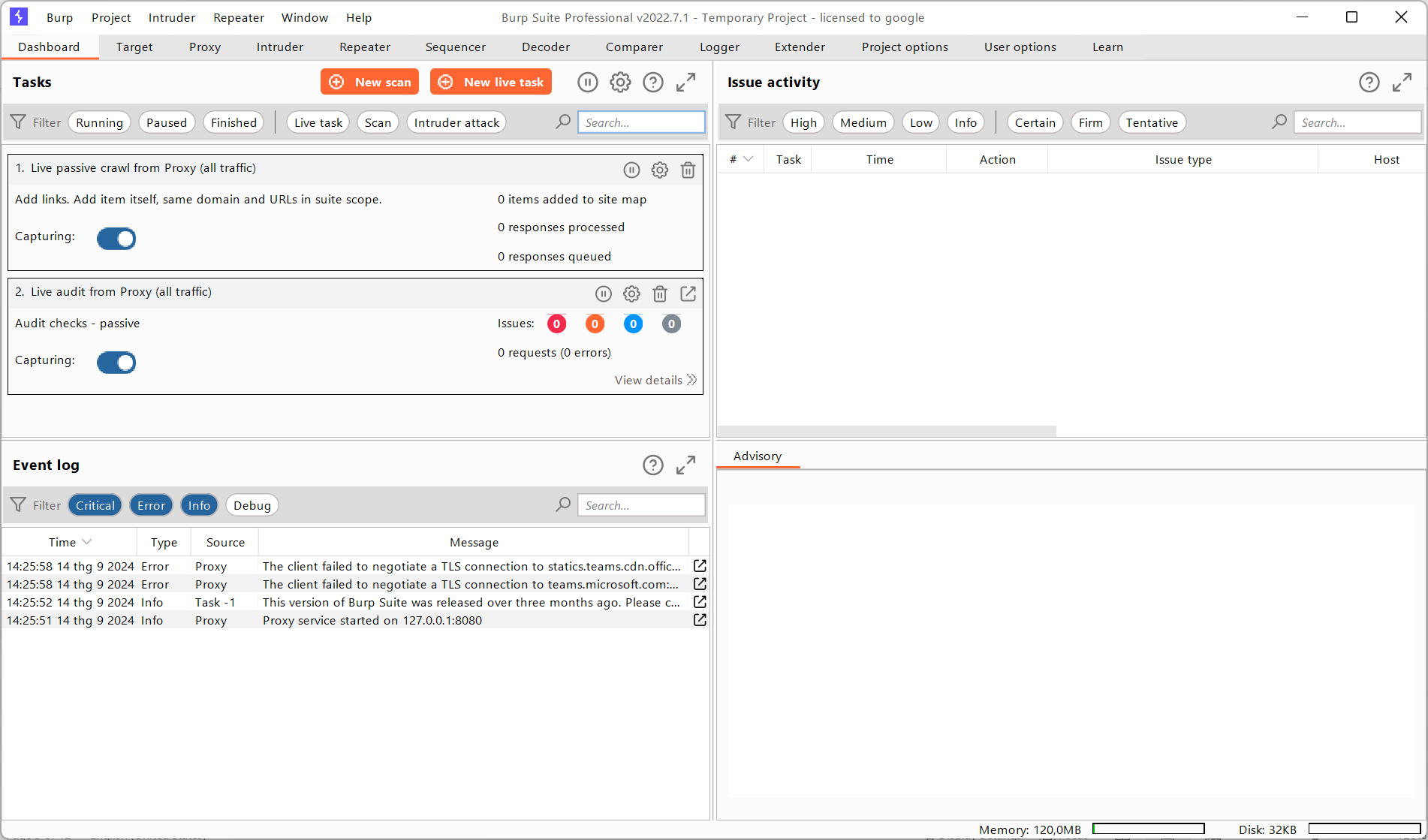
# Sử dụng BurpSuite để quét thông tin Website

## Tab Dashboard

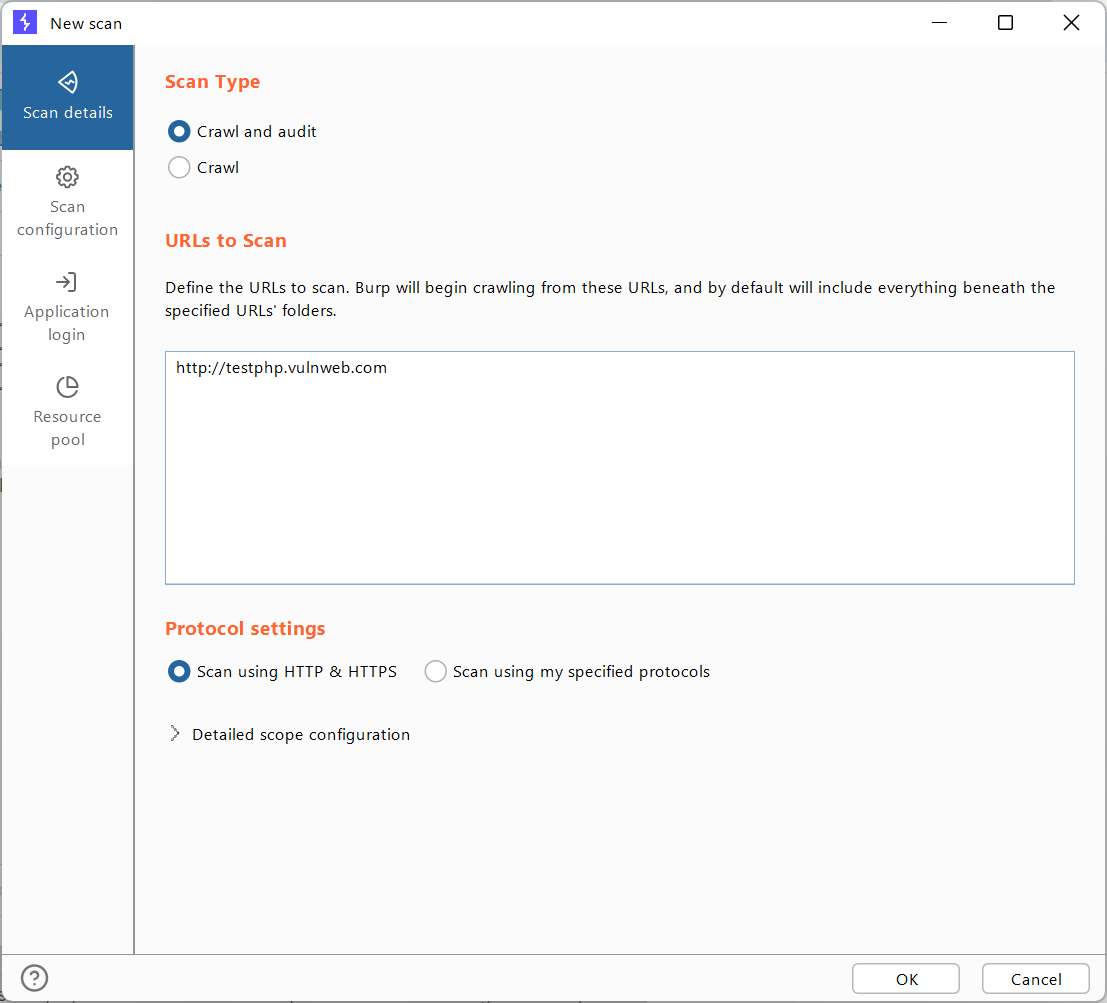
* Giao diện đầu tiên sau khi khởi động burpsuite
* Vào Dashboard ® New Scan.
* Cấu hình lại chế độ Scan bằng cách bấm vào tab Scan Configuation và chọn vào New ® Audit và chọn vào mục Issue Reported rồi chọn cách scan.
* Thực hiện scan theo Library Built-in hay là Custom.
* Chọn Build-in s® OK sau đó quay về Dashboard và chờ đợi kết quả scan.
* Ở bên phải phần Issue Activity sẽ xuất hiện danh sách các Issue phát hiện được trong lúc scan. Kích vào và xem các mô tả và request ở tab phía dưới.
* Sau khi Scan xong, xem kết quả tại tab Tartget sẽ có sitemap của website đã scan

Burp Suite có thể cài thêm các extension phục vụ cho các nhu cầu pentest khác như Spydir, Subfinder, etc... hoặc có thể là các extension do chính NSD tự viết bằng Java.

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



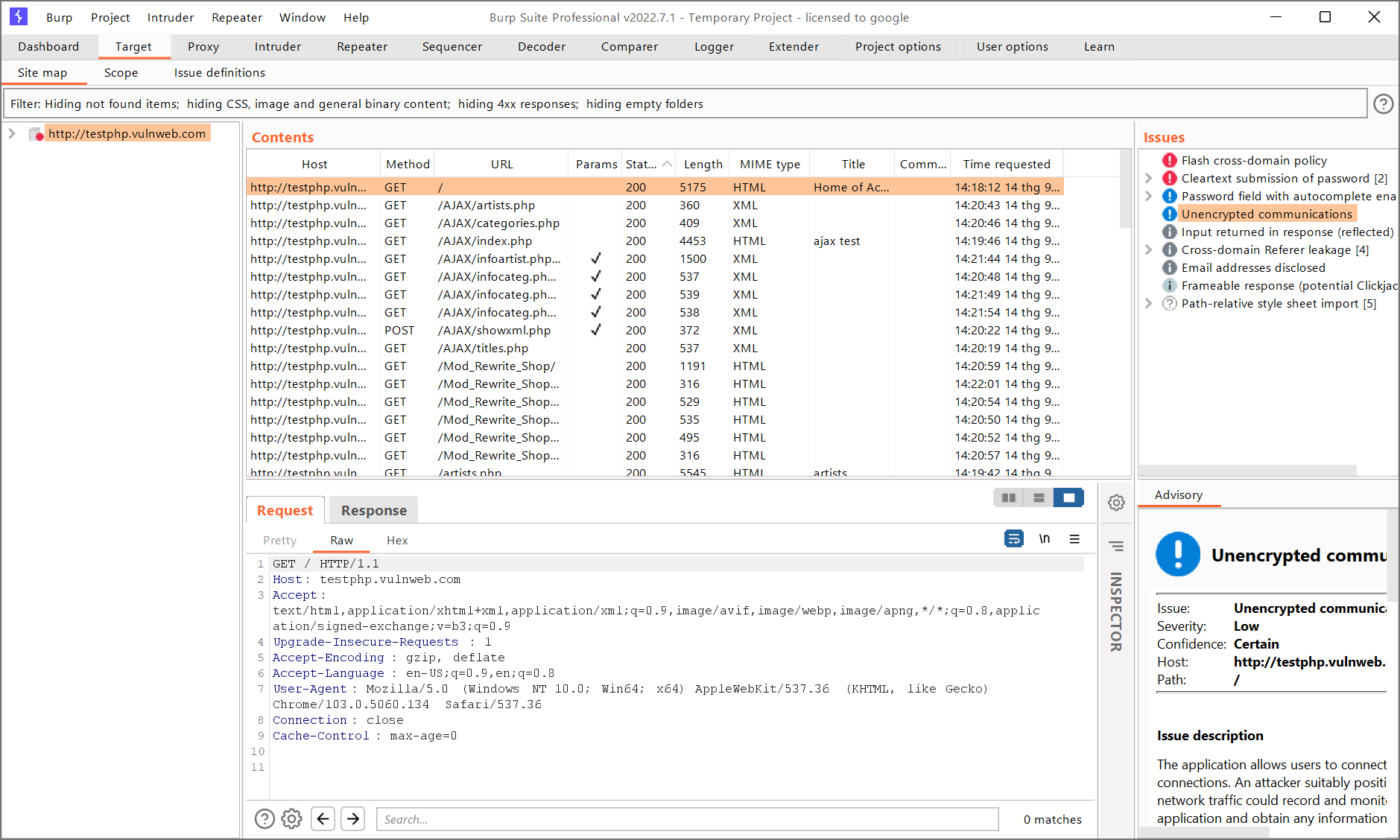
* Chọn [New scan] Nhập đường dẫn trang Web cần kiểm thử bảo mật



* Chọn chế độ scan: Lightweight. Chọn OK
* Chuyển sang Tab Target

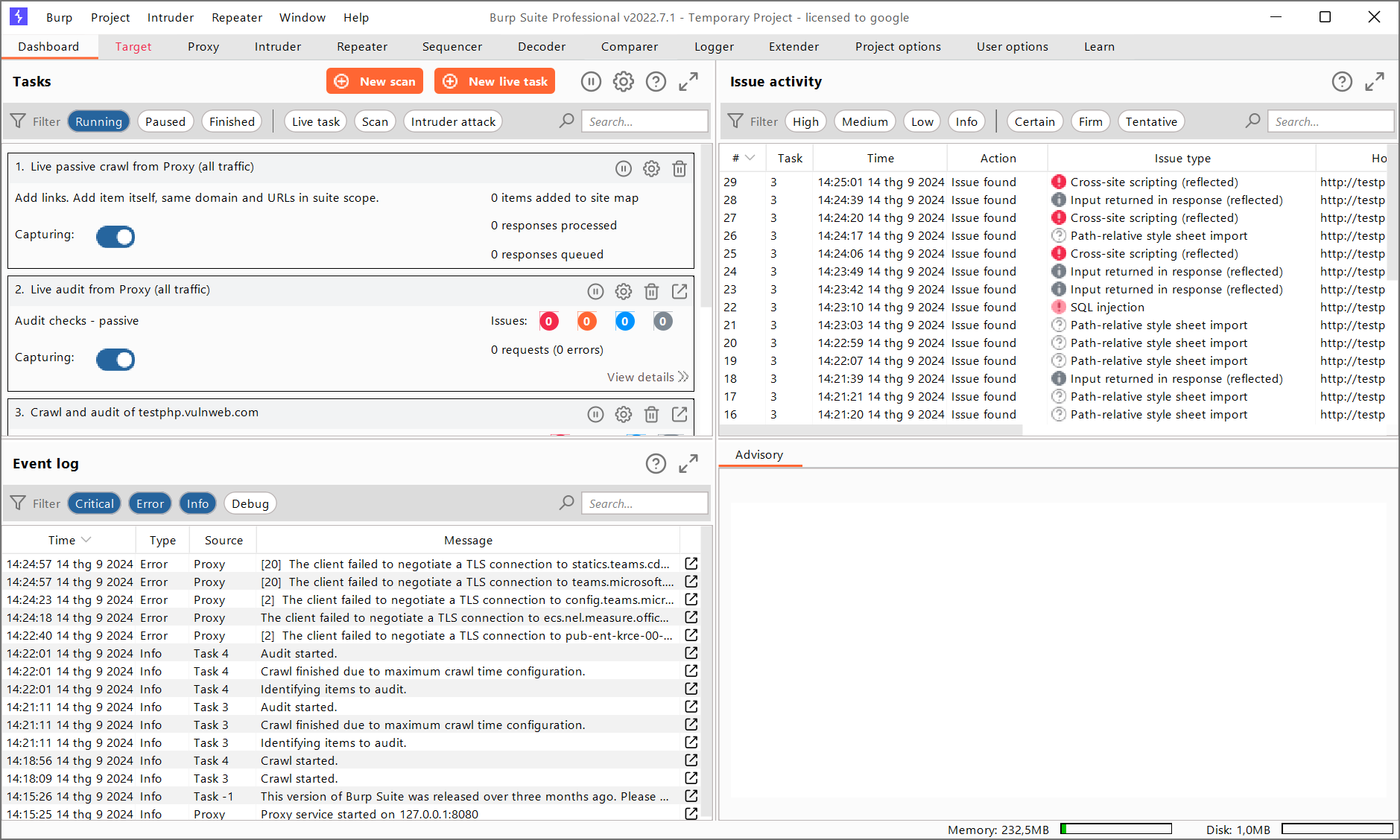
## Tab Target

* Tab Target là nơi chứa các thông tin tổng quan về Web. Cho phép xem site map và điều chỉnh phạm vi mục tiêu và có thể được xác định bằng cách điền loại giao thức, host/IP, port.
* Chọn đến độ Scan:  *passive scan* hoặc *active scan.*
* Chọn Tab [Site map]



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

* Chọn Tab [Scope]
* Chọn Tab [Issue definitions]
* Quay trở lại, chọn tab [Dashboard] để xem kết quả quét Web



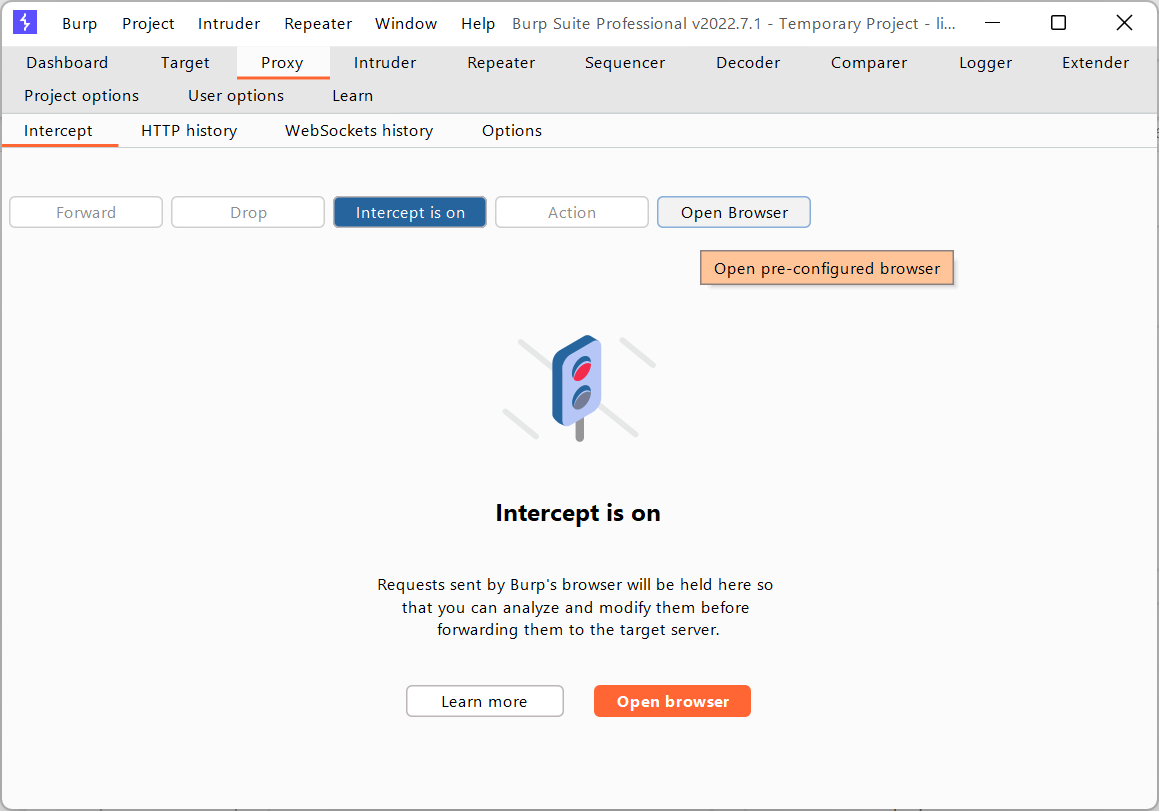
## Tab Proxy

Hiển thị chi tiết các request đi qua Burp Proxy.

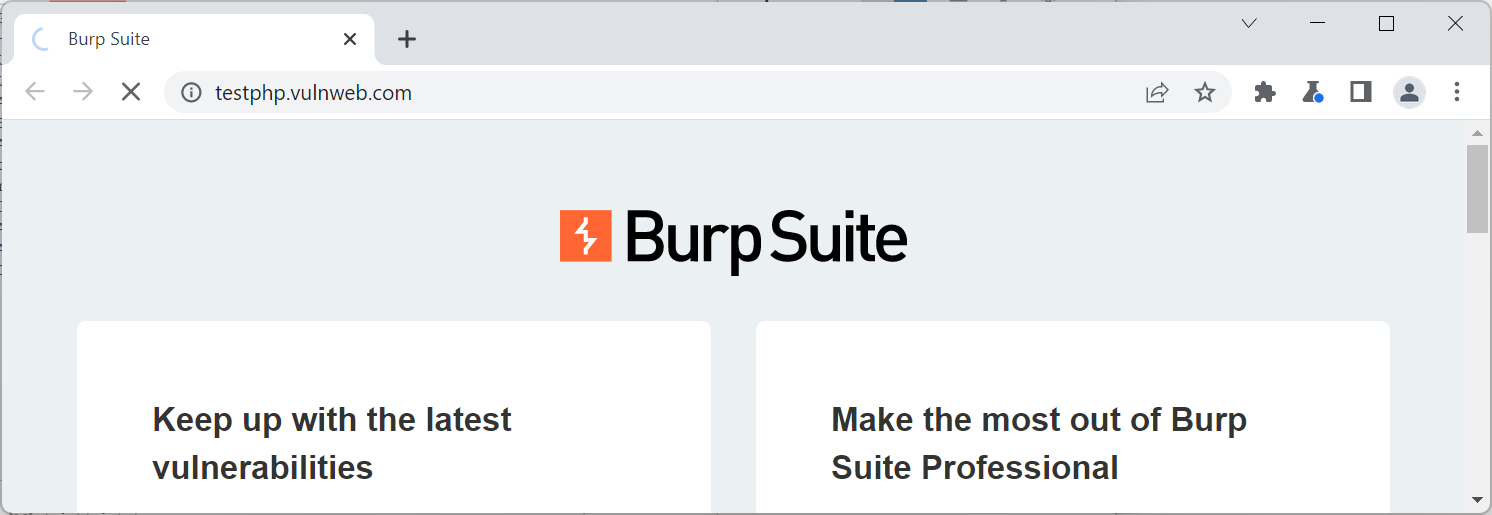
* Tại đây, có các tùy chọn Forward, Drop, Modify hay chuyển sang các action khác (repeater, intruder, etc...).
* Thông tin về header và các thông tin của request được show lên ở phần bên phải là INSPECTOR

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

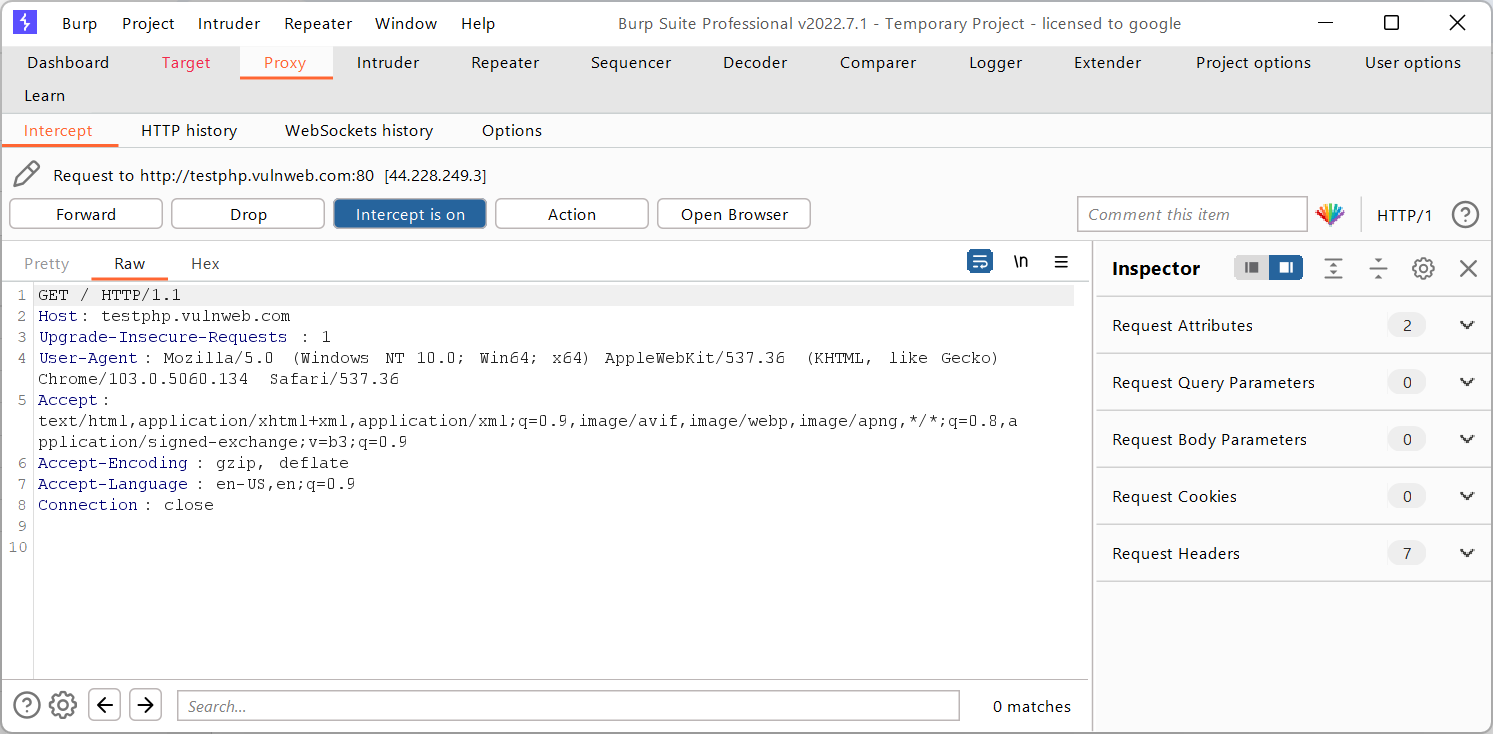
* Bước 1: Kiểm tra Tab Proxy của BurpSuite



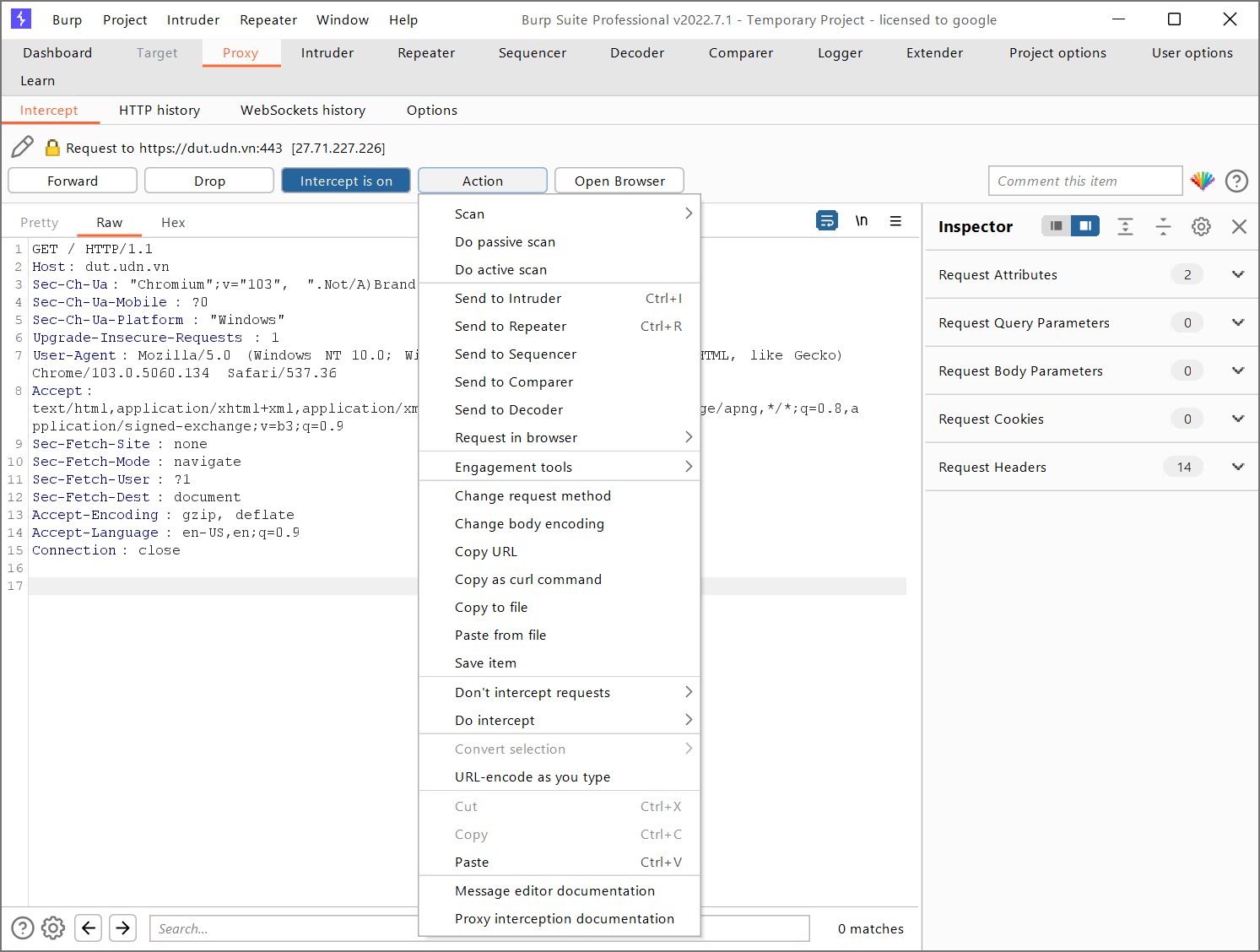
* Chọn mục Open browser. Nhập đường dẫn Website



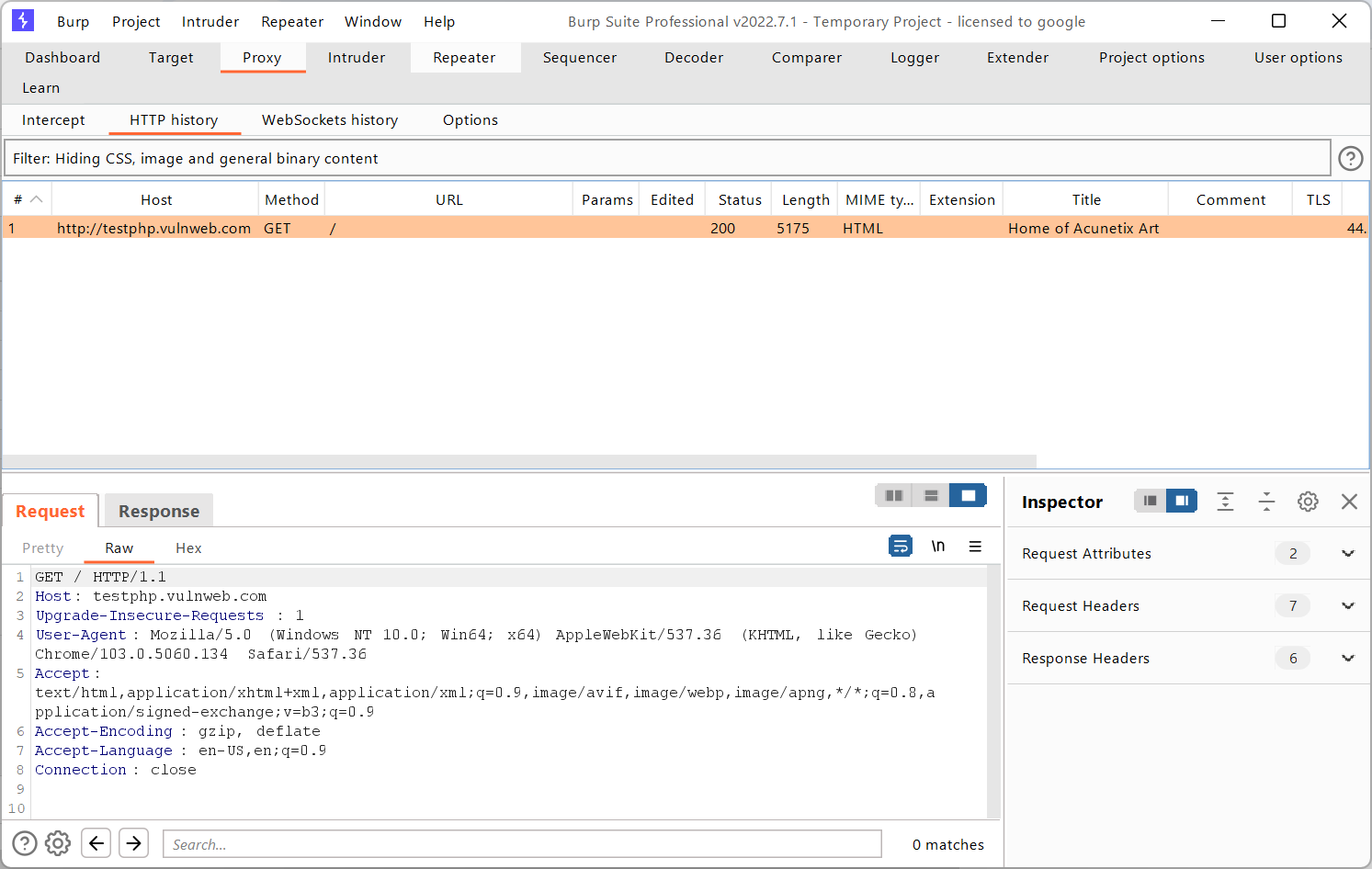
* Xem kết quả trong Tab Intercep on: Xem kết quả Burp kiểm tra đã bắt được request.



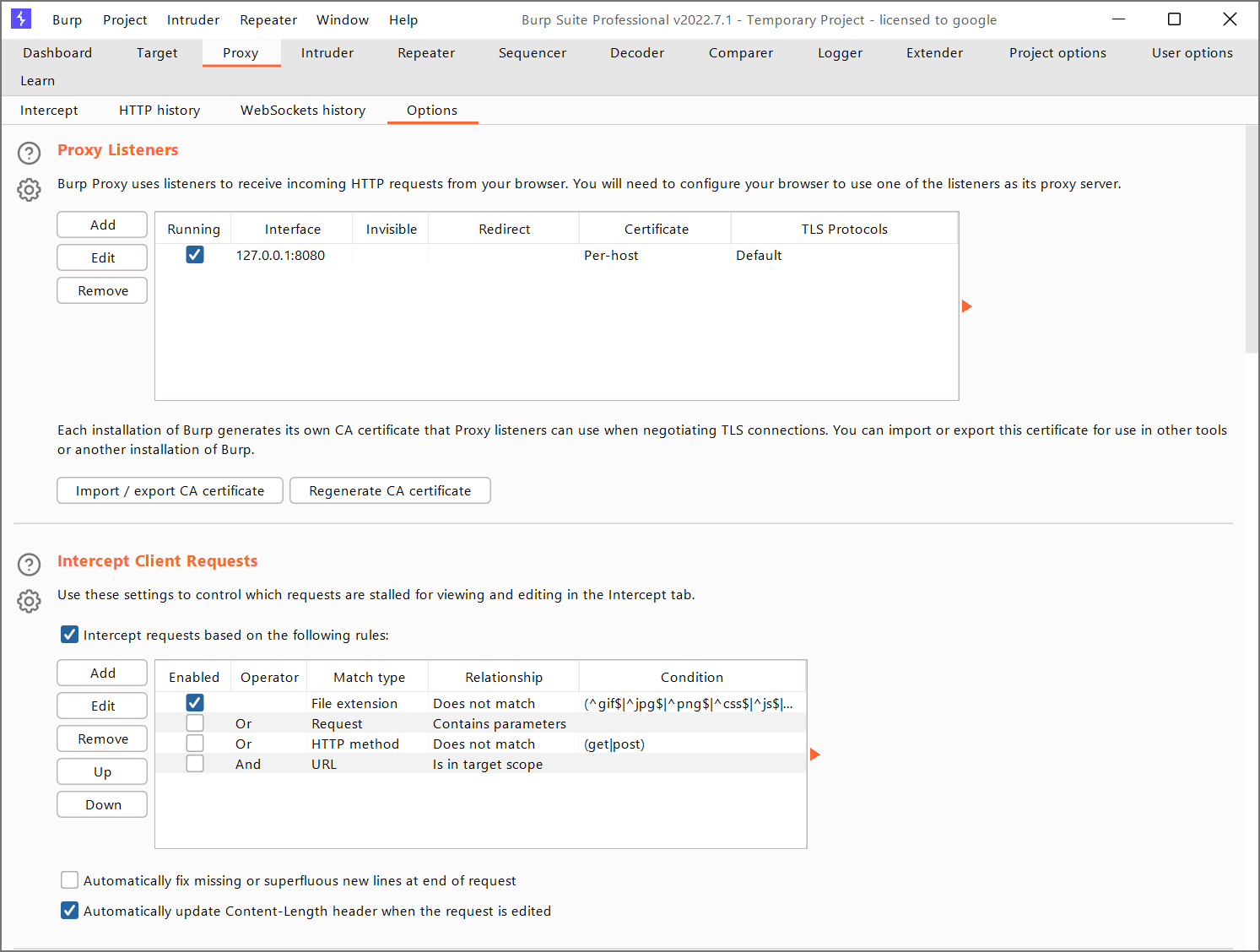
* Chọn mục Action



* Xem kết quả trong Tab HTTP history



* Xem kết quả trong Tab Options



## Tab Intruder

Cho phép test ứng dụng web bằng cách gửi các payloads đã được định nghĩa trước lên server, sau đó xem xét kết quả trả về (tương tự kỹ thuật brute-force)

* Thử đăng nhập vào Website URL bằng tài khoản và mật khẩu
* Kết quả bắt gói tin khi login rồi sau đó được gửi sang Intruder.
* Chọn mục [Positions]. Choose an attack type: Sniper

A screenshot of a computer

Description automatically generated

* Sau khi sang tab Intruder ta sẽ thấy đường link và port của website
* Custom lại chỗ cần inject payloads vào. Phần uname và pass được đặt trong cặp dấu $ (tượng trưng) ta có thể định dạng lại chỗ cần *inject* vào bằng cách thêm cặp dấu $ vào bằng cách bấm vào nút Add $ hay clear $.
* Trong phần payloads, có thể chọn payloads có sẵn hoặc tự custom => Sau đó bấm vào Start attack.
* Kiểm tra request mà có status code trả về thành công => 200
* Theo kết quả đúng, username và pass đã login thành công đúng như tài khoản ban đầu.

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

Các kiểu tấn công được Intruder hỗ trợ là Sniper, Battering ram, Pitchfork, Cluster Bomb.

### Sniper

* Sniper chỉ sử dụng một bộ payload, nếu có 1 position nó sẽ chèn lần lượt từng payload từ đầu đến cuối danh sách.
* Trường hợp có nhiều position, nó sẽ chèn từng payload trong danh sách vào position 1, sau đó tiếp tục đến với position 2, position 3…
* Tổng số request của kiểu tấn công Sniper = số payload của bộ payload x số position
* Ứng dụng: tìm lỗ hổng SQL injection, XSS, dò password một user biết trước…

Ví dụ:

Mã:

Request 1: position1=payload[0]&position2=

Request 2: position1=payload[1]&position2=

Request 3: position1=payload[2]&position2=

...

Sau khi chèn hết payload trong danh sách vào position1 sẽ tiếp tục với position2

Request 4: position1=&position2=payload[0]

Request 5: position1=&position2=payload[1]

Request 6: position1=&position2=payload[2]

...

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

### Battering ram

* Kiểu Battering ram (tương tự như Sniper) chỉ dùng 1 bộ payload, tuy nhiên nó được dùng trong trường hợp pentest ứng dụng có 2 position trở lên và các position sẽ dùng chung một payload tại một thời điểm.
* Tổng số request của kiểu tấn công Battering ram = số payload của bộ payload.
* Ứng dụng: dò giá trị user/password người đặt giống nhau…

Ví dụ:

Mã:

Request 1: position1=payload[0]&position2=payload[0]

Request 2: position1=payload[1]&position2=payload[1]

Request 3: position1=payload[2]&position2=payload[2]

...

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

### Pitchfork

* Tấn công Pitchfork sử dụng nhiều bộ payload. Mỗi position tương ứng với một bộ payload.
* Tại một thời điểm, các position sẽ chạy đồng thời tương ứng với bộ payload cho từng position. Nói cách khác, với request đầu tiên, tại position1 sẽ dùng payload đầu tiên trong bộ payload1, tại position2 sẽ dùng payload đầu tiên trong bộ payload2, sau đó tương tự với request tiếp theo...
* Tổng số request của kiểu tấn công Pichfork = số payload của bộ payload nhỏ nhất.

Ví dụ:

Mã:

Request 1: position1=payload1[0]&position2=payload2[0]

Request 2: position1=payload1[1]&position2=payload2[1]

Request 3: position1=payload1[2]&position2=payload2[2]

...

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

### Cluster Bomb

Cluster Bomb sử dụng nhiều bộ payload, mỗi bộ tương ứng với một position.

Tuy nhiên với Cluster Bomb các position sẽ được chạy đồng thời, payload tại các postion sẽ được kết hợp chéo với nhau.

Ứng dụng: brute force trang đăng nhập…

Ví dụ:

Mã:

Request 1: position1=payload1[0]&position2=payload2[0]

Request 2: position1=payload1[1]&position2=payload2[0]

Request 3: position1=payload1[2]&position2=payload2[0]

...

Sau khi chèn lần lượt hết bộ payload1 vào position1 với payload đầu tiên ở position2 quá trình sẽ tiếp tục như sau:

Request 4: position1=payload1[0]&position2=payload2[1]

Request 5: position1=payload1[1]&position2=payload2[1]

Request 6: position1=payload1[2]&position2=payload2[1]

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

## Tab Repeater

Chức năng này dùng để thay đổi và gửi lại những request khác nhau tới server. Đồng thời sẽ nhận về response từ server để có thể phân tích được gói tin.

* Chọn Tab Repeater bấm vào dấu edit để thêm host và port của target, sau đó nhập vào phần request ở khung bên trái rồi gửi đi.

A screenshot of a computer

Description automatically generated

* Xem các redierect action bằng cách chuột phải vào phần request chọn vào Send To Repeater. Kết quả sẽ được chuyển sang luôn và có request sẵn từ trước.
* Chọn chế độ xem reponse là source code ở tab pretty hoặc raw
* Chọn Tab render để xem chế độ Web

A screenshot of a computer

Description automatically generated

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

Trước khi tiến hành làm việc với Burp, cần cấu hình để trình duyệt làm việc với nó.

# Phân tích và đánh giá kết quả kiểm thử bảo mật Website

* **Đường dẫn URL của Website cần kiểm thử: http://....**

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

1. ..
2. ..

# Tham khảo

1. https://viblo.asia/p/burp-suite-co-ban-do-lo-hong-bao-mat-tren-ung-dung-web-L4x5xreqZBM
2. https://portswigger.net/burp/documentation
3. https://digtvbg.com/files/books-for-hacking/Burp Suite Cookbook - Practical recipes to help you master web penetration testing with Burp Suite by Sunny Wear.pdf
4. https://portswigger.net/web-security/all-labs