CÀI ĐẶT VÀ CẤU HÌNH BURPSUITE

1. Giới thiệu công cụ

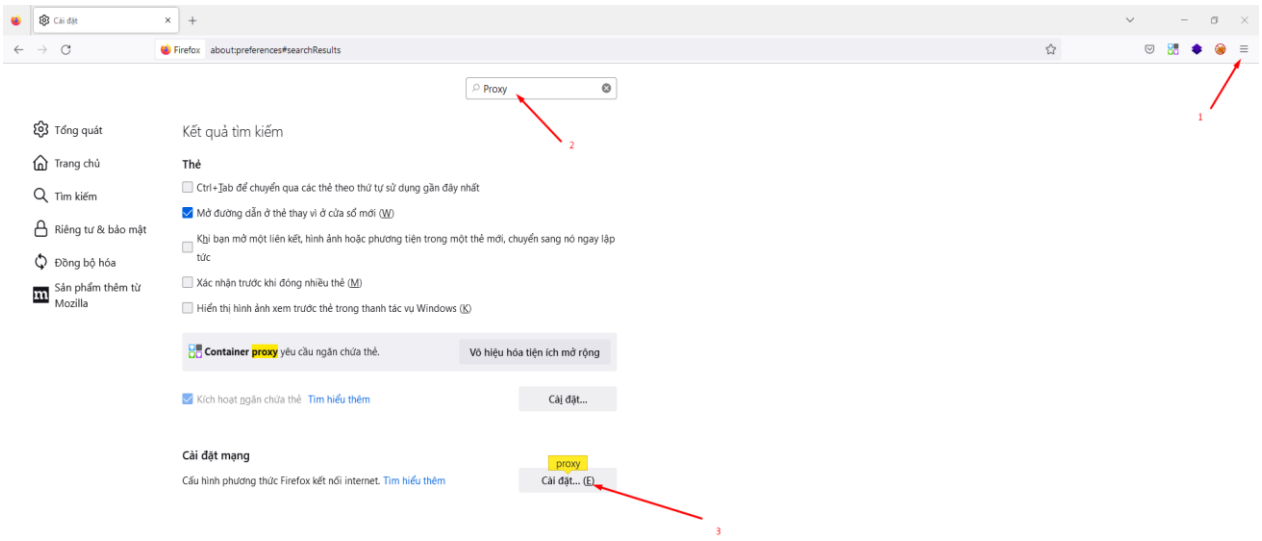
- Burpsuite là phần mềm bắt và sửa đổi gói tin HTTP/HTTPS, giúp bắt/sửa đổi/thực hành khai thác lỗ hổng bảo mật web
- Lab sẽ hướng dẫn cài đặt và cấu hình Burpsuite cơ bản để sử dụng trong các bài Lab tiếp theo

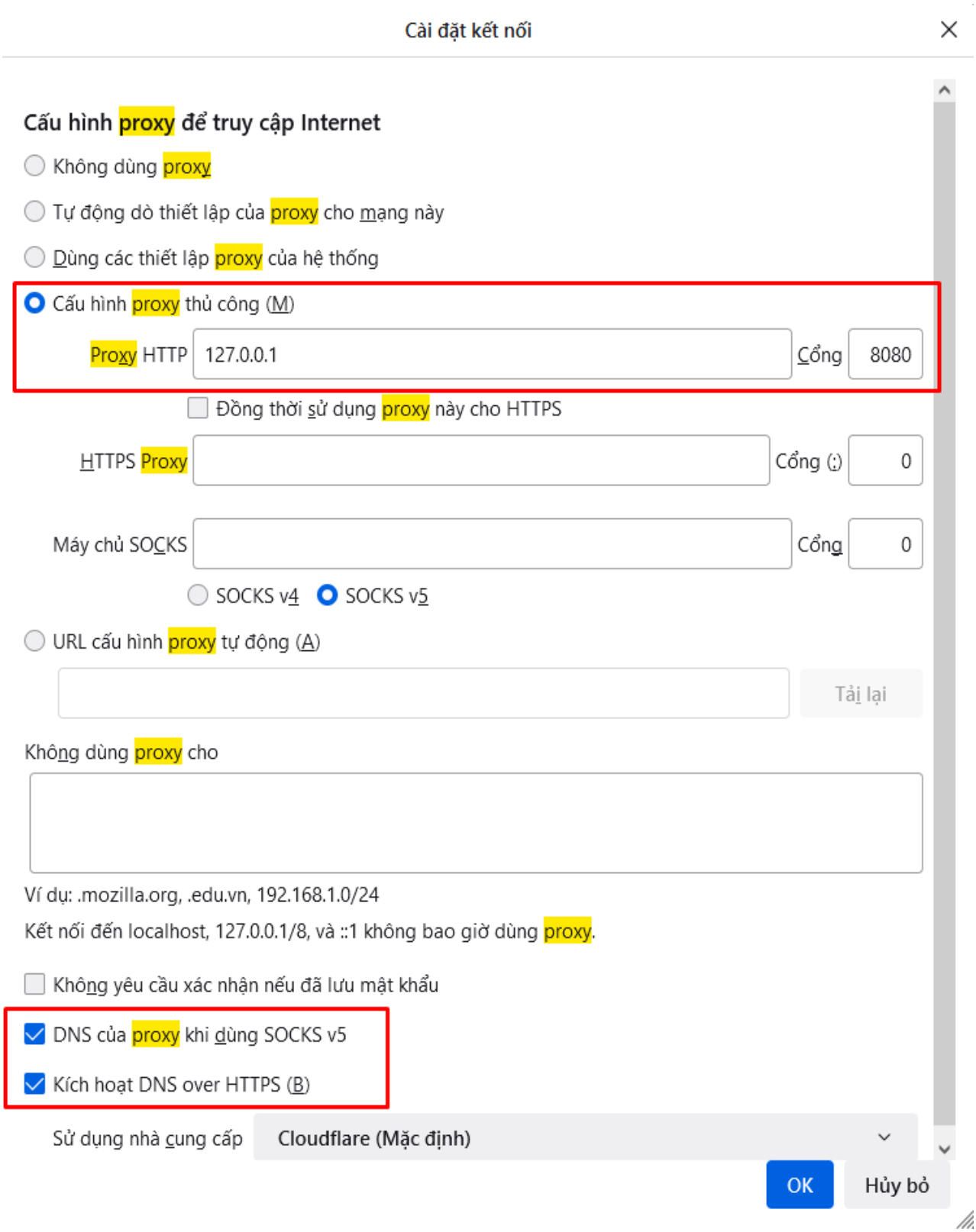
2. Cài đặt trên Firefox

Cài đặt trình duyệt Firefox, hoặc download và cài đặt bản mới nhất của Firefox tại địa trang chủ https://www.mozilla.org/en-US/firefox/new/

3. Cấu hình Proxy cho Firefox

- Mở Firefox
- Tại menu Settings, gõ tìm kiếm: Proxy





- Click Settings…, Chọn Manual proxy configuration, cấu hình proxy: 127.0.0.1 port 8080 và chọn “Also use this proxy for HTTPS”

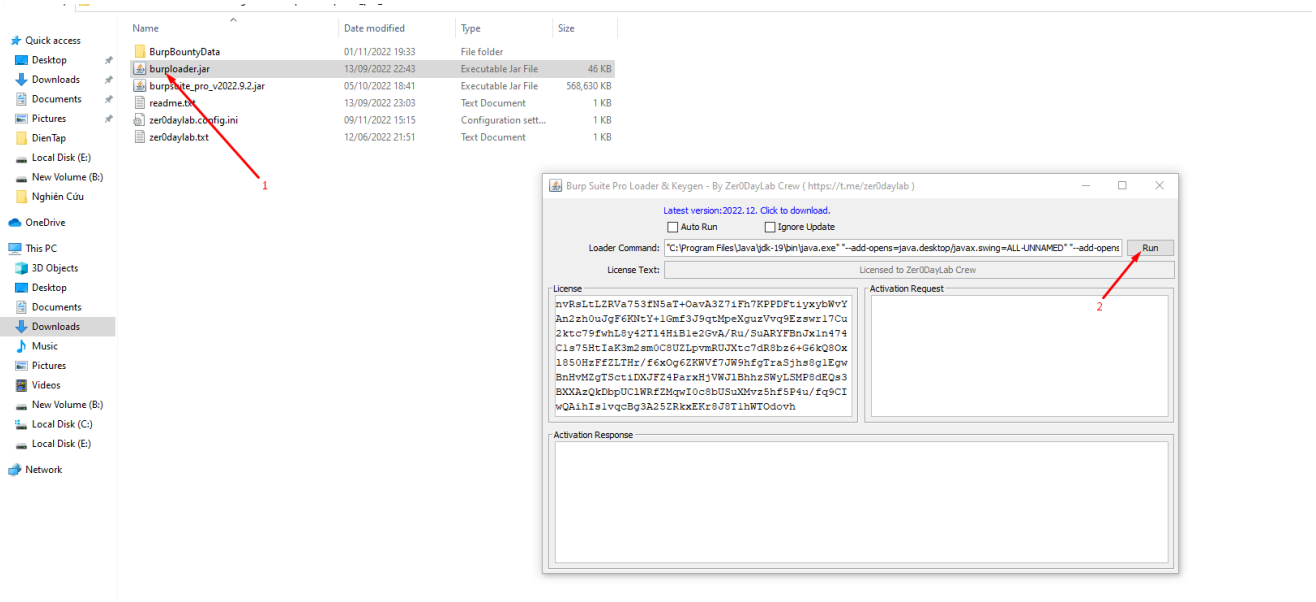
4. Cài đặt Java

Cài đặt Java tại D:\Setup\Java hoặc download

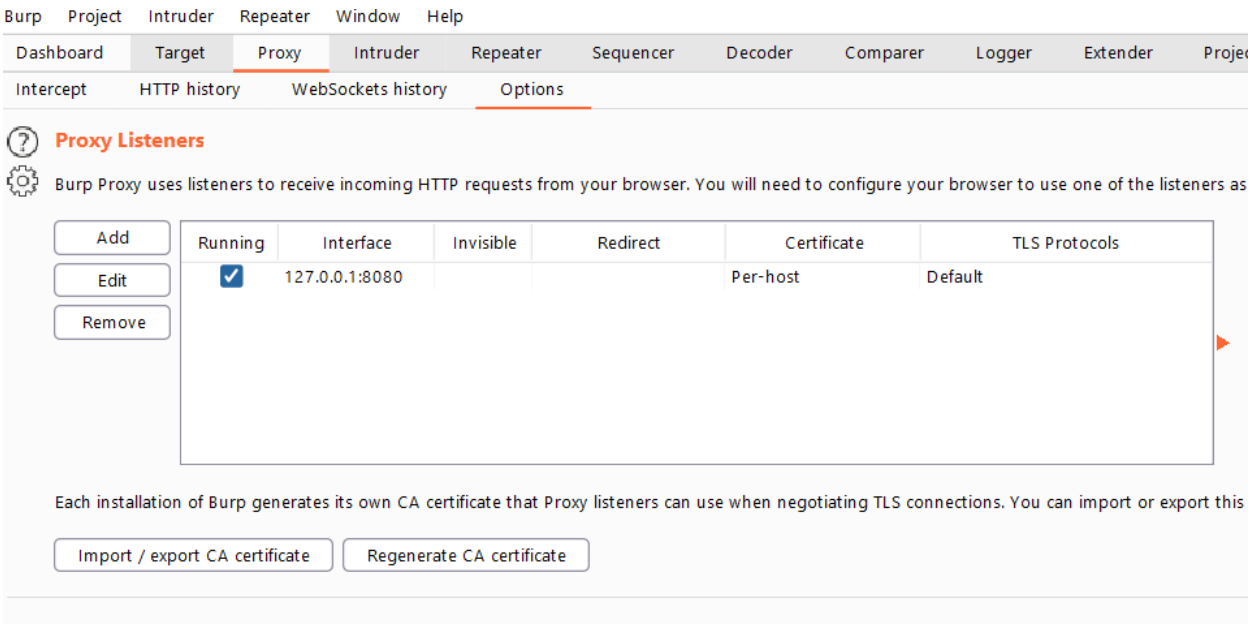
và cài đặt từ
https://www.oracle.com/java/technologies/downloads/

5. Khởi chạy Burpsuite:

- Tại thư mục Burpsuite trên desktop click double file burploader.jar
- Cửa sổ mới hiện ra, click “Run”

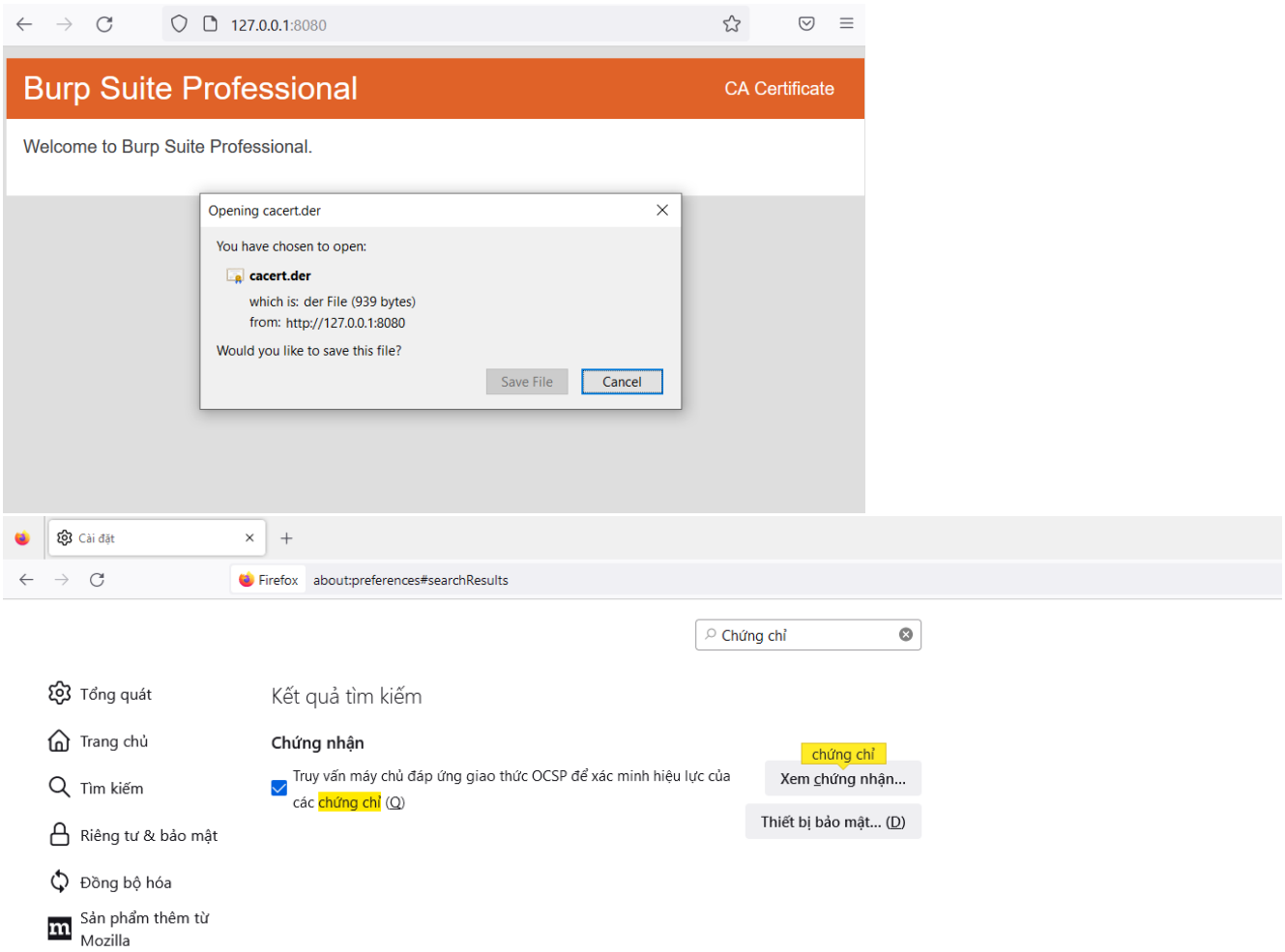


- Nếu chương trình yêu cầu license thì copy license request vào Burploader rồi copy license response paste vào Burpsuite
- Ấn Next, chọn Temporaty Project, Ấn Start Burp
- Click vào menu Proxy/Options, đảm bảo rằng Proxy đang có trạng thái Running được checked ở địa chỉ 127.0.0.1



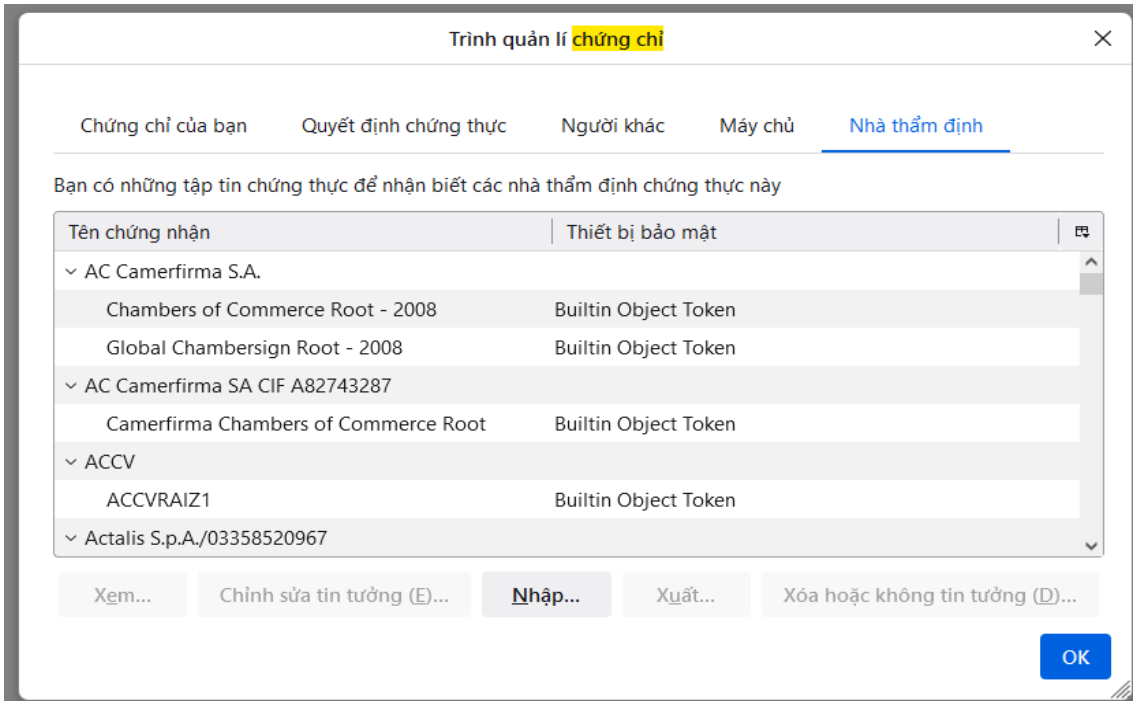
6. Add chứng thư số của Burpsuite vào Firefox

Tại trình duyệt Firefox (đã được cấu hình proxy trỏ vào 127.0.0.1:8080 ở bước 2, truy cập URL: http://127.0.0.1:8080
Click vào chữ: CA Certificate và tải file về thư mục Download

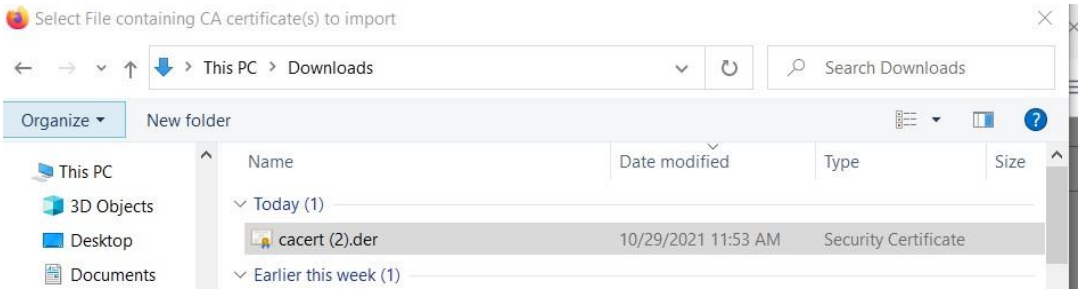


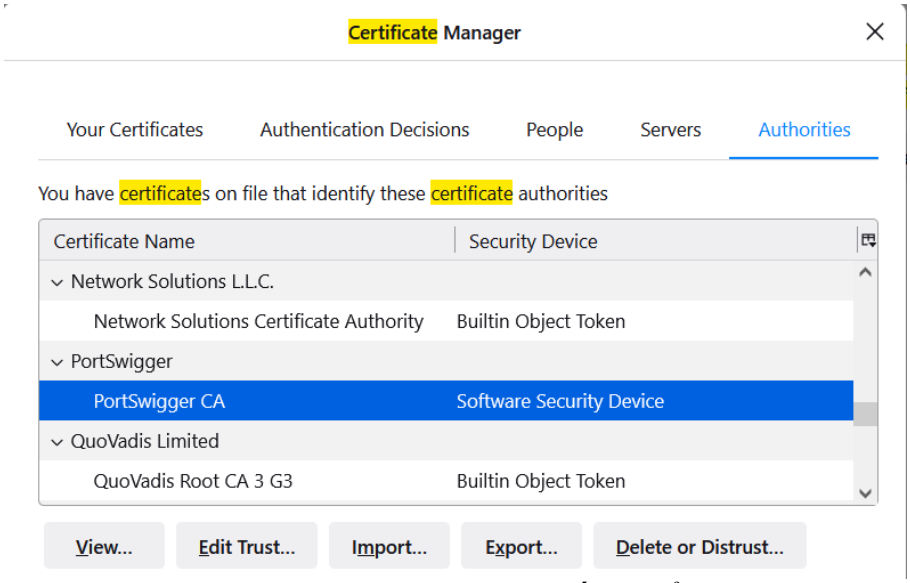
Mở Firefox setttings, gõ vào ô tìm kiếm chữ: certificate, click View Certificates

- Tại cửa sổ Certificate Manager chuyển sang tab Autority, click nút Import



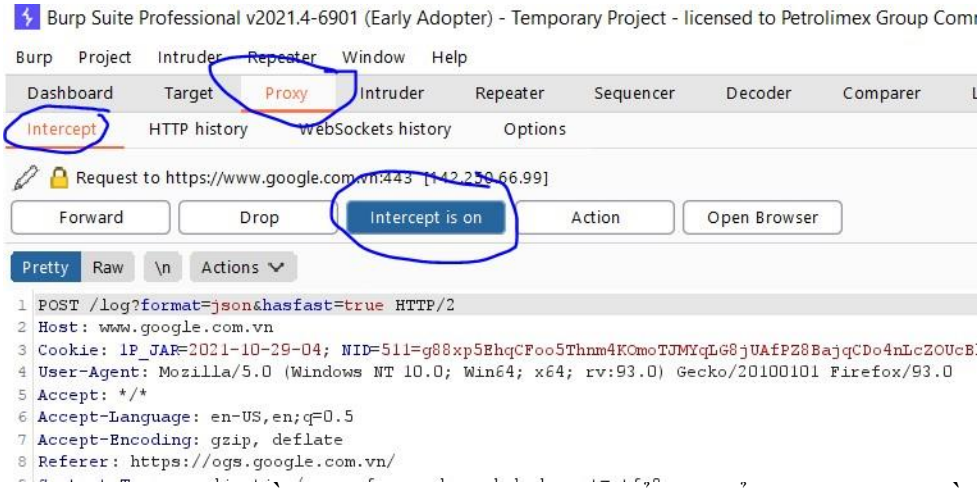
- Chuyển đến thư mục vừa Save chứng thư ở bước 1 và chọn file carcert.der, nhấn Open





- Chờ thông báo import thành công và kéo xuống kiểm tra đã có cert của PortSwigger CA
- Nhấn OK để đóng cửa sổ setting của Firefox.

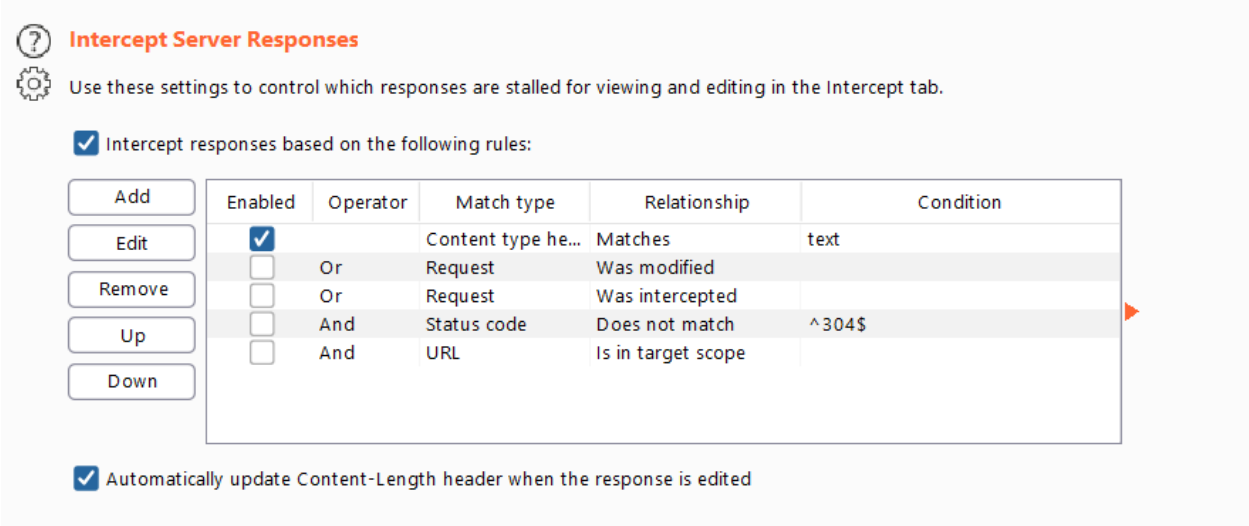
- Chú ý: nếu Burpsuite đang để Intercep Request thì chuyển sang màn hình



Burpsuite/Proxy rồi click: Intercept is on để chuyển trạng thái về Intercept is off

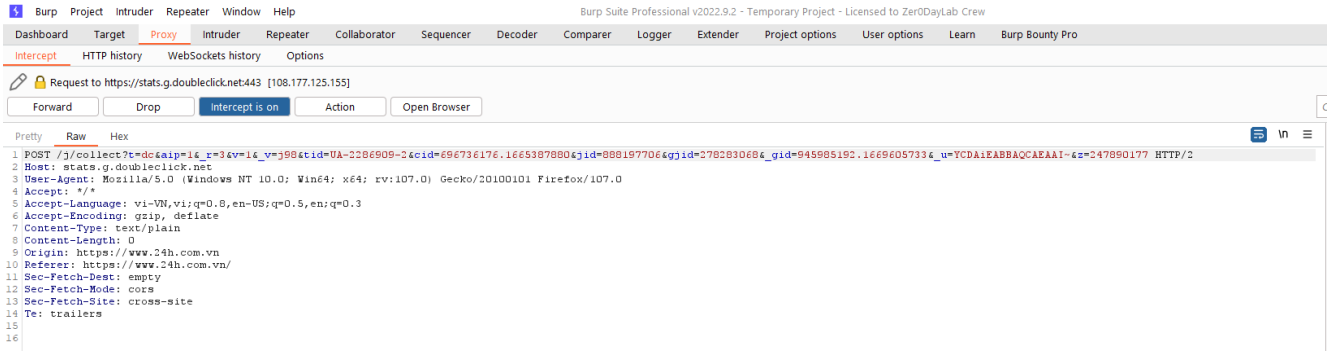
7. Cấu hình Burpsuite bắt Response trả về

- Trên Burpsuite chuyển sang màn hình Proxy/Options
- Kéo xuống dưới tick chọn Intercept Response:

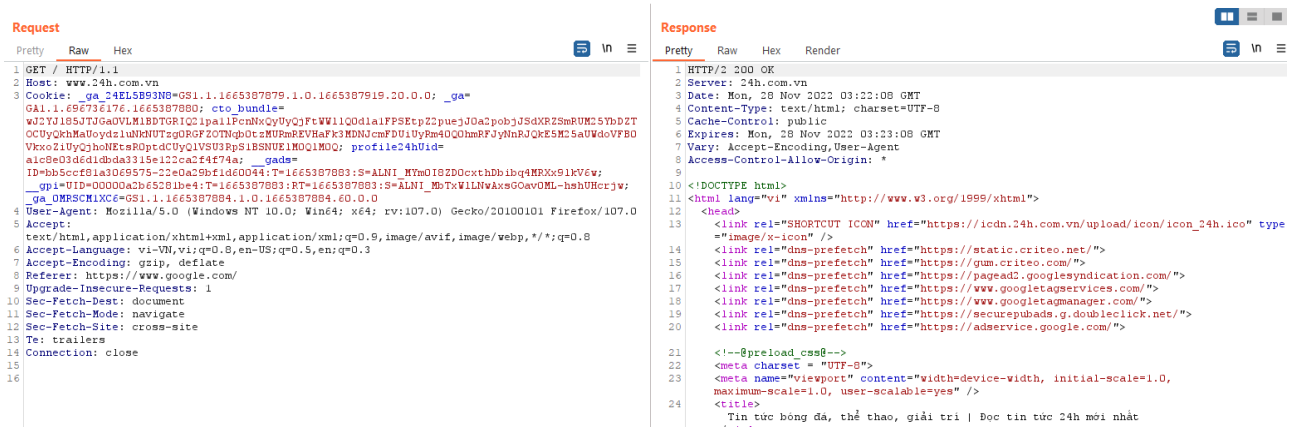


8. Kiểm tra khả năng bắt request của Burpsuite

- Trên Burpsuite chuyển sang chế độ Proxy/Intercept is on
- Trên Firefox truy cập: https://24h.com.vn



- Chuyển sang Burpsuite kiểm tra HTTP request đã được bắt:
- Nhấn vào nút Forward để chuyển request đến Webserver
- Burpsuite còn bắt cả HTTP Response trả về:

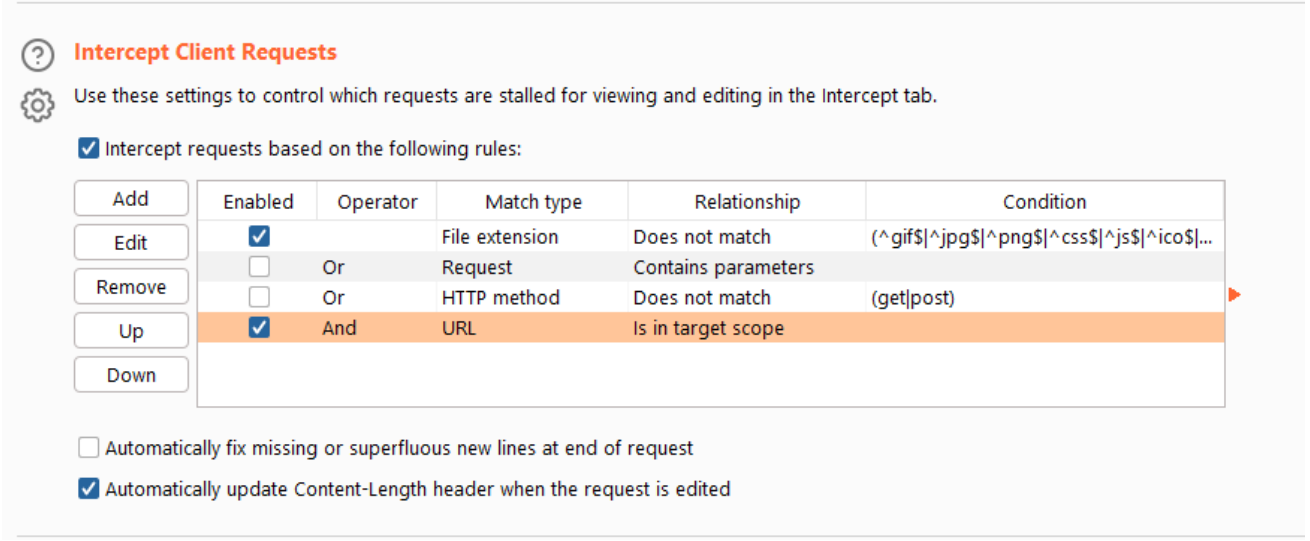


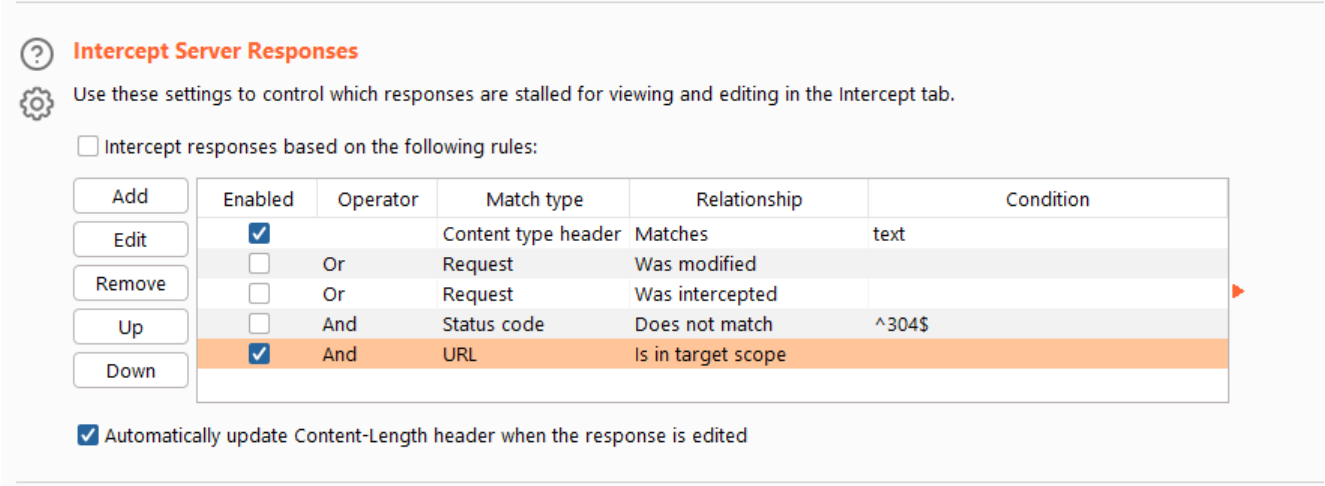
- Nhấn vào Forward để chuyển dữ liệu về trình duyệt

9. Cấu hình Scope Target cho Burpsuite

Khi chỉ muốn bắt Request/Response cho một/một số trang web nhất định, bạn có thể cấu hình cho Burpsuite chỉ bắt các dữ liệu mình muốn:

- Trong menu Proxy/Option, cấu hình chỉ bắt request và response trong scope:





- Trong menu Target/Sitemap, click chuột phải vào domain muốn test rồi chọn Add to scope