

# CÀI ĐẶT VÀ CẤU HÌNH BURPSUITE

## 1. Giới thiệu công cụ

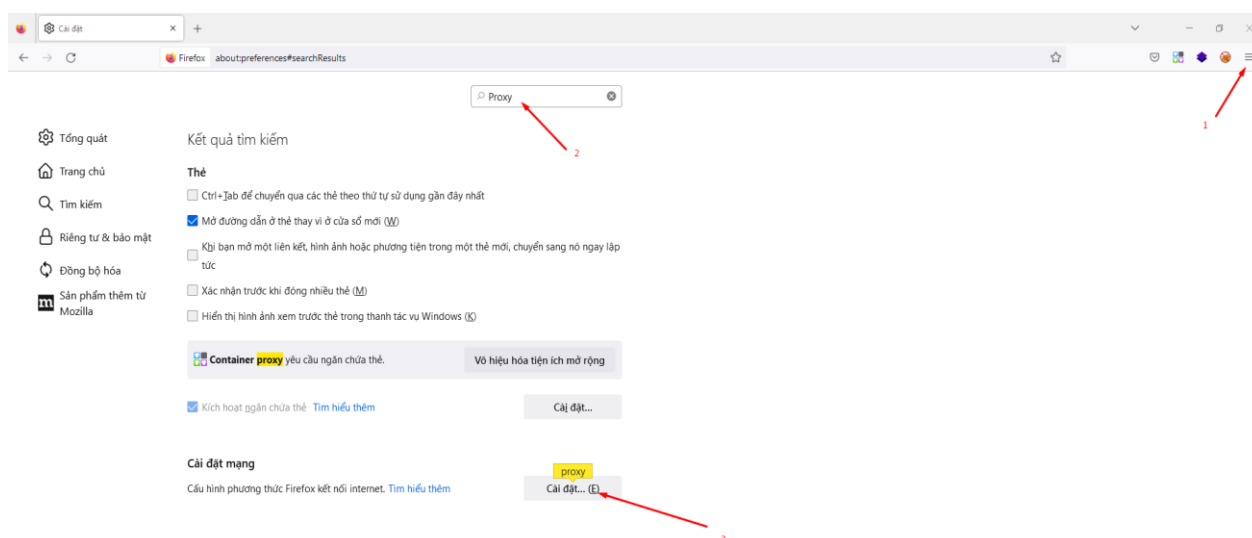
- Burpsuite là phần mềm bắt và sửa đổi gói tin HTTP/HTTPS, giúp bắt/sửa đổi/thực hành khai thác lỗ hổng bảo mật web
- Lab sẽ hướng dẫn cài đặt và cấu hình Burpsuite cơ bản để sử dụng trong các bài Lab tiếp theo

## 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



Cài đặt kết nối

Cấu hình proxy để truy cập Internet

☐ Không dùng proxy

☐ Tự động dò thiết lập của proxy cho mạng này

☐ Dùng các thiết lập proxy của hệ thống

☒ Cấu hình proxy thủ công (M)

Proxy HTTP

127.0.0.1

Cổng

8080

☐ Đồng thời sử dụng proxy này cho HTTPS

HTTPS Proxy

Cổng (:) 0

Máy chủ SOCKS

Cổng 0

☐ SOCKS v4

☒ SOCKS v5

☐ URL cấu hình proxy tự động (A)

Tải lại

Không dùng proxy cho

Ví dụ: .mozilla.org, .edu.vn, 192.168.1.0/24

Kết nối đến localhost, 127.0.0.1/8, và ::1 không bao giờ dùng proxy.

☐ Không yêu cầu xác nhận nếu đã lưu mật khẩu

☒ DNS của proxy khi dùng SOCKS v5

☒ Kích hoạt DNS over HTTPS (B)

Sử dụng nhà cung cấp

Cloudflare (Mặc định)

OK

Hủy bỏ

- 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

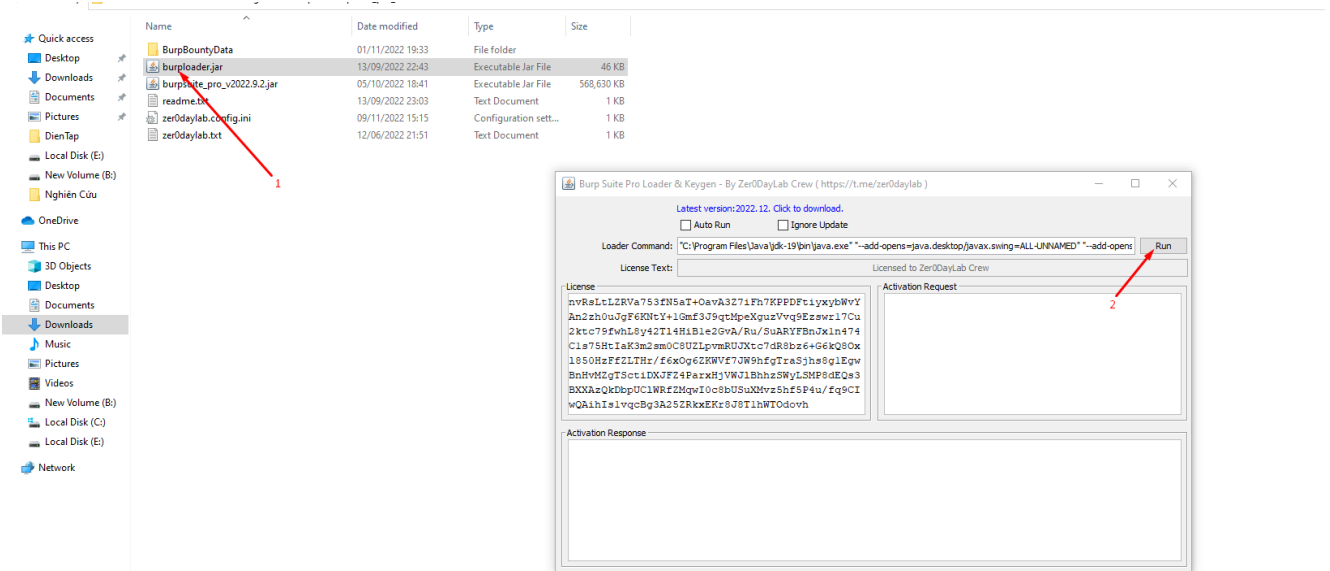
Cài đặt Java tại D:\Setup\Java hoặc download

và cài đặt từ

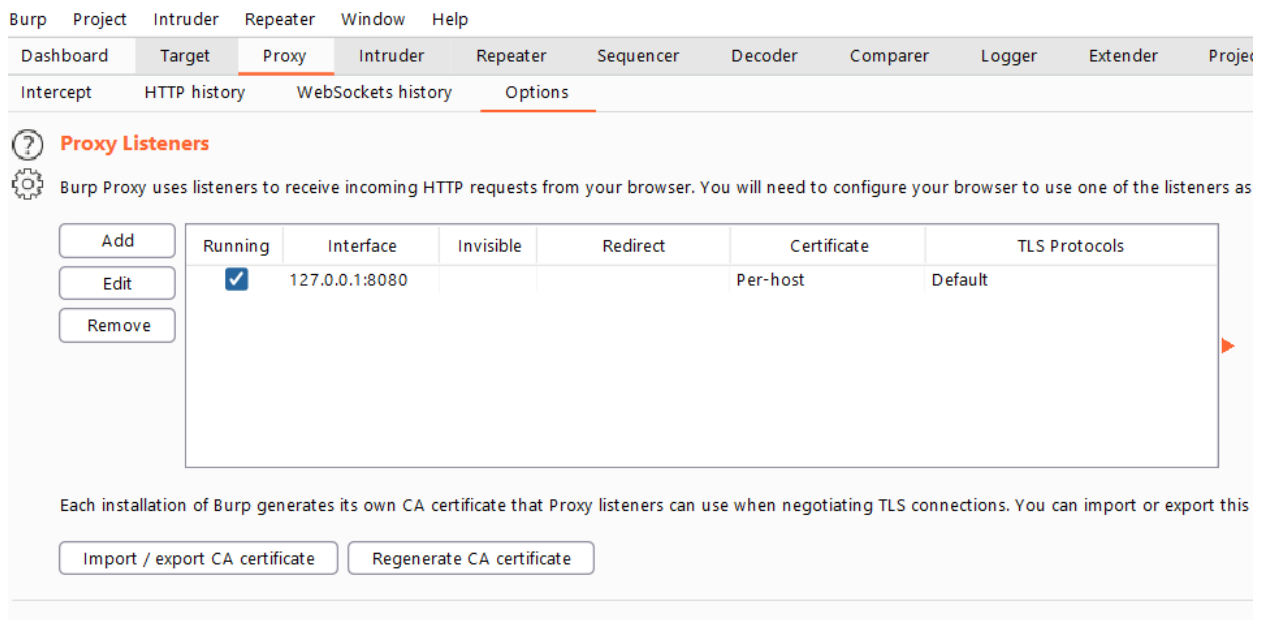
<https://www.oracle.com/java/technologies/downloads/>

## 5. Khởi chạy Burpsuite:

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

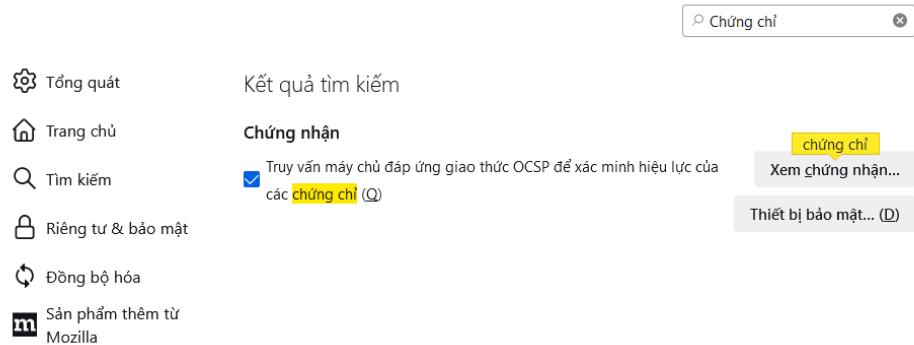
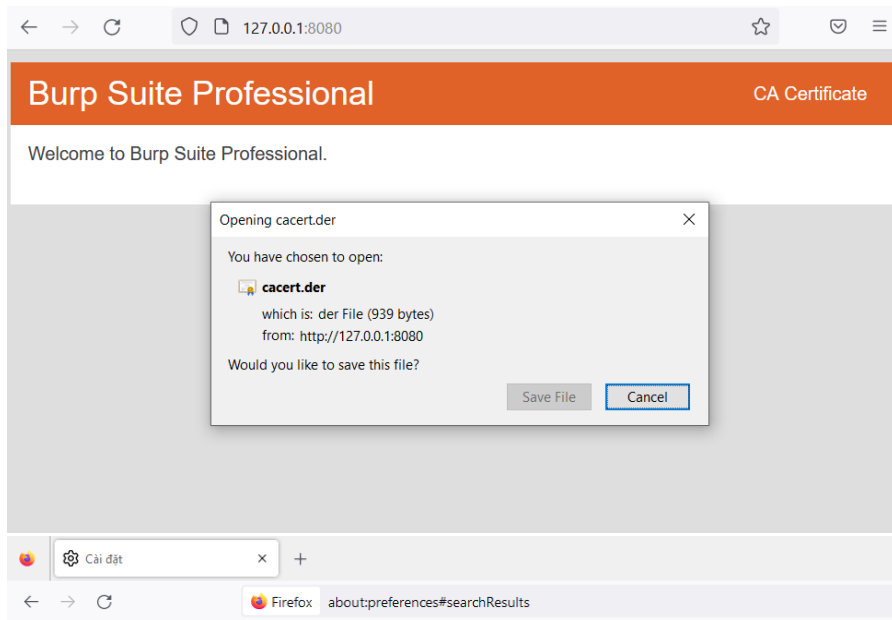


- Nếu chương trình yêu cầu license thì copy license request vào Burploader rồi copy license response paste vào Burpsuite
- Ấn Next, chọn Temporary Project, Ấn Start Burp
- Click vào menu Proxy/Options, đảm bảo rằng Proxy đang có trạng thái Running được checked ở địa chỉ 127.0.0.1

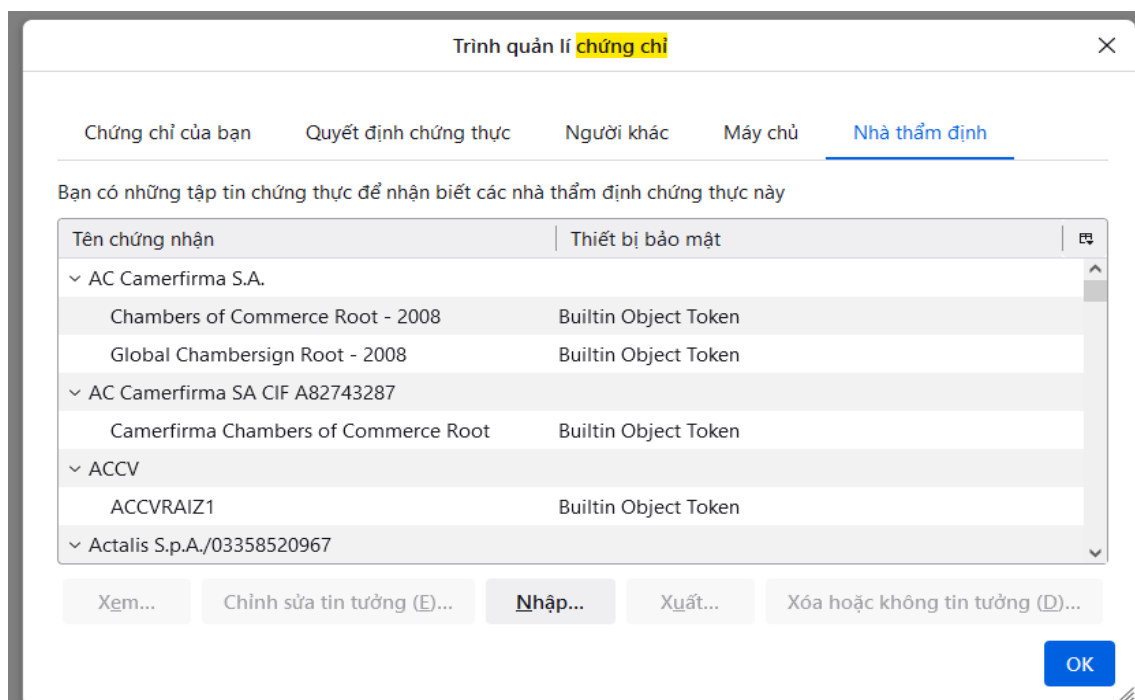


## 6. Add chứng thư số của Burpsuite vào Firefox

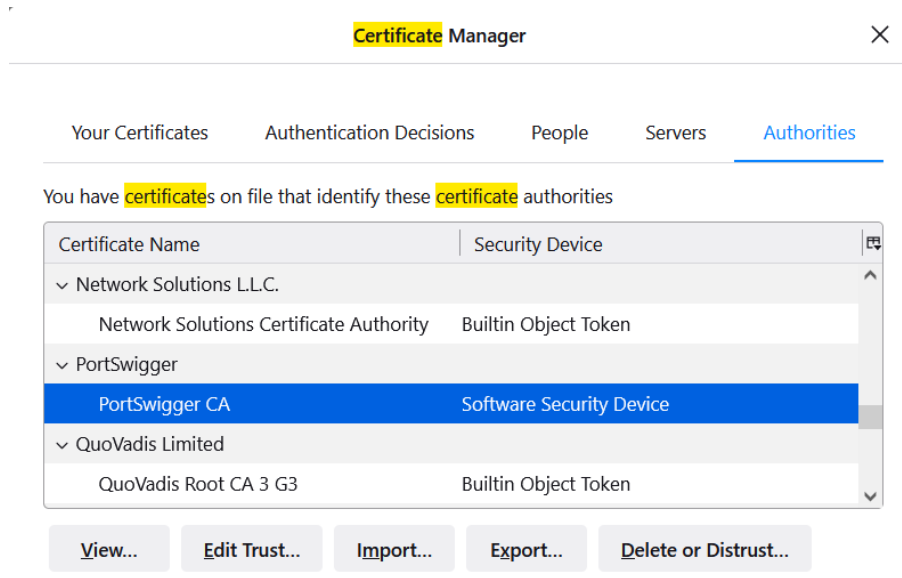
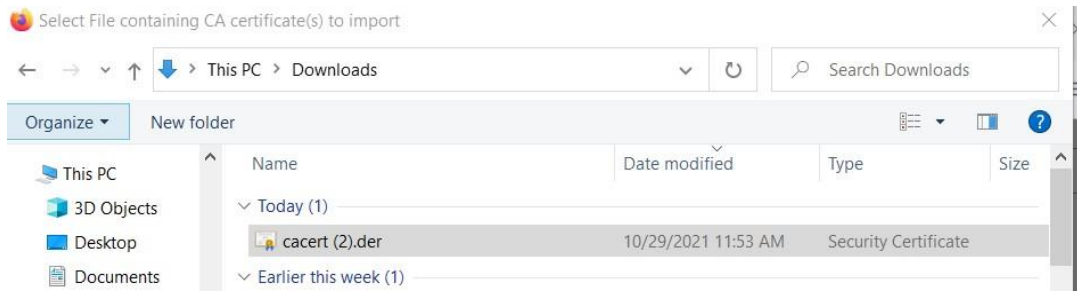
Tại trình duyệt Firefox (đã được cấu hình proxy trở vào 127.0.0.1:8080 ở bước 2, truy cập URL: <http://127.0.0.1:8080>  
Click vào chữ: CA Certificate và tải file về thư mục Download



- Mở Firefox settings, gõ vào ô tìm kiếm chữ: certificate, click View Certificates
- Tại cửa sổ Certificate Manager chuyển sang tab Authority, click nút Import

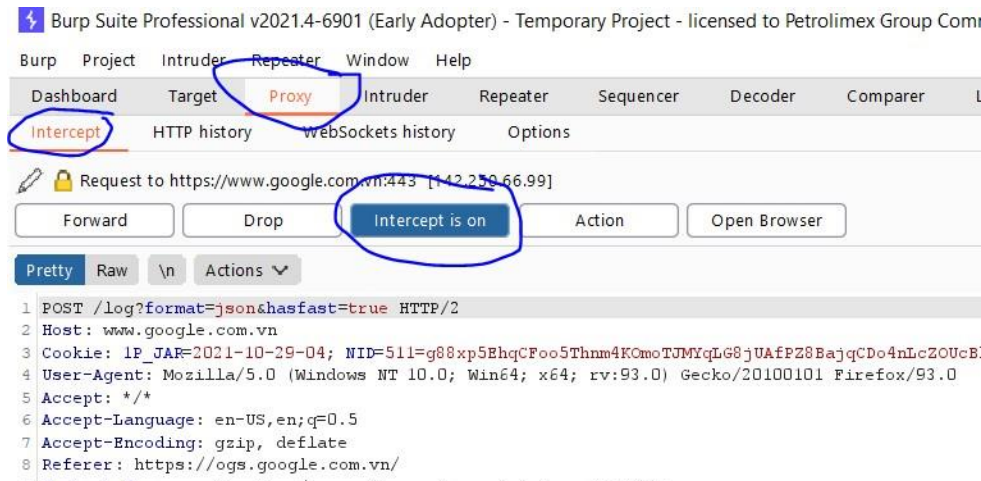


- Chuyển đến thư mục vừa Save chứng thư ở bước 1 và chọn file carcert.der, nhấn Open



- 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 Intercept 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:



## Intercept Server Responses



Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

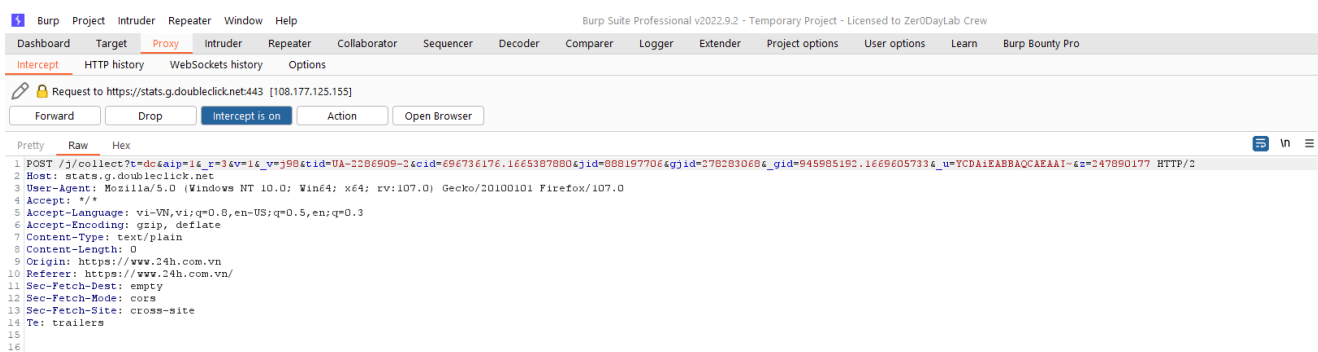
☒ Intercept responses based on the following rules:

<input checked="" type="checkbox"/>	Enabled		Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>				Content type he...	Matches	text
<input type="checkbox"/>		Or		Request	Was modified	
<input type="checkbox"/>		Or		Request	Was intercepted	
<input type="checkbox"/>		And		Status code	Does not match	^304\$
<input type="checkbox"/>		And		URL	Is in target scope	

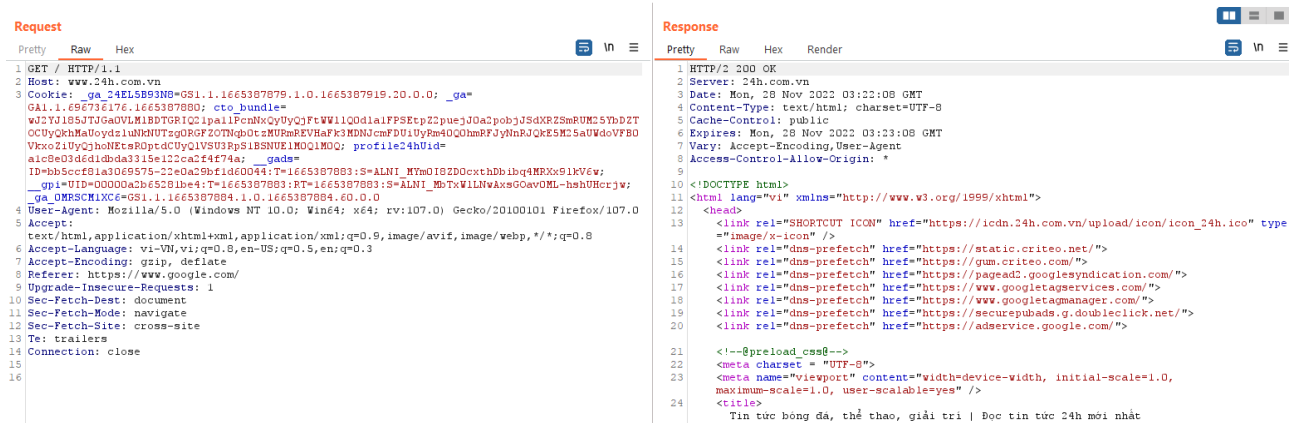
☒ Automatically update Content-Length header when the response is edited

## 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:

?

Intercept Client Requests

⚙

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☒ Intercept requests based on the following rules:

	Enabled	Operator	Match type	Relationship	Condition
Add	<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$ ...
Edit	<input type="checkbox"/>	Or	Request	Contains parameters	
Remove	<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
Up	<input checked="" type="checkbox"/>	And	URL	Is in target scope	
Down					

☐ Automatically fix missing or superfluous new lines at end of request

☒ Automatically update Content-Length header when the request is edited

## Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☐ Intercept responses based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
Edit	<input checked="" type="checkbox"/>		Content type header	Matches	text
Remove	<input type="checkbox"/>	Or	Request	Was modified	
Up	<input type="checkbox"/>	Or	Request	Was intercepted	
Down	<input type="checkbox"/>	And	Status code	Does not match	^304\$
	<input checked="" type="checkbox"/>	And	URL	Is in target scope	

☒ Automatically update Content-Length header when the response is edited

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

Burp Suite Professional v2022.9.2 - Temporary Project - Licensed to Zer0Day

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extender Project options User options

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Target Site map

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL	Params	Status	Length	MIME type	Title
https://cdn.24h.com.vn	GET	/js/24hgatracking/fe/pro...		200	114458	script	
https://cdn.24h.com.vn	GET	/upload/24h_js_library/b...		200	15613	script	
https://cdn.24h.com.vn	GET	/upload/24h_js_library/jq...		200	86003	script	
https://cdn.24h.com.vn	GET	/upload/24h_js_library/vi...	✓	200	251859	script	
https://cdn.24h.com.vn	GET	/upload/24h_js_library/vi...		200	27701	script	
https://cdn.24h.com.vn	GET	/upload/creativeGa4Trac...		200	3025	script	
https://cdn.24h.com.vn	GET	/upload/creativeGa4Trac...		200	9285	script	
https://cdn.24h.com.vn	GET	/upload/html-live/ck-tran...	✓	200	2686	JSON	
https://cdn.24h.com.vn	GET	/upload/html-live/ck-tran...	✓	200	2685	JSON	
https://cdn.24h.com.vn	GET	/upload/html-live/ck-tran...	✓	200	2685	JSON	

Request

Pretty Raw Hex

```

1 GET
  /js/24hgatracking/fe/prod/24huidutil.min.js
  HTTP/1.1
2 Host: cdn.24h.com.vn
3 Cookie: __ga_24EL5B93N8=
  GS1.1.1665387879.1.0.1665387919.20.0.0; __ga=
  GA1.1.696736176.1665387880; cto_bundle=
  wJ2YJ185JTJGaOVLMI8DTGRIQ21pallFenNxQyUyQjFtWW
  11QOd1a1FPSEtpZ2puejJ0a2pobjJSdXRZSmRUM25YbD2T
  OCUyQkhMaUoyds1uNkNUTzgORGFZOTNqb0tzmURmREVHaF
  k3MDNJcmFDU1UyRm40Q0hmRFJyNnRjQkESM25aUWdoVFB0
  VxkoZiUyQjhoNEtsROptdCUyQ1VSU3RpS1BSNUE1MQQ1MO
  Q; __gads=
  ID=bb5ccf81a3069575-22e0a29bf1d60044; T=1665387
  
```

Inspector

Request Attributes 2

Request Cookies 6

Request Headers 12

Response Headers 13

0 matches