

Android Mobile Pentest 101

© tsug0d, September 2018

Bài 5 – Phân tích động

Mục tiêu: Phân tích động sử dụng BurpSuite

Giới Thiệu

- **Phân tích động là quá trình kiểm thử và đánh giá trong thời gian thực**
- Mục đích của phân tích động là xem kết quả trả về, biểu hiện của chương trình, thay vì ngồi đọc source-code như phân tích tĩnh
- Chúng ta sẽ sử dụng BurpSuite để tiến hành phân tích động

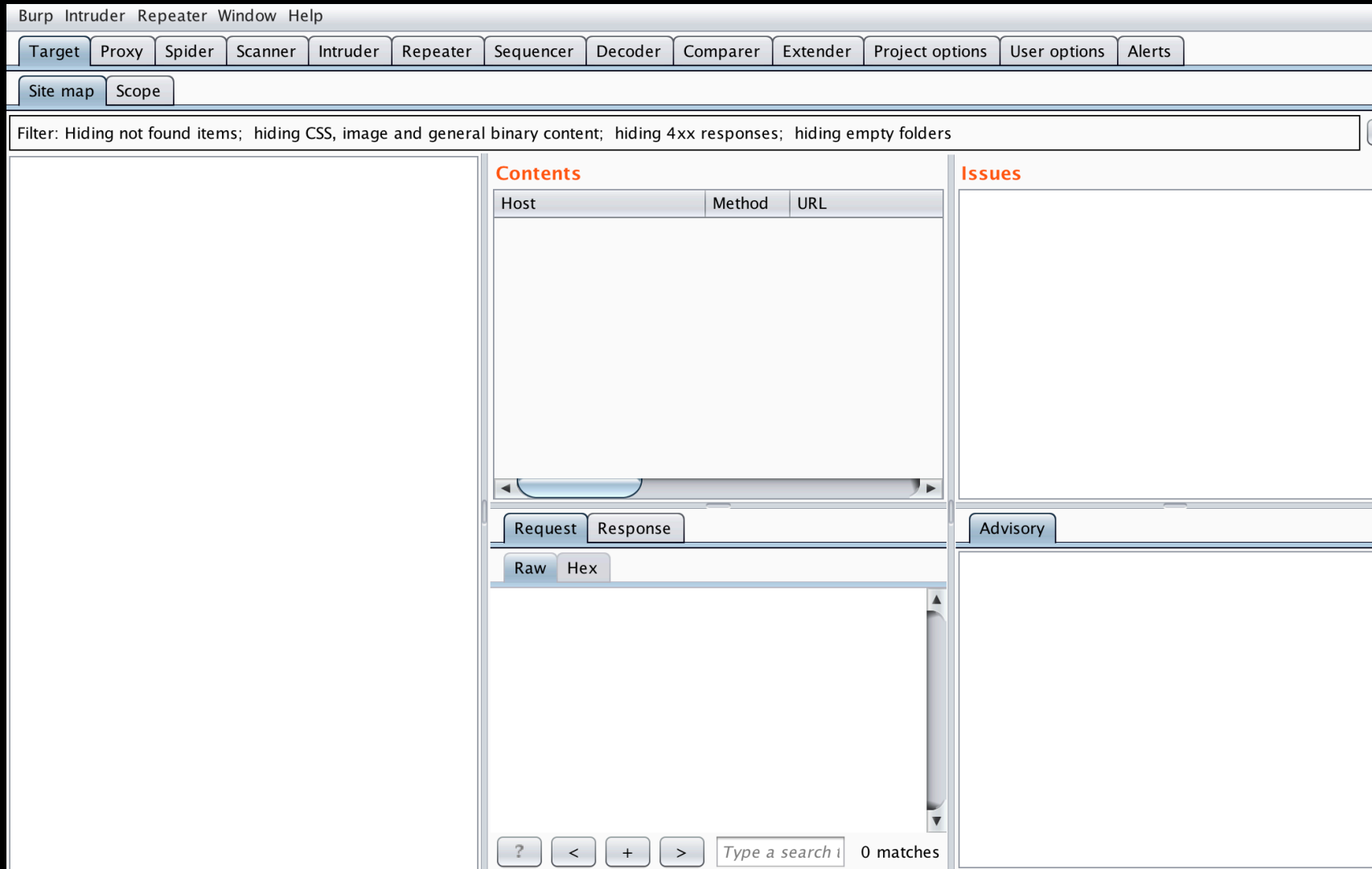


Giới Thiệu

- Burp suite là một ứng dụng java dùng để kiểm thử xâm nhập ứng dụng web, được sử dụng bởi nhiều nhà bảo mật chuyên nghiệp trên thế giới
- Để cài Burp Suite, truy cập:
<https://portswigger.net/burp/communitydownload>
- Tải về file phù hợp với máy bạn, trong bài này, mình sử dụng file **.jar**

Cách Sử Dụng

- Mở **Burp Suite** lên, giao diện như sau:



Cách Sử Dụng

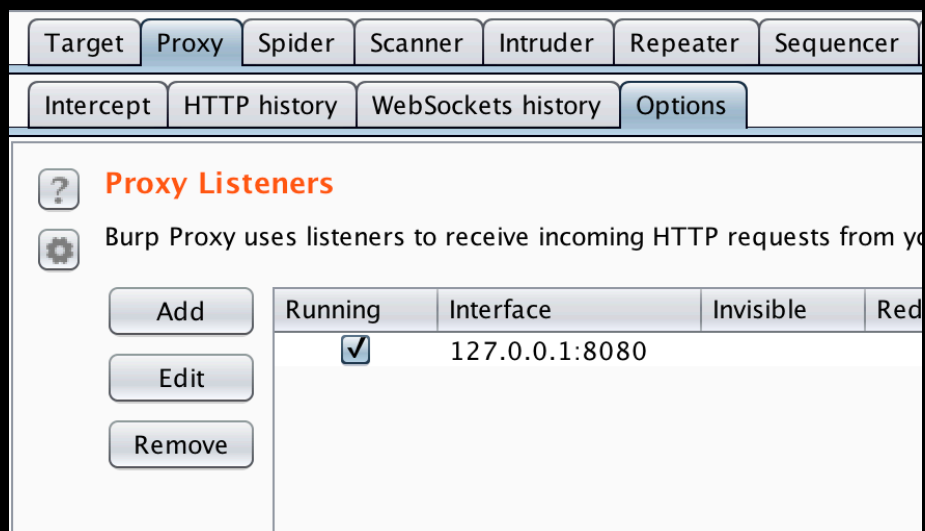
- Trong bài này mình sẽ không giới thiệu tất cả tính năng của Burp, mình chỉ tập trung vào những tính năng quan trọng đối với pentest mobile app
- Đầu tiên cần phải cấu hình cho điện thoại ảo “**proxy**” thông qua BurpSuite, nghĩa là mọi request được gửi ra từ điện thoại ảo đều được **BurpSuite** bắt lại, rồi mới đi lên server
- Kiểm tra địa chỉ ip điện thoại ảo để cấu hình cho đúng:

```
🍏 ~/Desktop/mobile/tools/ ./adb devices
```

```
List of devices attached
```

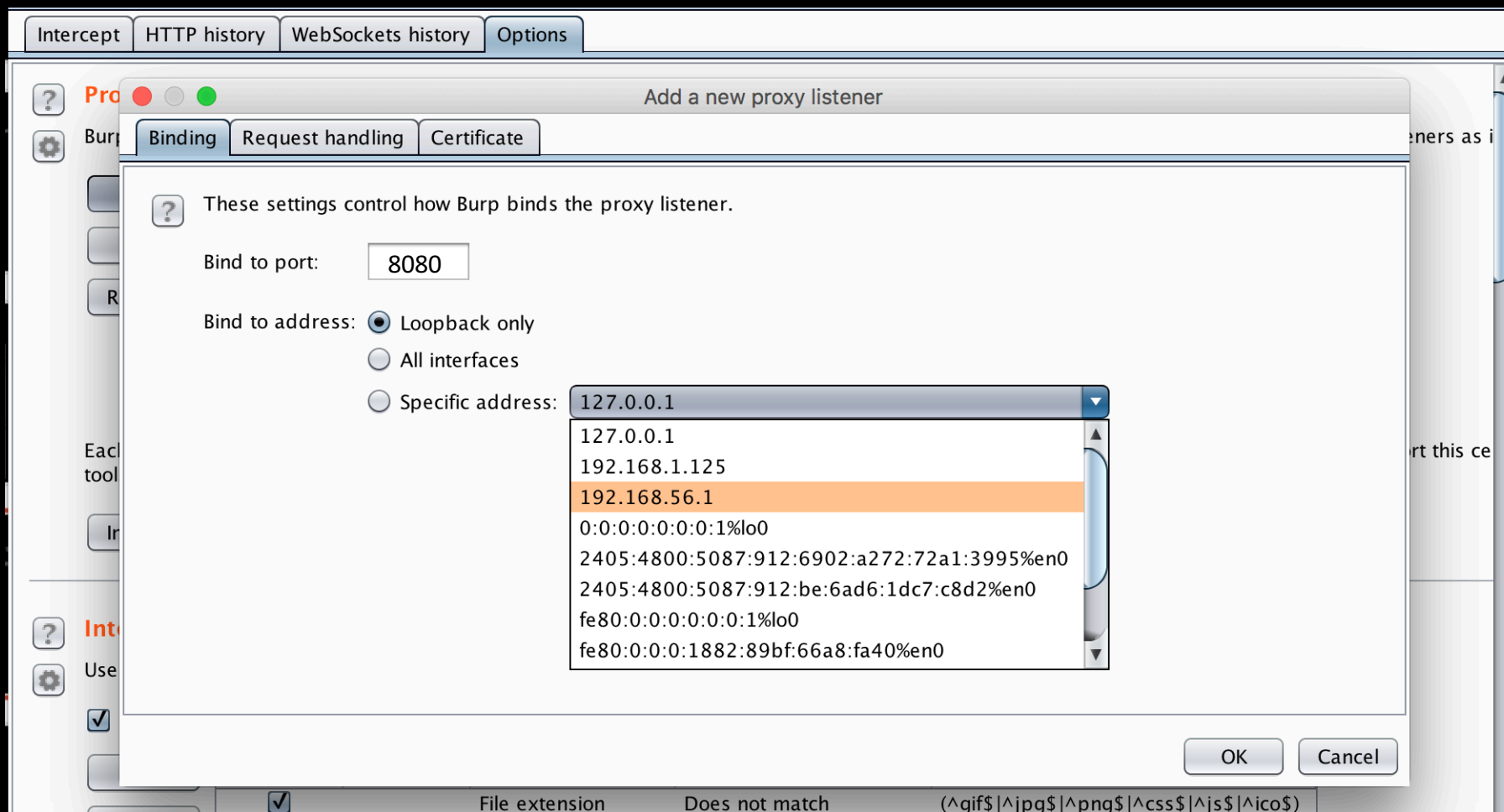
```
192.168.56.101:5555      device
```

- **Burp Suite -> Proxy -> Options**



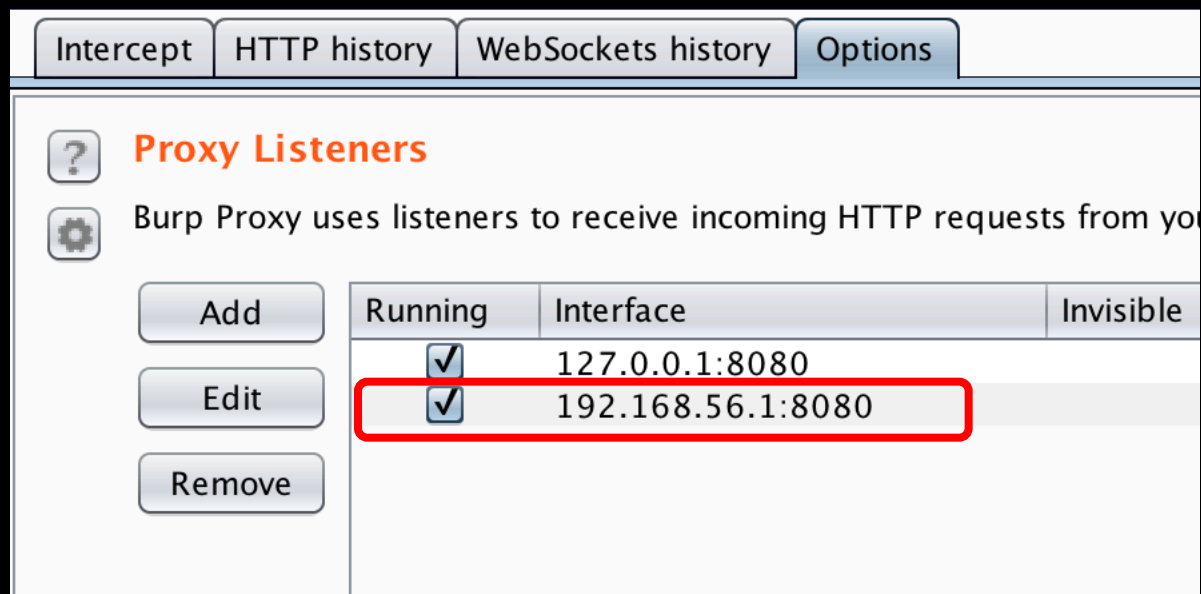
Cách Sử Dụng

- Click Add, Chọn ip address nằm trong dải mạng của ip address điện thoại ảo



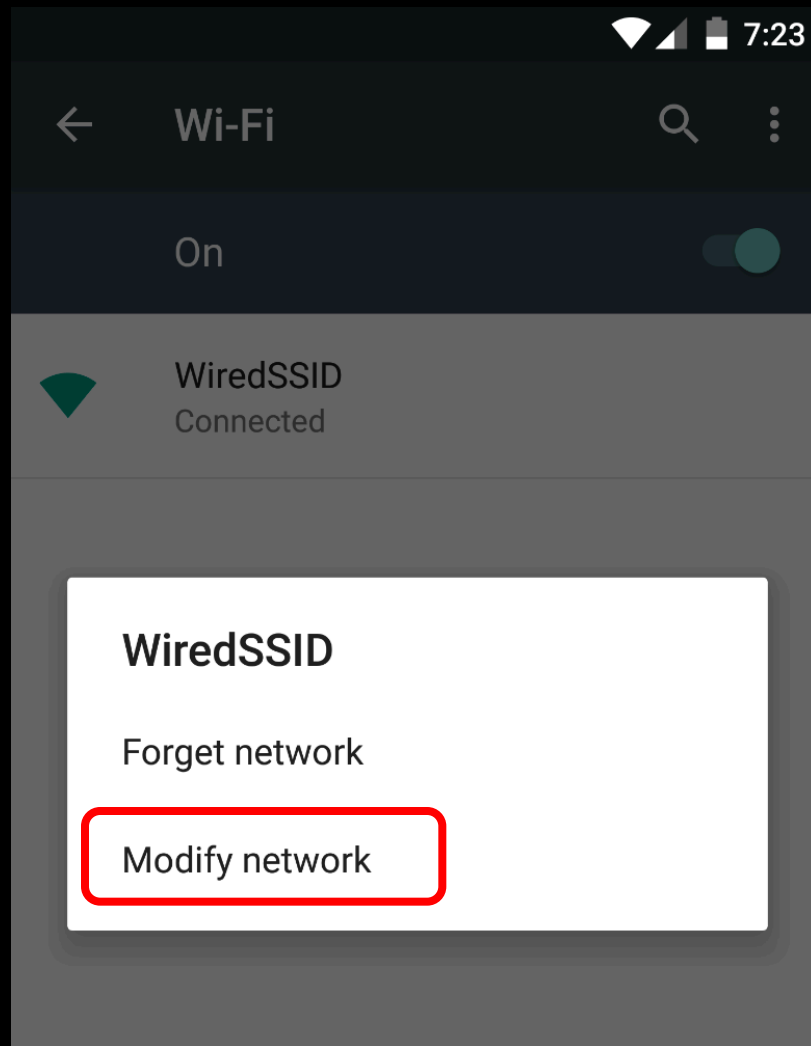
Cách Sử Dụng

- Ở **Proxy Listeners** đã xuất hiện interface ta vừa tạo, tick vào Running



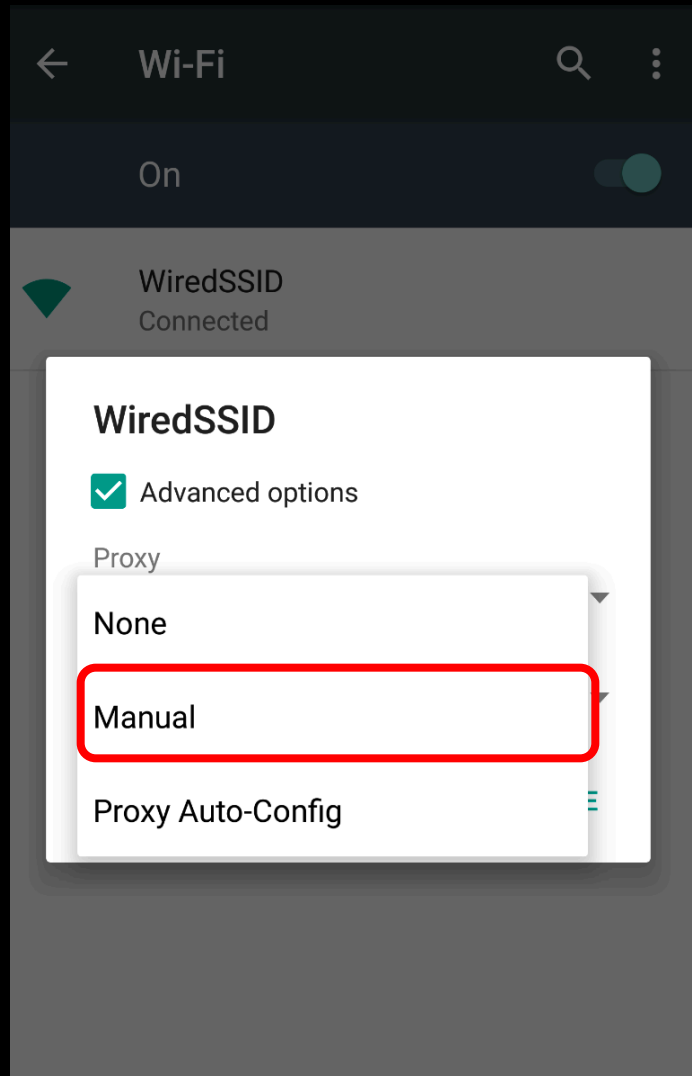
Cách Sử Dụng

- Vào điện thoại ảo -> Settings -> Wifi, Click và giữ chuột vào trường wifi



Cách Sử Dụng

- Chọn **Modify network**, tick vào **Advanced options**, Ở **Proxy scroll**, chọn **Manual**



Cách Sử Dụng

- Điền thông tin proxy chúng ta đã tạo ở trên -> Save

WiredSSID

☒ Advanced options

Proxy
Manual

The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname
192.168.56.1

Proxy port
8080

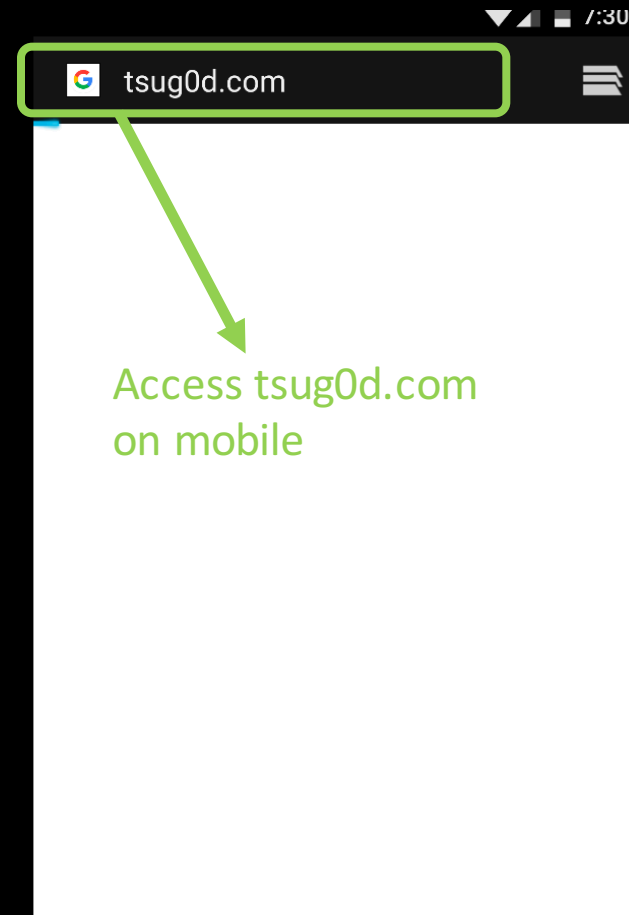
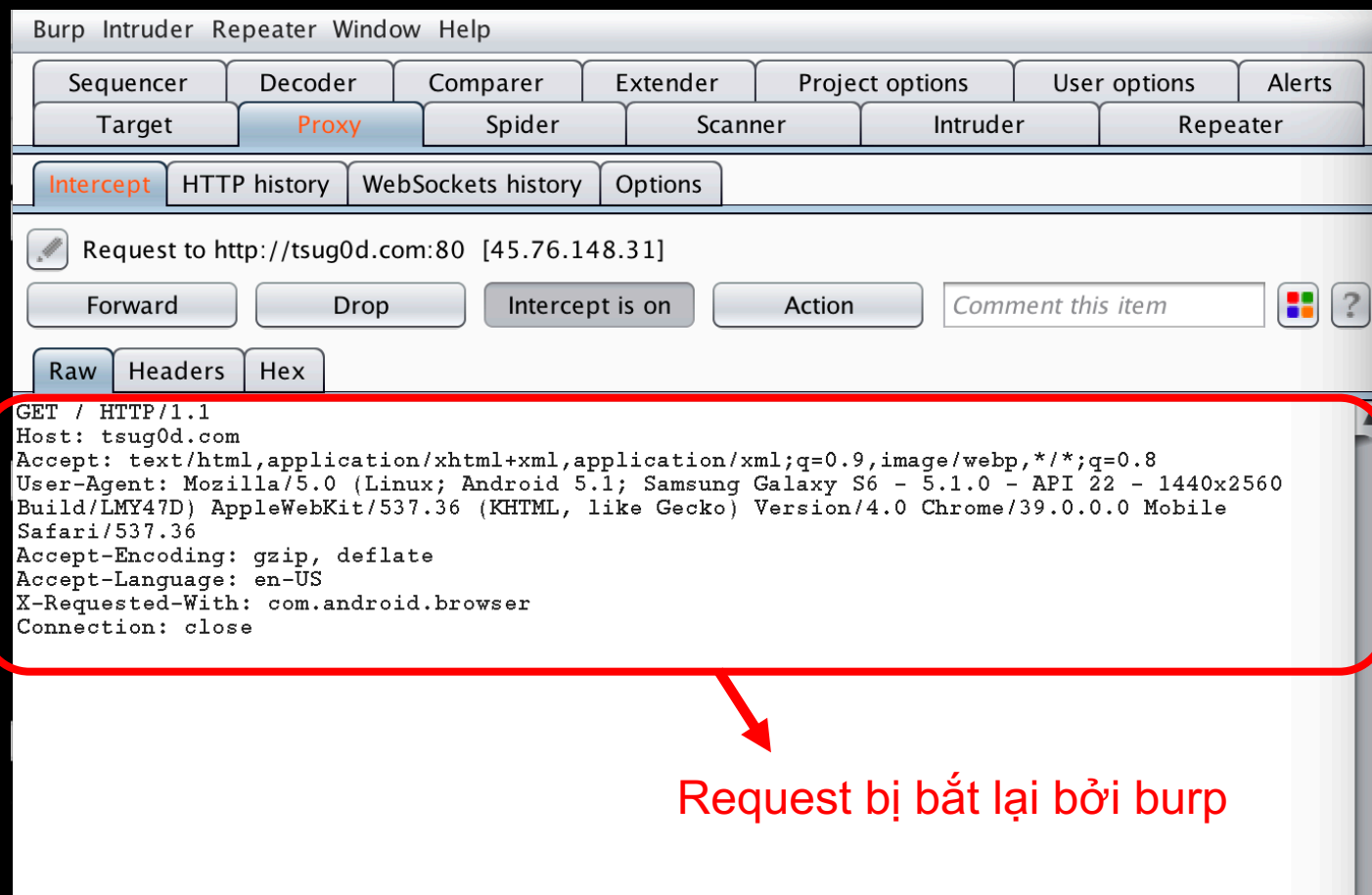
Bypass proxy for
example.com,mycomp.test.com,l

IP settings
DHCP

CANCEL SAVE

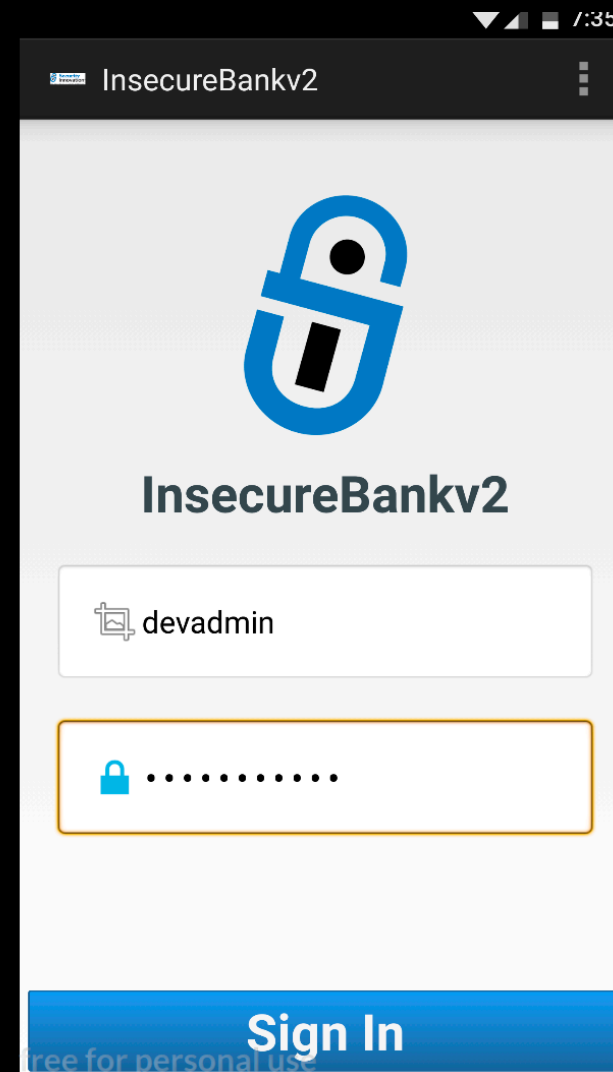
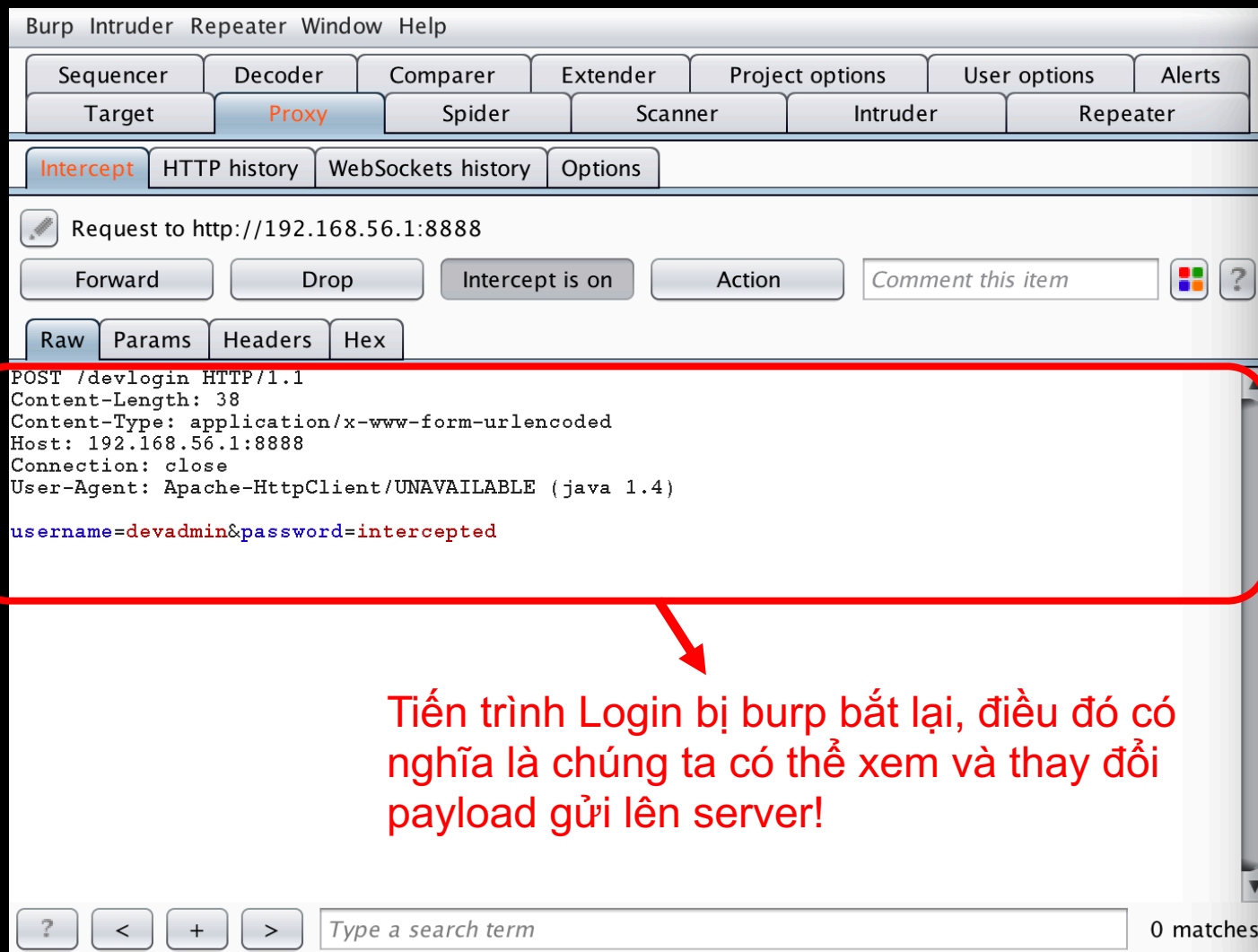
Cách Sử Dụng

- Chúng ta gần như hoàn thành phần cấu hình, truy cập thử trang tsug0d.com



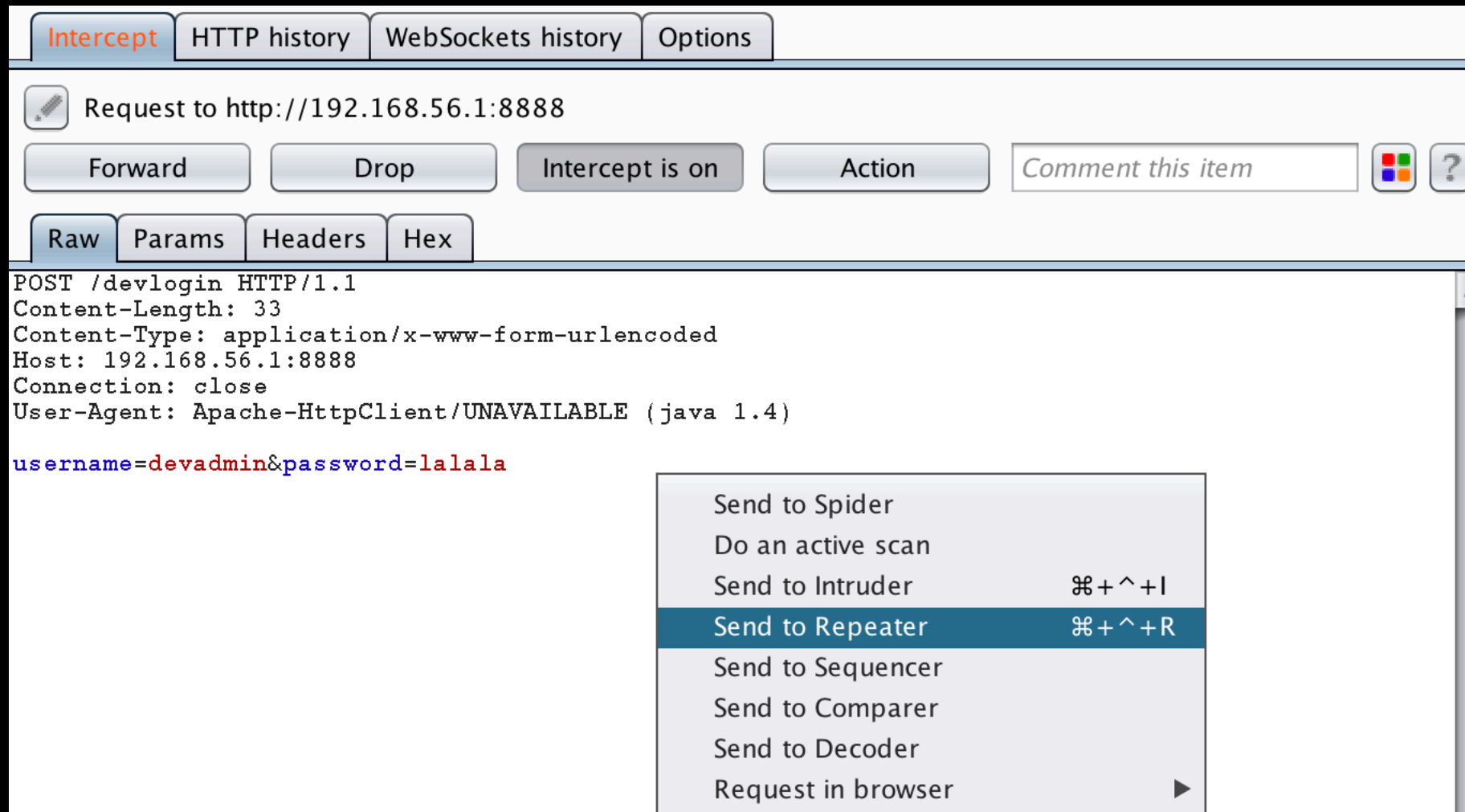
Cách Sử Dụng

- Sử dụng thử app:



More Burp

- Burp có nhiều tính năng rất hay, 1 trong số đó là **Repeater**, tính năng này giúp bạn tiết kiệm thời gian, không cần request và bắt lại nhiều lần nữa



More Burp

- Send request vào **Repeater**, và sử dụng lại nhiều lần tại tab này

The screenshot displays the Burp Suite interface with the **Repeater** tab selected. The top toolbar includes buttons for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and Alerts. Below the toolbar, a tab bar shows '1 x' and an ellipsis. The main area is divided into two panels: **Request** and **Response**.

Request Panel: It has sub-tabs for Raw, Params, Headers, and Hex. The **Raw** tab is active, showing the following text:

```
POST /devlogin HTTP/1.1
Content-Length: 37
Content-Type: application/x-www-form-urlencoded
Host: 192.168.56.1:8888
Connection: close
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
username=devadmin&password=lalalanana
```

The **Go** button is highlighted with a red rectangle. To its right are **Cancel**, **< | ▾**, and **> | ▾** buttons.

Response Panel: It has sub-tabs for Raw, Headers, and Hex. The **Raw** tab is active, showing the following text:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 54
Connection: close
Date: Tue, 11 Sep 2018 18:40:34 GMT
Server: localhost

{"message": "Correct Credentials", "user": "devadmin"}
```

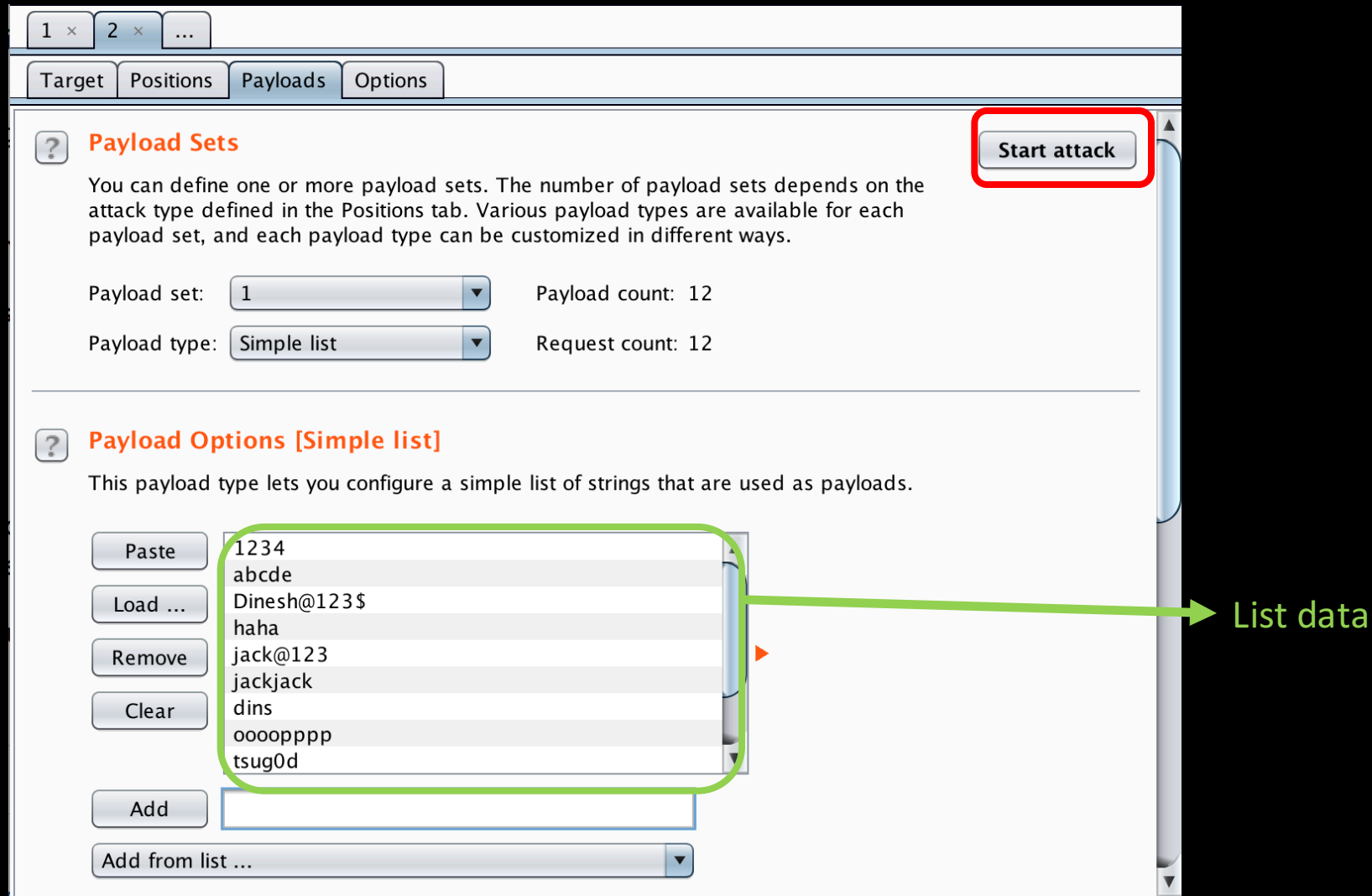
More Burp

- Bạn cũng có thể tấn công vét cạn bằng cách gửi request vào tab **Intruder**
- Ta thử **vét cạn mật khẩu** cho user “dinesh”:

The screenshot shows the Burp Suite interface with the **Intruder** tab selected. The **Payload Positions** sub-tab is active, displaying a configuration window for an attack. The **Attack type** is set to **Sniper**. The base request is a POST to `/login HTTP/1.1` with headers: `Content-Length: 28`, `Content-Type: application/x-www-form-urlencoded`, `Host: 192.168.56.1:8888`, `Connection: close`, and `User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)`. The payload is `username=dinesh&password=dkm`. A green box highlights the `dkm` part, with a green arrow pointing to it and a text annotation: "Ký hiệu \$ để định danh cho phần được vét cạn" (The \$ symbol is used to identify the part to be brute-forced). On the right side of the configuration window, there are buttons for **Start attack**, **Add \$**, **Clear \$**, **Auto \$**, and **Refresh**.

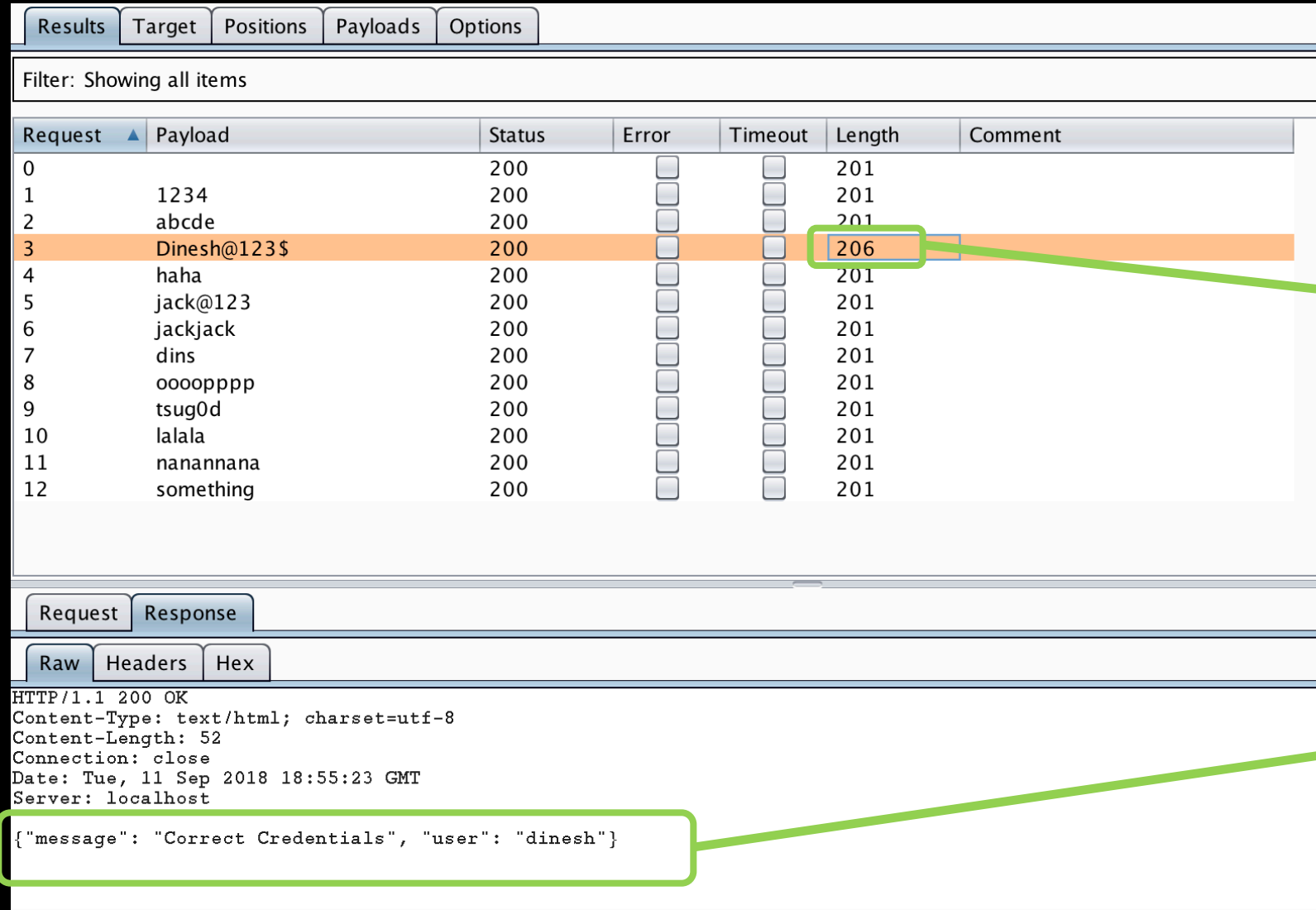
More Burp

- Trong tab **intruder**, bấm qua **Payloads tab**, ở phần **Payload Options** là bộ payload ta dùng để vét cạn vào vị trí password, bấm **Start attack**



More Burp

- Kết quả!



The screenshot shows the Burp Suite interface. At the top, there are tabs for 'Results', 'Target', 'Positions', 'Payloads', and 'Options'. Below these is a filter bar that says 'Filter: Showing all items'. The main table lists 13 requests. Request 3 is highlighted in orange. A green box highlights the 'Length' column for Request 3, which is '206'. A green arrow points from this box to a text annotation. Below the table, there are tabs for 'Request' and 'Response'. The 'Request' tab is selected, and it shows the raw HTTP request details. A green box highlights the JSON body of the request, and a green arrow points from this box to another text annotation.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	201	
1	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
2	abcde	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
3	Dinesh@123\$	200	<input type="checkbox"/>	<input type="checkbox"/>	206	
4	haha	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
5	jack@123	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
6	jackjack	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
7	dins	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
8	ooooopppp	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
9	tsug0d	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
10	lalala	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
11	nanannana	200	<input type="checkbox"/>	<input type="checkbox"/>	201	
12	something	200	<input type="checkbox"/>	<input type="checkbox"/>	201	

Request: HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 52
Connection: close
Date: Tue, 11 Sep 2018 18:55:23 GMT
Server: localhost

Raw Headers Hex

```
{"message": "Correct Credentials", "user": "dinesh"}
```

Có 1 request có độ dài khác với các request còn lại!

True!

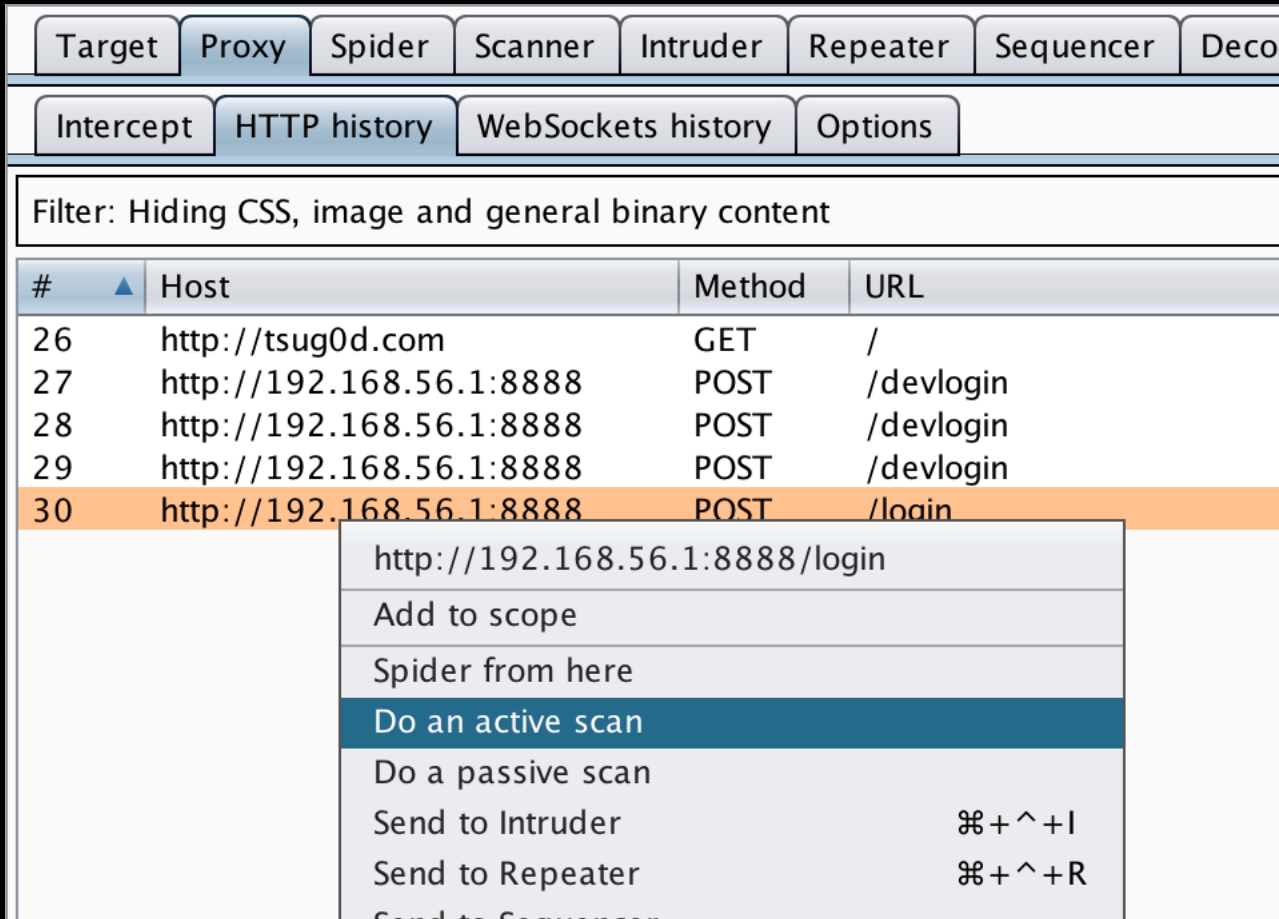
More Burp

- **History**, hiển thị lịch sử các request được gửi ra từ điện thoại ảo

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender
Intercept	HTTP history	WebSockets history	Options						
Filter: Hiding CSS, image and general binary content									
#	▲	Host	Method	URL	Params	Edit			
26		http://tsug0d.com	GET	/					
27		http://192.168.56.1:8888	POST	/devlogin	✓				
28		http://192.168.56.1:8888	POST	/devlogin	✓				
29		http://192.168.56.1:8888	POST	/devlogin	✓				
30		http://192.168.56.1:8888	POST	/login	✓				

More Burp

- Sử dụng tab Scanner (BurpSuite pro mới có nha) để tiến hành scan tìm lỗi trong request được chỉ định



The screenshot displays the Burp Suite interface with the 'Scanner' tab selected. The top navigation bar includes 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', and 'Decoder'. Below this, a secondary bar shows 'Intercept', 'HTTP history', 'WebSockets history', and 'Options'. A filter is applied: 'Filter: Hiding CSS, image and general binary content'. The main panel shows a table of HTTP requests:

#	Host	Method	URL
26	http://tsug0d.com	GET	/
27	http://192.168.56.1:8888	POST	/devlogin
28	http://192.168.56.1:8888	POST	/devlogin
29	http://192.168.56.1:8888	POST	/devlogin
30	http://192.168.56.1:8888	POST	/login

A context menu is open over the selected request (row 30), showing the following options:

- http://192.168.56.1:8888/login
- Add to scope
- Spider from here
- Do an active scan**
- Do a passive scan
- Send to Intruder ⌘+^+I
- Send to Repeater ⌘+^+R
- Send to Sequencer

More Burp

- Kết quả

The screenshot displays the Burp Suite interface. At the top, there's a menu bar with 'Burp', 'Intruder', 'Repeater', 'Window', and 'Help'. Below it is a toolbar with buttons for 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Project options', 'User options', and 'Alerts'. A secondary toolbar shows 'Issue activity', 'Scan queue', 'Live scanning', 'Issue definitions', and 'Options'.

The main table lists scan results:

#	Host	URL	Status	Issues	Requests
1	http://192.168.56.1:8888	/login	finished	3	459

A detailed view of 'Scan item 1' is shown in a pop-up window. It has tabs for 'Issues', 'Base request', and 'Base response'. The 'Issues' tab is active, showing three issues:

- ❗ Cross-site scripting (reflected)
- ? Cross-site request forgery
- i Input returned in response (reflected)

Below the issues, there are tabs for 'Advisory', 'Request', and 'Response'. The 'Request' tab is active, showing the raw HTTP request:

```
POST /login HTTP/1.1
Content-Length: 28
Content-Type: application/x-www-form-urlencoded
Host: 192.168.56.1:8888
Connection: close
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

username=dineshb4ekj%3cscript%3ealert(1)%3c%2fscript%3esipog&password=dkm
```

At the bottom, there's a search bar with a magnifying glass icon, a search term input field, and a '1 highlight' indicator.