

# CÀI ĐẶT VÀ CẤU HÌNH BURPSUITE

## 1. Giới thiệu công cụ

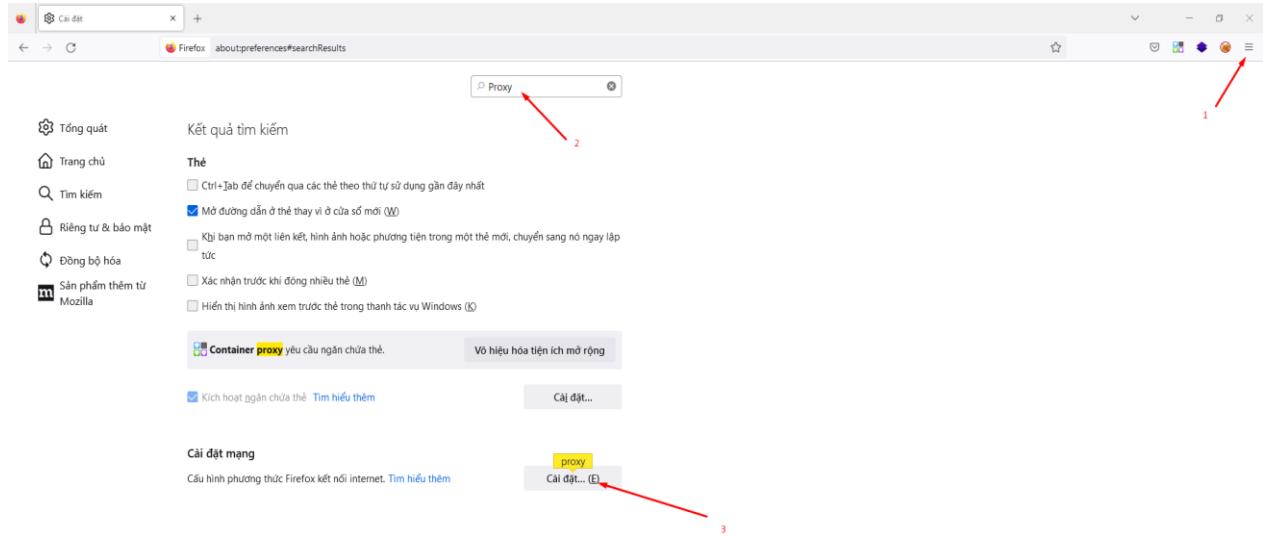
- Burpsuite là phần mềm bắt và sửa đổi gói tin HTTP/HTTPS, giúp bắt/sửa đổi/thực hành khai thác lỗ hổng bảo mật web
- Lab sẽ hướng dẫn cài đặt và cấu hình Burpsuite cơ bản để sử dụng trong các bài Lab tiếp theo

## 2. Cài đặt trên Firefox

Cài đặt trình duyệt Firefox, hoặc download và cài đặt bản mới nhất của Firefox tại địa chỉ <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

X

### 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  Cổng

Đồng thời sử dụng proxy này cho HTTPS

HTTPS Proxy  Cổng (i)

Máy chủ SOCKS  Cổng

SOCKS v4  SOCKS v5

- URL cấu hình proxy tự động (A)

Tài 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

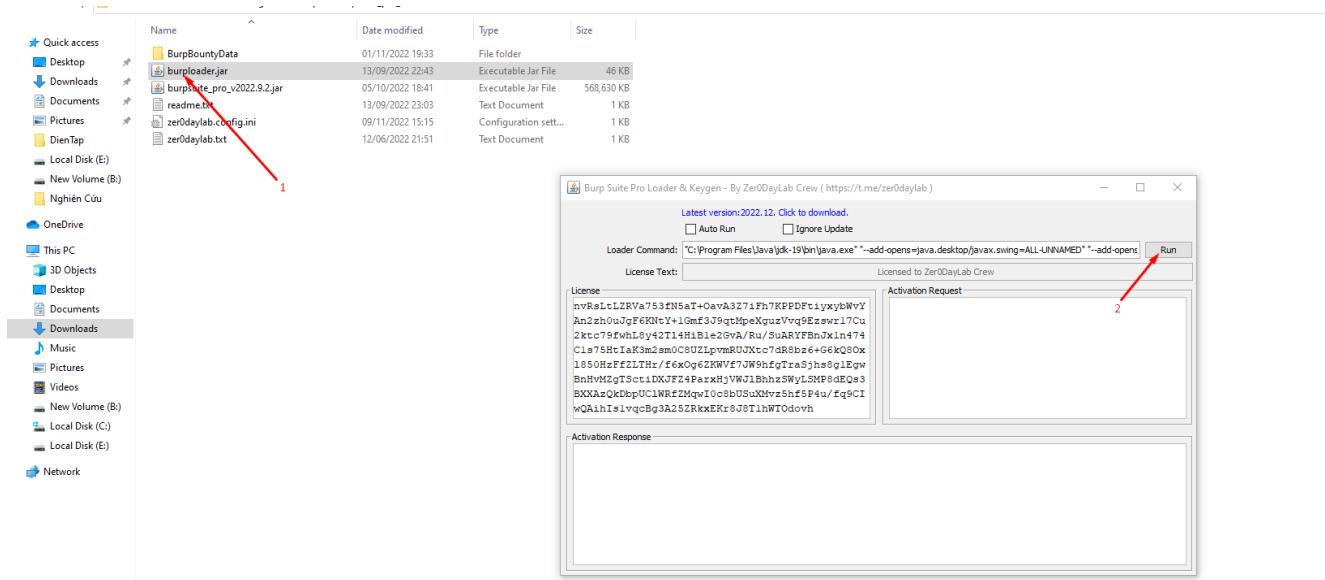
Cài đặt Java tại D:\Setup\Java hoặc download

và cài đặt từ

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

## 5. Khởi chạy Burpsuite:

- Tại thư mục Burpsuite trên desktop click double file 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 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

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project

Intercept HTTP history WebSockets history Options

**Proxy Listeners**

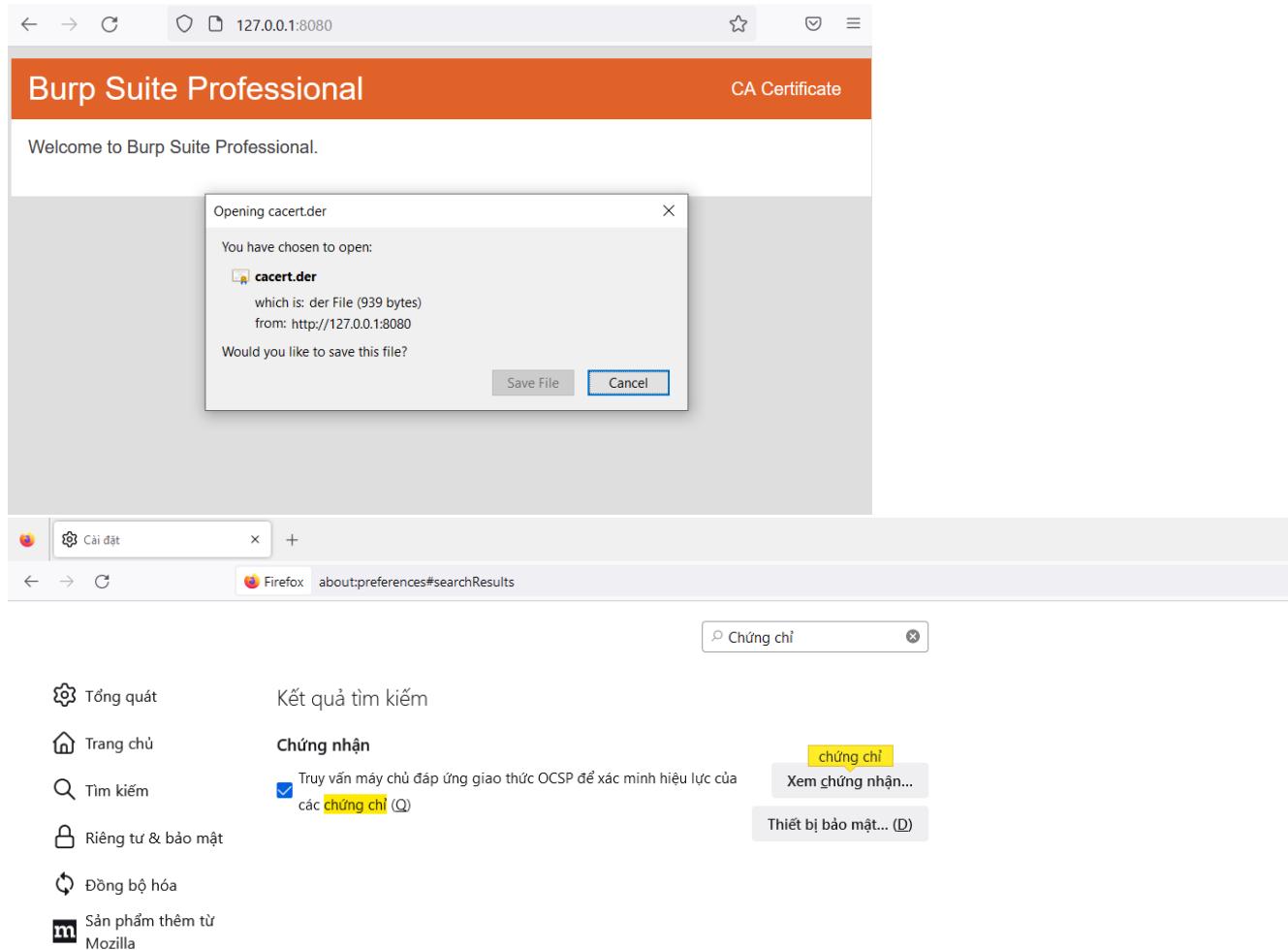
💡 Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy.

Add	Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/> 127.0.0.1:8080				Per-host	Default
<input type="button" value="Remove"/>						

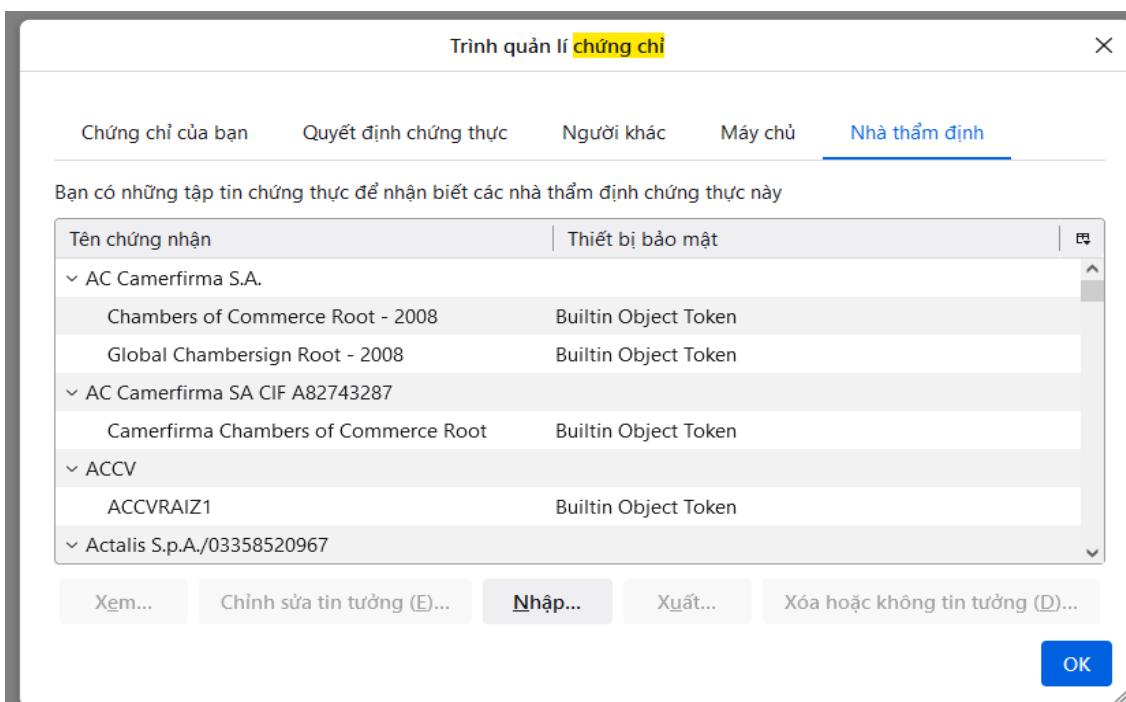
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate.

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

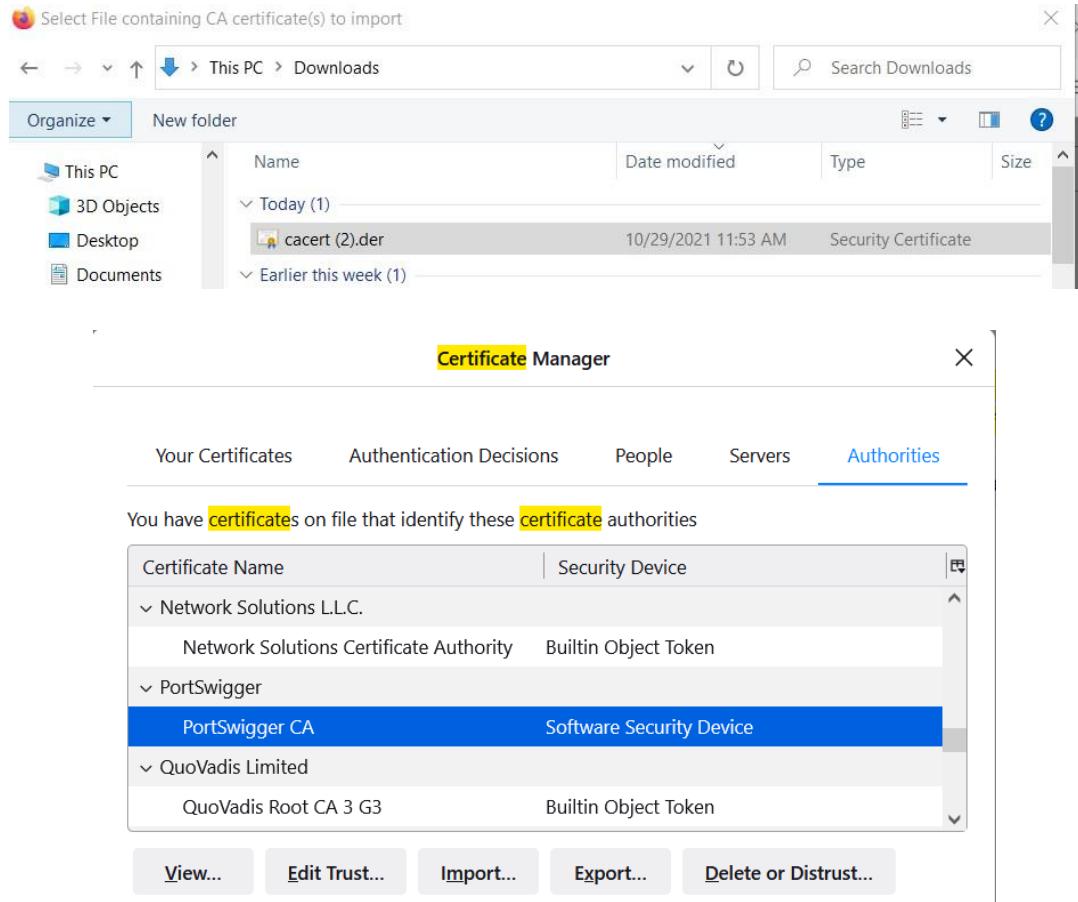
Tại trình duyệt Firefox (đã được cấu hình proxy trả vào 127.0.0.1:8080 ở bước 2, truy cập URL: <http://127.0.0.1:8080>  
Click vào chữ: CA Certificate và tải file về thư mục Download



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

```

    POST /log?format=json&hasfast=true HTTP/2
    Host: www.google.com.vn
    Cookie: 1P_JAR=2021-10-29-04; NID=511=g88xp5EhqCFoo5Thnm4KQmoTJMqLg8jUAfpZ8BajqCD04nLcZOUcB
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
    Accept: /*
    Accept-Language: en-US,en;q=0.5
    Accept-Encoding: gzip, deflate
    Referer: https://ogs.google.com.vn/
  
```

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:

Add	Enabled	Operator	Match type	Relationship	Condition
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>		Content type he...	Matches	text
<input type="button" value="Remove"/>	<input type="checkbox"/>	Or	Request	Was modified	
<input type="button" value="Up"/>	<input type="checkbox"/>	Or	Request	Was intercepted	
<input type="button" value="Down"/>	<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>

Burp Suite Professional v2022.9.2 - Temporary Project - Licensed to Zer0DayLab Crew

POST /j/collect?t=dc&alp=1&r=3&v=14\_v=j90&tid=UA-2206909-2&cid=69673176.1665307880&jid=800197706&gjid=2702830684\_gid=945985192.1669605733&u=YCDAiEABBAQCAAAI-4e=247890177 HTTP/2

Host: stats.g.doubleclick.net

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0

Accept: \*/\*

Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Content-Type: text/plain

Content-Length: 0

Origin: https://www.24h.com.vn

Referer: https://www.24h.com.vn/

Sec-Fetch-Dest: empty

Sec-Fetch-Mode: cors

Sec-Fetch-Site: cross-site

Tel: trailers

- 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:

```

Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: www.24h.com.vn
3 Cookie: _ga=2AEL5B93NB=GS1.1.16e5307879.1.0.16e53078919.20.0.; _gat=GAI.1.e9e73f17e.16e5307880; cto_bundle=w2JYj185jTJGauVLM1BDTGRIQClpailPcnNxQyUQjFtWllQ0dla1FPSEtpZ2puejJ0a2pobj5dXRSmRUM25YbDZT0CUCYQkhMaJoydzlunNNNTzg0RGFZOTnghOtzMUPnREVAHfk3MDNncmFDUiUyPm40Q0nmFyJhlnPQjKE5M25aUWdoVFBD0VxkzIUYq3hNEtsR0ptdC0yQ1VSU3p81SNUE1MQ1MOQ; profile24huid=aicSeetw1lbdal315e12cfa4f74a; gads=D-mp-Script-a10e5f75-22e0-481d-e0044:T-16e5307883:S-ALN1_HYmo1BZD0cxthDbibq4MRXx91kVew;-_ga_0M8CM1XG=0S1.1.16e5307884.1.0.16e5307884.16.0.0
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Referer: https://www.google.com/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: cross-site
13 Te: trailer
14 Connection: close
15
16

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Server: 24h.com.vn
3 Date: Mon, 28 Nov 2022 03:22:08 GMT
4 Content-Type: text/html; charset=UTF-8
5 Cache-Control: public
6 Expires: Mon, 28 Nov 2022 03:23:08 GMT
7 Vary: Accept-Encoding,User-Agent
8 Access-Control-Allow-Origin: *
9
10 <!DOCTYPE html>
11 <html lang="v1" xmlns="http://www.w3.org/1999/xhtml">
12   <head>
13     <link rel="SHORTCUT ICON" href="https://icdn.24h.com.vn/upload/icon/icon_24h.ico" type="image/x-icon" />
14     <link rel="dns-prefetch" href="https://static.criteo.net/" />
15     <link rel="dns-prefetch" href="https://gum.criteo.com/" />
16     <link rel="dns-prefetch" href="https://pagead2.googlesyndication.com/" />
17     <link rel="dns-prefetch" href="https://www.googletagservices.com/" />
18     <link rel="dns-prefetch" href="https://www.googletagmanager.com/" />
19     <link rel="dns-prefetch" href="https://securepubads.g.doubleclick.net/" />
20     <link rel="dns-prefetch" href="https://adservice.google.com/" />
21   <!--@preload_css@-->
22   <meta charset="UTF-8">
23   <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=yes" />
24 </head>
  Tin tức bóng đá, thể thao, giải trí | Đọc tin tức 24h mới nhất
  ...

```

- 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:

Add	Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="button"/> Add	<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$...)
<input type="button"/> Edit	<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="button"/> Remove	<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="button"/> Up	<input checked="" type="checkbox"/>	And	URL	Is in target scope	
<input type="button"/> 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
Add	<input checked="" type="checkbox"/>		Content type header	Matches	text
Edit	<input type="checkbox"/>	Or	Request	Was modified	
Remove	<input type="checkbox"/>	Or	Request	Was intercepted	
Up	<input type="checkbox"/>	And	Status code	Does not match	^304\$
Down	<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

Target

Site map Scope Issue definitions

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/24hgttracking/fe/prod/24huidutil.min.js		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...		✓	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/24hgttracking/fe/prod/24huidutil.min.js
HTTP/1.1
2 Host: cdn.24h.com.vn
3 Cookie: _ga=GA1.1.1665387879.1.1665387919.20.0; _ga=GA1.1.696736176.1665387880; cto_bundle=wJ2YJ185jTJGaoOVL1LBDTGR1Q2lpa1FcNnxQyUyQjFtWW11QDla1PFSstpZ2puej0JaapobjJSdXZSmRUM35YdZT
OCUyQkhMaUoydzluNKNUTzg0RGFZOTNgb0tzMURmEVHafk3MDNJcmFDUiUyRm40Q0hmRFJyNnRJQkE5M25aUWdoVFBOVkxoZ1UyQjhNETsR0ptdCuyQ1VSU3RpS1BSNUE1MOQ1MO
Q; __gads=ID:b5ccf81a3069575-22e0a29bf1d60044:T=1665387

```

Inspector

Request Attributes  
Request Cookies  
Request Headers  
Response Headers