

BÀI 1. CÔNG CỤ WEBGOAT, BURP SUITE

I. Công cụ Burp suite

1.1 Mục đích

Cấu hình Burp proxy và tìm hiểu một số tính năng cơ bản.

1.2 Cài đặt Java

Trong trình duyệt web, truy cập trang <https://www.java.com/en/>

Tải về và cài đặt phiên bản Java mới nhất.

1.3 Cài đặt công cụ Burp suite

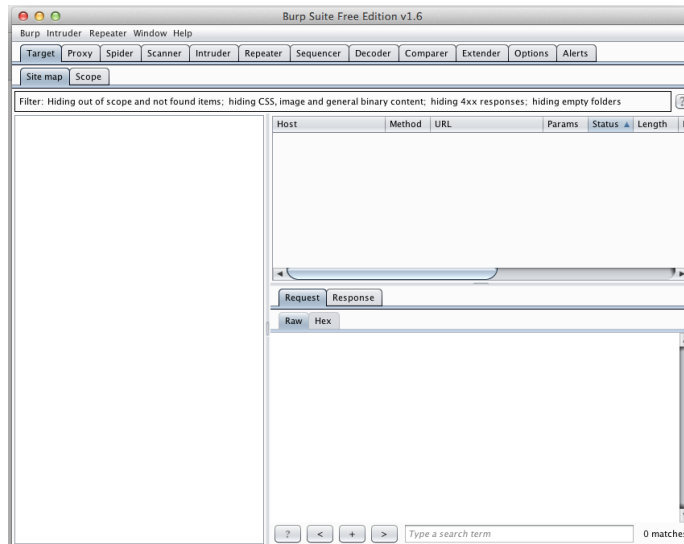
Trong trình duyệt Web, truy cập trang <http://portswigger.net/burp/download.html>

Ở cuối cột "Free Edition", nhấn vào "**Download now**".

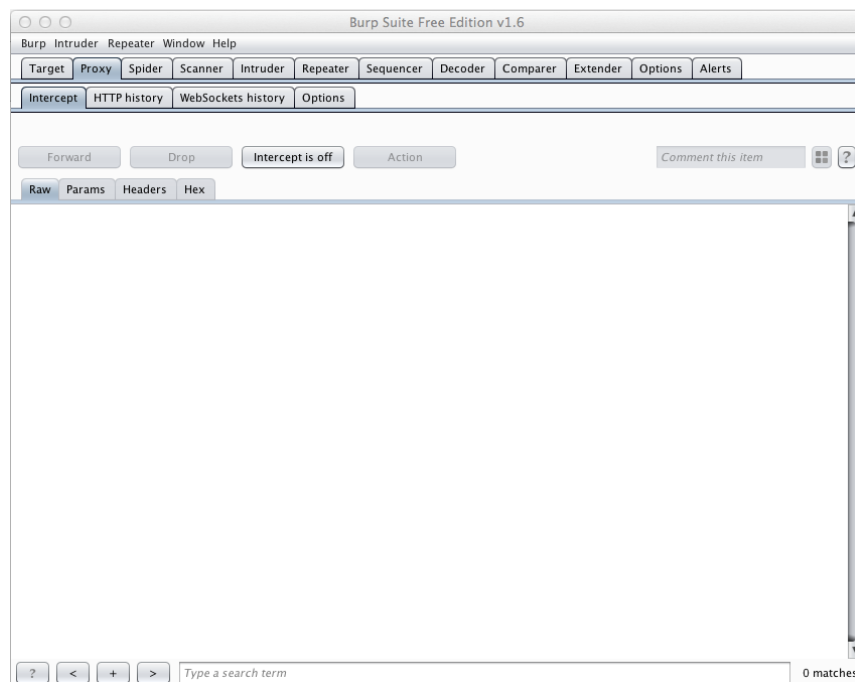
Một tập tin "burpsuite_free_v1.7.03.jar" được tải xuống (có thể có phiên bản mới hơn). Nhấp đúp vào nó để cài đặt.

Trong màn hình đầu tiên, chấp nhận lựa chọn mặc định của "**Temporary project**" và nhấn **Next**. Nhấn tiếp vào "**Start Burp**".

Công cụ Burp suite mở ra, như hình bên dưới.



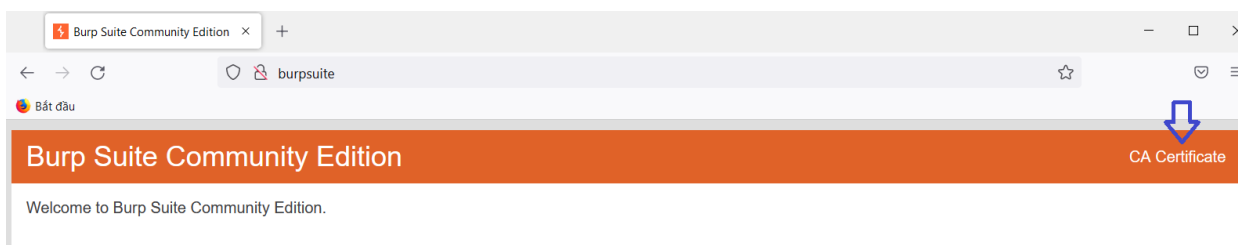
Trong cửa sổ Burp suite, chọn tab **Proxy**. Nhấn vào nút Intercept. Nếu nhấn nút hiển thị "Intercept is on", nhấn vào nhãn đó để hiển thị "**Intercept is off**", như hình dưới đây.



1.4 Điều chỉnh trình duyệt Firefox để sử dụng một Proxy Server

Công cụ Burp suite hoạt động như một máy chủ proxy, bắt lưu lượng Web giữa một trình duyệt đang sử dụng và Internet.

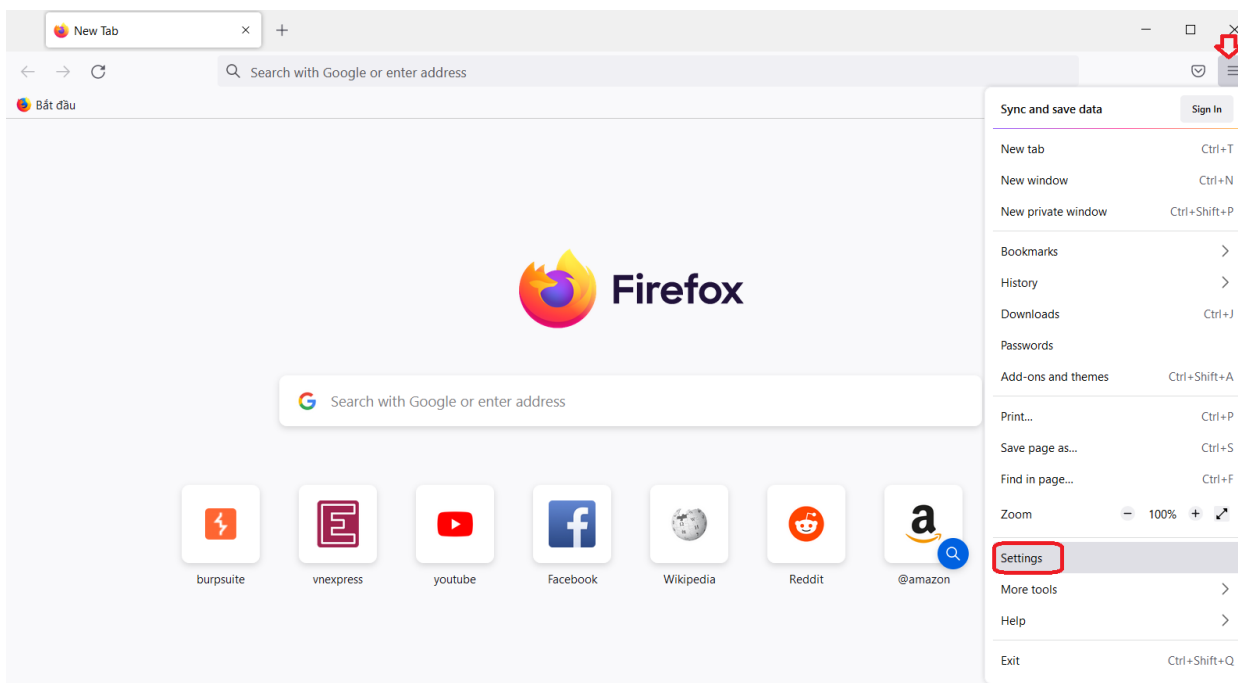
Truy cập địa chỉ: <http://burpsuite>. Tại góc phải phía trên của cửa sổ web, nhấn chọn CA Certificate để tải chứng nhận thiết lập của Burp Suite như hình dưới đây:



Tiếp theo, để sử dụng công cụ Burp suite, cần điều chỉnh cài đặt proxy trên trình duyệt Firefox.

Nếu chưa cài đặt Firefox, nhấn vào link bên dưới để tải: <http://getfirefox.com/>

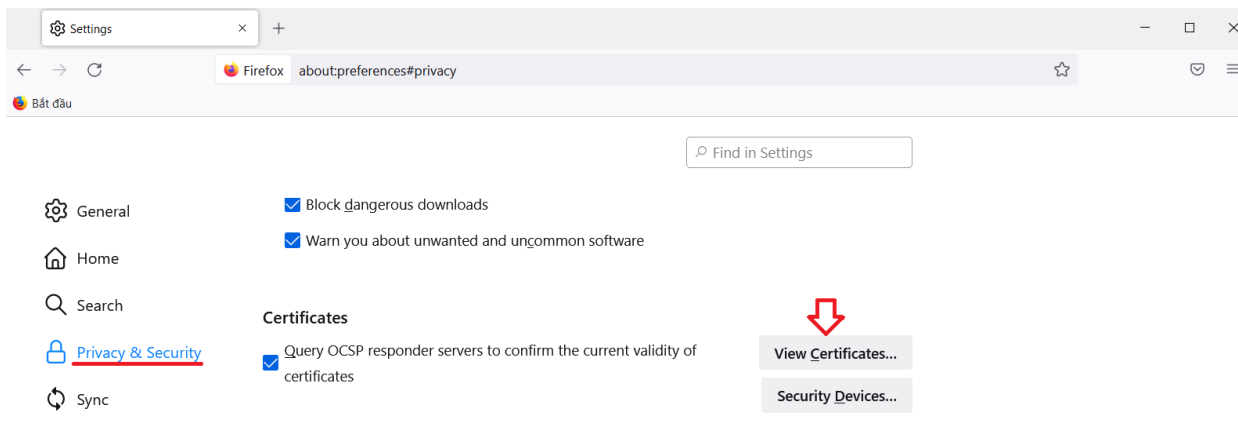
Khi Firefox được cài đặt và khởi động, ở góc trên bên phải, nhấn vào biểu tượng với 3 thanh ngang, như hình dưới đây:



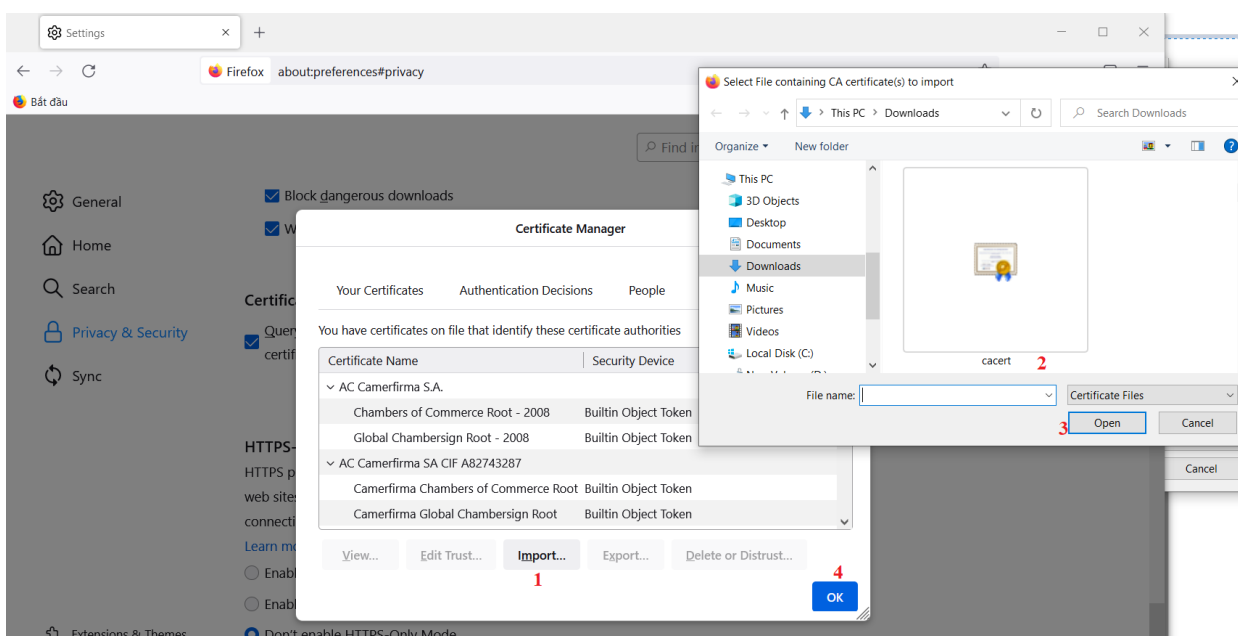
Nhấn chọn **Settings**.

Ở Menu bên trái, nhấn vào **Privacy & Security**.

Trên tab **Certificates**, nhấn vào nút **View Certificates...** như hình dưới đây:



Tại hộp thoại **Certificate Manager**, nhấn vào nút **Import** để thêm tập tin chứng thực của Burp Suite như hình dưới đây:



Ngay tại **Settings**.

Ở phía bên trái, nhấn vào **General**.

Trên tab **Network Settings**, nhấn vào nút **Settings**.

Chọn vào nút "**Manual proxy configuration**" và nhập địa chỉ HTTP Proxy là **localhost** và port **8080**

Đánh dấu check vào ô "**Also use this proxy for HTTPS**", như hình dưới đây:

Connection Settings

×

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy

localhost

Port

8080

☒ Also use this proxy for HTTPS

HTTPS Proxy

localhost

Port

8080

SOCKS Host

Port

0

☐ SOCKS v4

☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

OK

Cancel

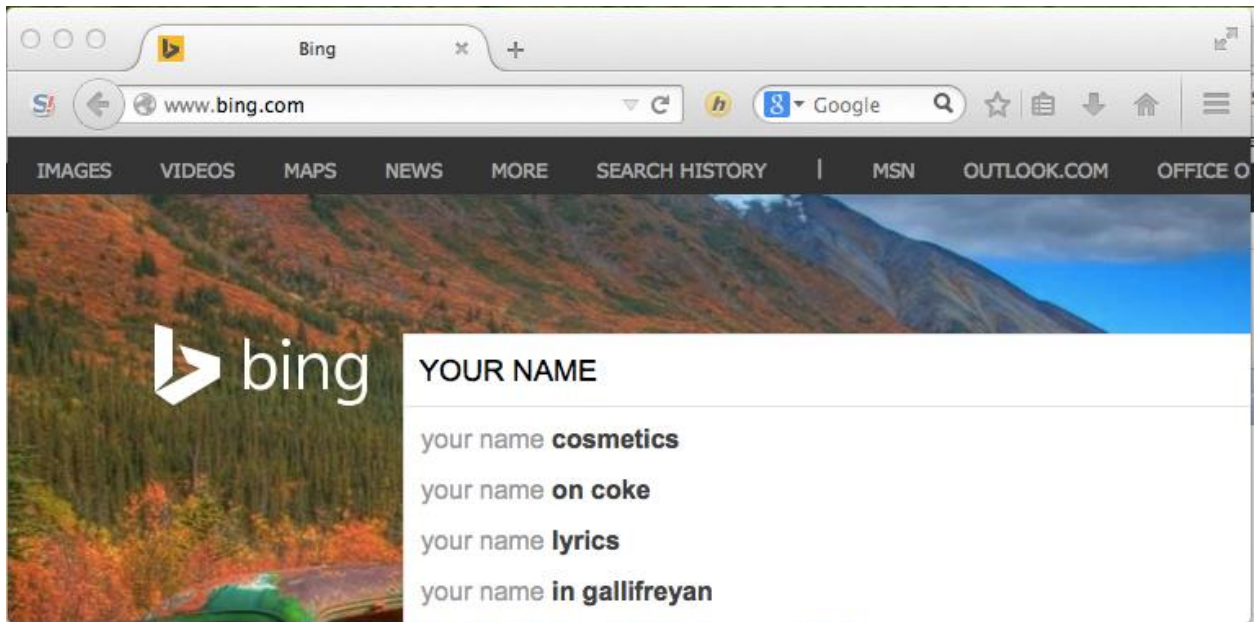
Help

Nhấn **OK**.

1.5 Ngăn chặn tìm kiếm

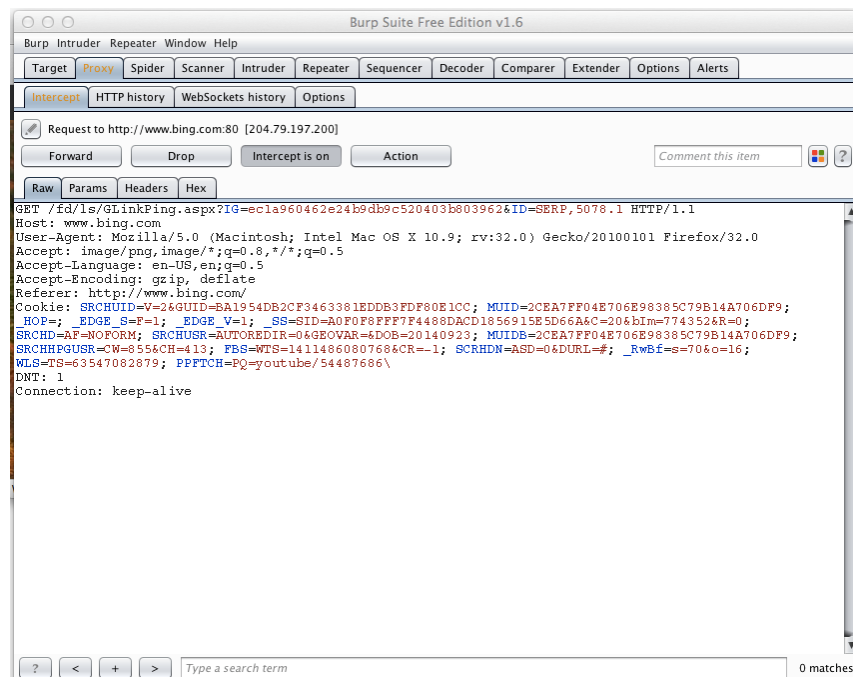
Trong Firefox, đi đến trang [bing.com](https://www.bing.com)

Trên thanh tìm kiếm của trang Bing, nhập YOUR NAME, như hình bên dưới.



Trong công cụ Burp suite, nhấn vào nút **"Intercept is off"**. Nhấn sẽ thay đổi thành **"Intercept is on"**, như hình dưới đây.

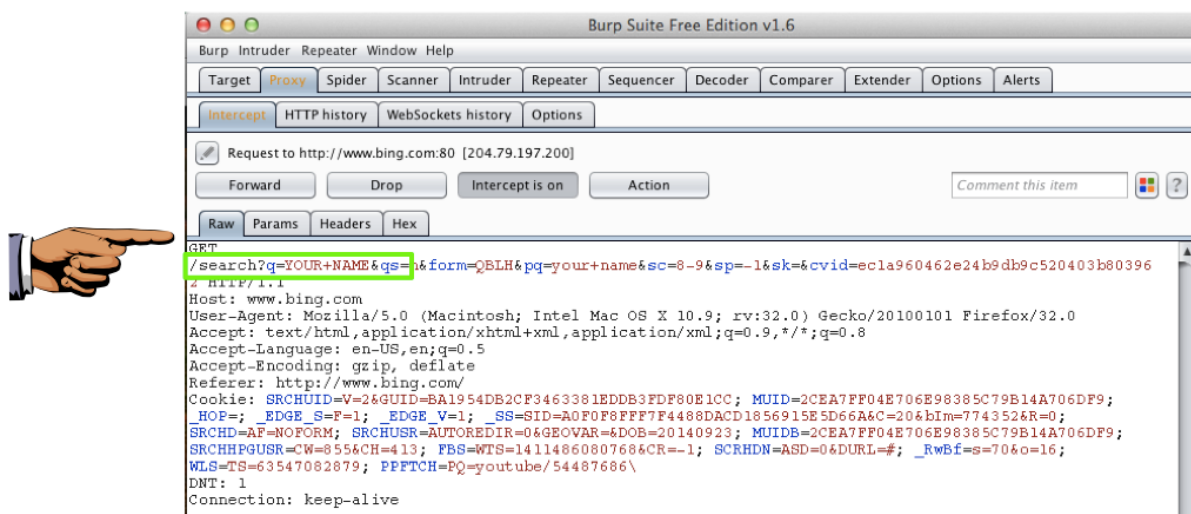
Trong Firefox, ở trang Bing, nhấn Enter. Công cụ Burp suite hiển thị một yêu cầu GET.



Trong công cụ Burp suite, nhấn vào nút **Forward** cho đến khi bạn thấy yêu cầu GET, như hình dưới đây. Khi làm điều đó, nhấn vào nút Forward hai lần,

nhưng nếu có phần mở rộng của trình duyệt, có thể nhấn vào nút đó nhiều lần hơn.

Sẽ nhìn thấy yêu cầu GET với từ YOUR NAME trong đó, như hình dưới đây.



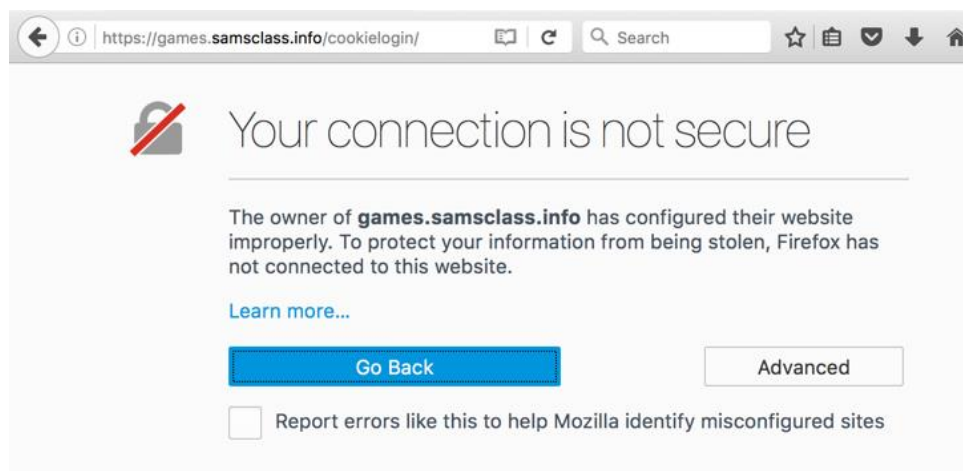
1.6 Cho phép công cụ Bing hoàn thành việc tìm kiếm.

Trong công cụ Burp suite, nhấn vào nút "Intercept is on". Nhấn thay đổi thành "Intercept is off". Điều này cho phép lưu lượng đi qua để công cụ Bing tìm kiếm có thể hoàn thành.

1.7 Ngăn chặn một đăng nhập mã hóa

Trong Firefox, truy cập vào trang <https://games.samsclass.info/cookielogin/>

Một cảnh báo xuất hiện, như hình dưới đây.



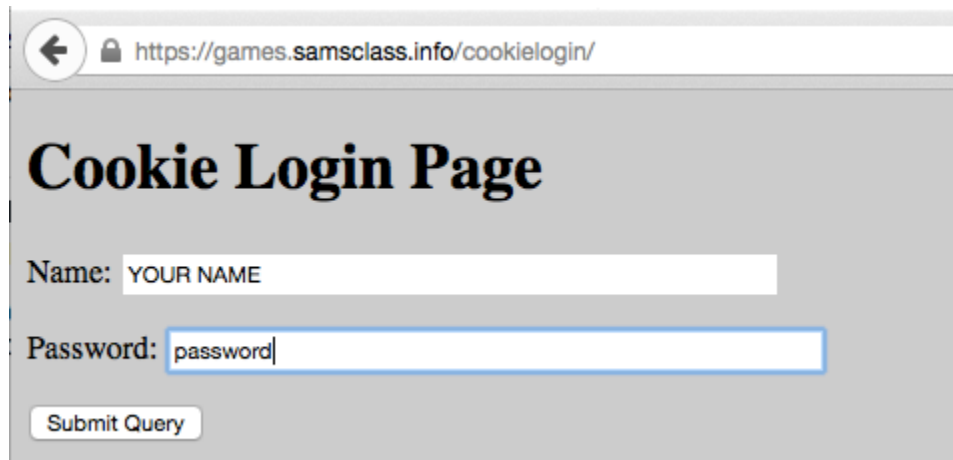
Nhấn vào **Advanced**, "**Add exception**" và "**confirm security exception**".

Những cảnh báo này cho biết rằng kết nối đang bị chặn bởi một bên thứ 3 (công cụ burp suite).

Nếu cảnh báo không xuất hiện, nghĩa là trước đây đã xác nhận ngoại lệ.

Trong trang Cookie Login, nhập YOUR NAME, như hình dưới đây.

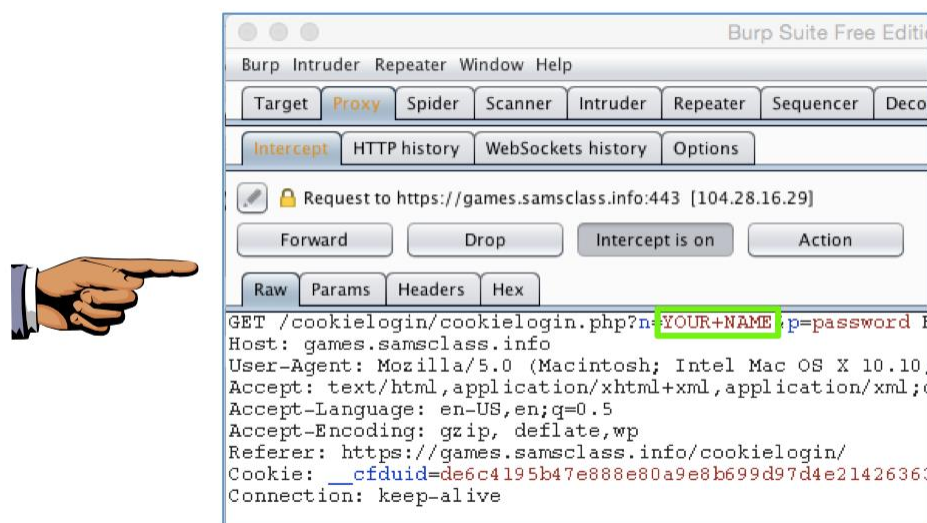
Nhập password của tại trường **password**.



The screenshot shows a web browser window with the address bar displaying `https://games.samsclass.info/cookielogin/`. The page title is "Cookie Login Page". It features two input fields: "Name:" with the placeholder text "YOUR NAME" and "Password:" with the placeholder text "password". Below the fields is a button labeled "Submit Query".

Trong công cụ Burp suite, nhấn vào nút "**Intercept is off**". Nhấn sẽ thay đổi thành "**Intercept is on**".

Trong Firefox, ở trang Cookie Login, nhấn vào nút "**Submit Query**". Công cụ Burp suite hiển thị yêu cầu Get, như hình dưới đây:



Lưu ý rằng từ YOUR NAME xuất hiện trong yêu cầu này, mặc dù nó được mã hóa.

Đó là bởi vì công cụ Burp suite thực hiện một tấn công man-in-the-middle, hoạt động như một tổ chức phát hành chứng chỉ, cung cấp một khóa công khai giả thay vì khóa chính thức.

Trình duyệt đã cảnh báo về sự cố này, nhưng khi thêm ngoại lệ an toàn, chúng ta đã yêu cầu nó tiếp tục tiến hành.

1.8 Cho phép đăng nhập

Trong công cụ Burp suite, nhấn vào nút **"Intercept is on"**. Nhấn thay đổi thành **"Intercept is off"**. Điều này cho phép đăng nhập.

Username và password bị từ chối. Điều đó hoàn toàn chính xác.

1.9 Sử dụng Site Map trong công cụ Burp suite

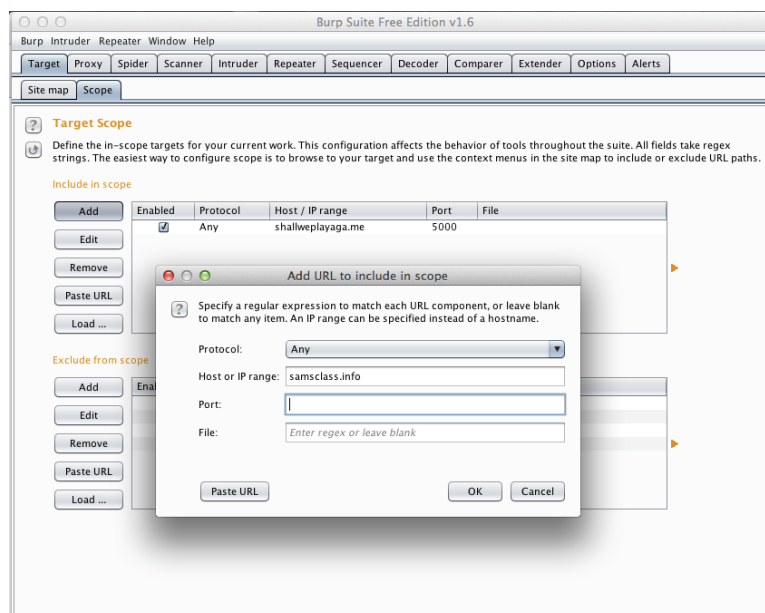
Site Map hiển thị tất cả tên miền phụ, thư mục và các trang được liên kết bởi một trang Web. Điều này rất hữu ích cho thử nghiệm thâm nhập và kiểm tra toán viên an ninh, do đó họ có thể tìm tất cả các vấn đề an ninh tiềm ẩn trong một trang Web.

Trong công cụ Burp suite, nhấn vào tab **Target**.

Trong tập hợp các tab thấp hơn, nhấn vào tab **Scope**.

Trong phần "include in scope", nhấn vào nút **Add**.

Trong hộp thoại xuất hiện "Add URL to include in scope", trong trường "Host or IP range", nhập vào **samsclass.info** như hình dưới đây.



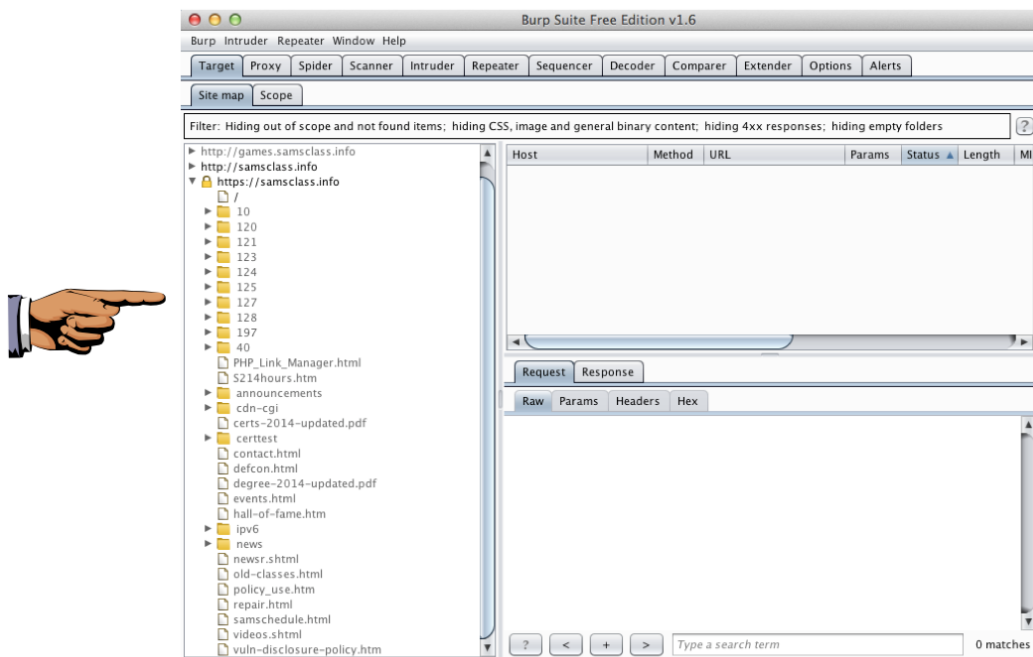
Nhấn **OK**.

Trong công cụ Burp suite, nhấn vào tab **"Site map"**.

Trong Firefox, truy cập <https://samsclass.info/>

Nếu Firefox hiển thị một thông báo "This Connection is Untrusted", nhấn vào **Advanced**, **"Add exception"**, và **"Confirm security exception"**.

Công cụ Burp suite hiển thị tên miền **samsclass.info**, như hình dưới đây.



Mở rộng phần `https://samsclass.info`, như hình phía trên. Tất cả các tập tin và thư mục đều hiển thị, giúp dễ dàng tìm kiếm các mục thú vị và các lỗ hổng bảo mật.

II. Xác định cấu trúc trang web sử dụng công cụ Burp suite

2.1 Yêu cầu

Java và công cụ Burp suite đã được cài đặt.

Một trình duyệt Web được cấu hình để sử dụng Burp Proxy, như đã thiết lập trong lab trước đó.

2.2 Mục đích

Sử dụng các kỹ thuật khác nhau để xác định cấu trúc trang Hackazon.

2.3 Khởi động công cụ Burp suite

Khởi động công cụ Burp suite. Chấp nhận lựa chọn mặc định "Temporary Project" và nhấn Next.

Chấp nhận lựa chọn mặc định của "Use Burp Defaults" và nhấn vào "Start Burp".

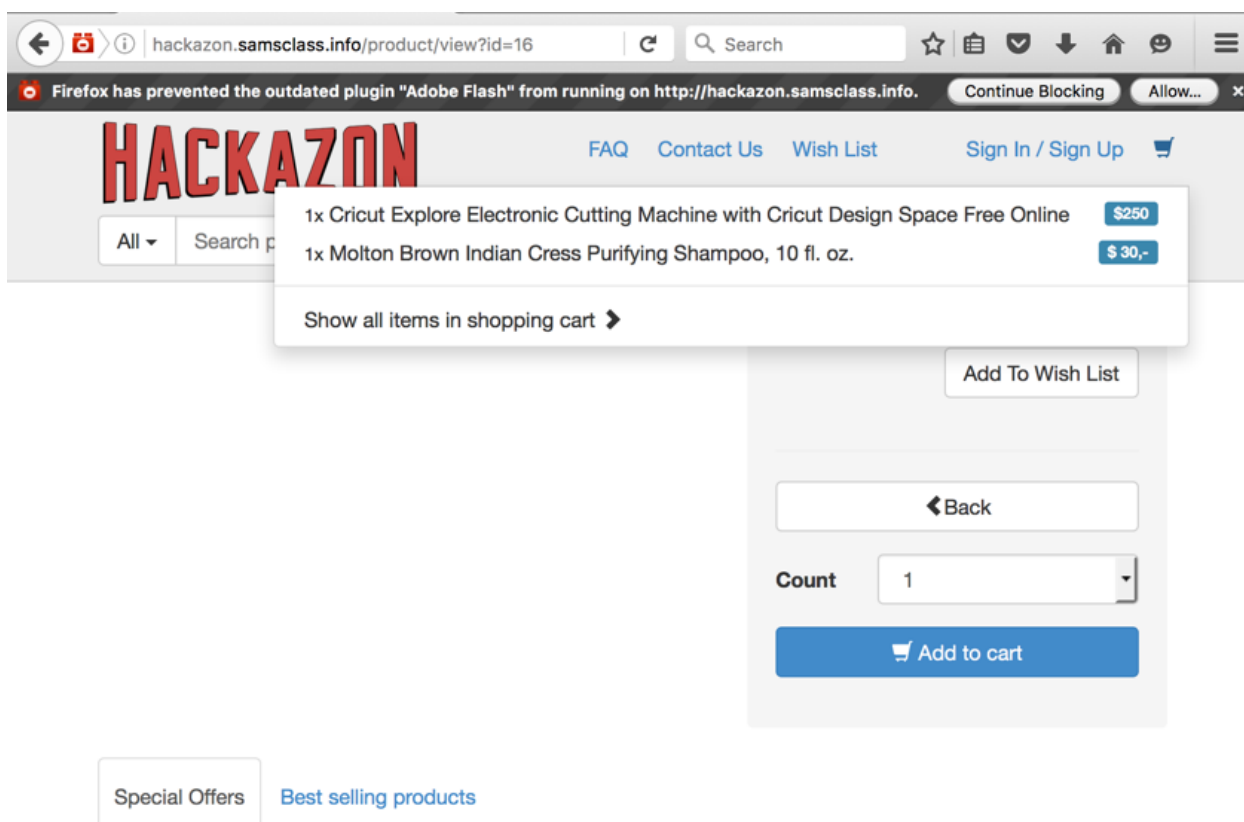
Trong chương trình Burp suite, trên tab Proxy, nhấn vào nút "Intercept is on" để chuyển thành "Intercept is off".

2.4 Truy cập trang hackazon

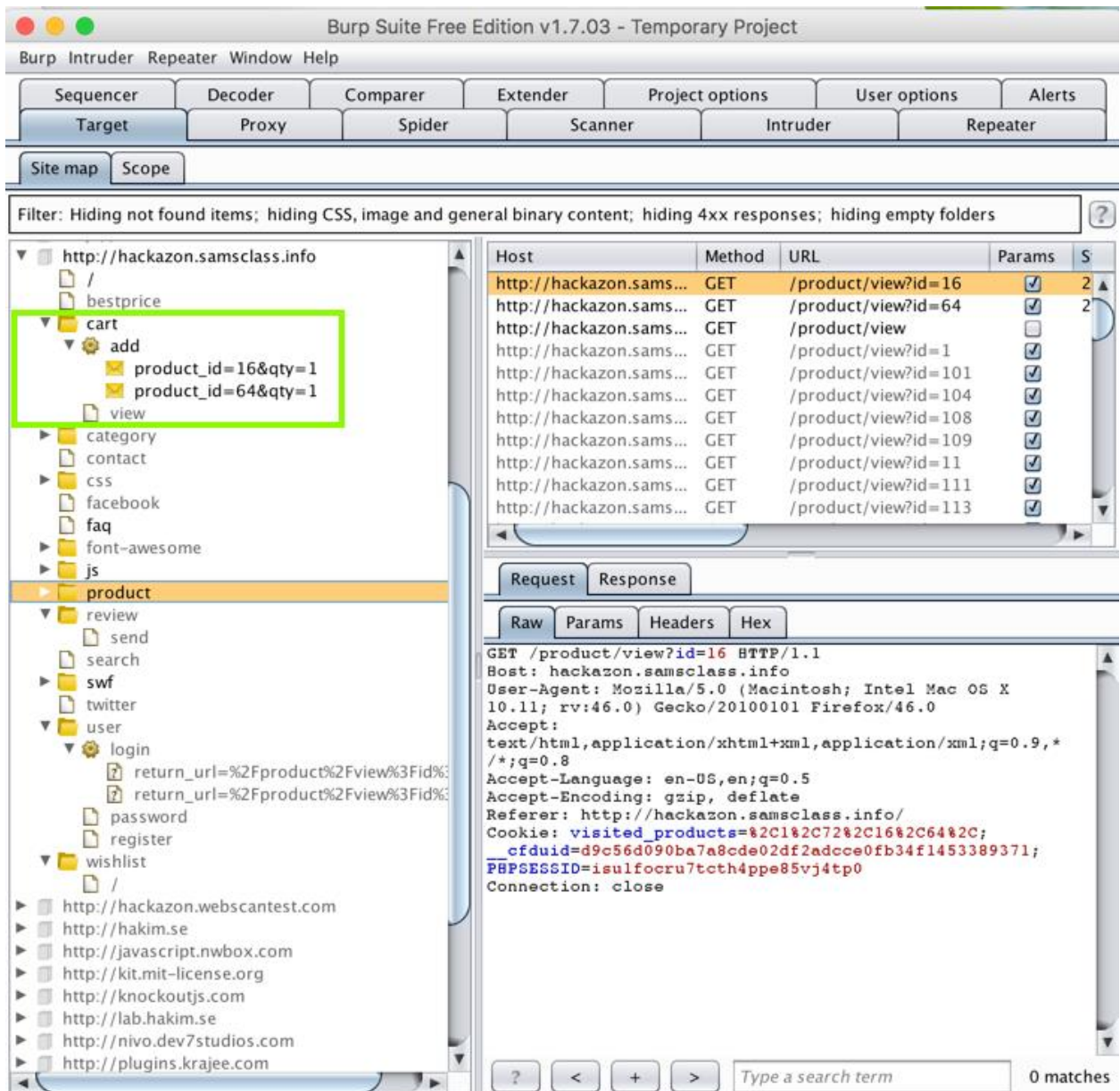
Trong trình duyệt được cấu hình để sử dụng công cụ Burp suite, truy cập trang hackazon.samsclass.info.

Đảm bảo rằng thấy link "Sign In/Sign Up" ở phía trên bên phải của trang Hackazon, như hình dưới đây. Nếu không thấy, nhấn vào Logout để đăng xuất.

Nhấp vào bất kỳ mặt hàng nào và thêm vào giỏ hàng của bạn.



Trong chương trình Burp suite, trên tab "Site map", mở rộng http://hackazon.samsclass.info. Mở rộng cart và add. Bạn sẽ nhìn thấy 2 mặt hàng của mình, như được phát họa màu xanh lá cây trong hình dưới đây.

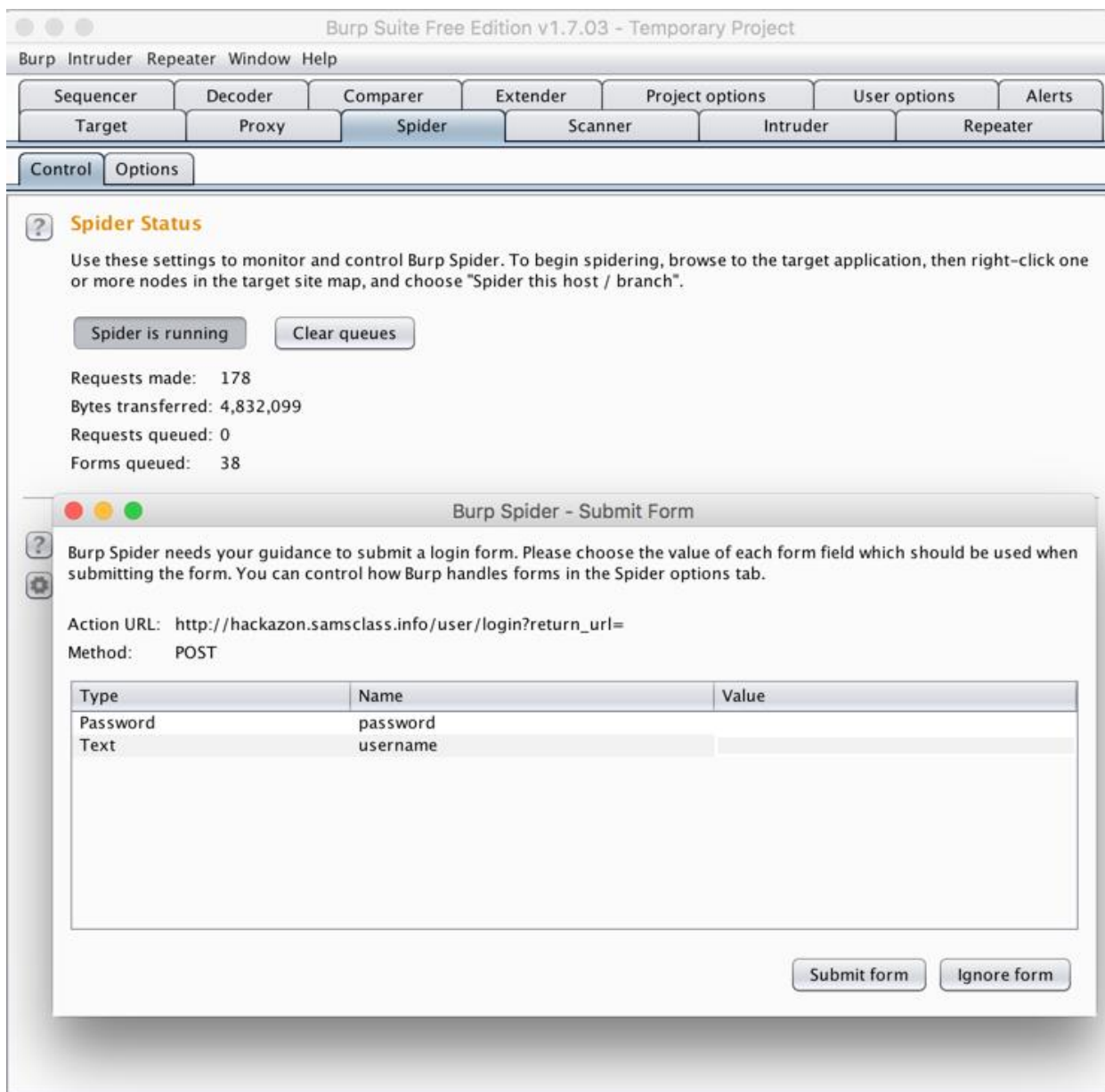


2.5 Tự động duyệt trang hackazon và xác định cấu trúc

Trong chương trình Burp suite, trên tab "Site map", nhấn chuột phải vào <http://hackazon.samsclass.info> và nhấn vào "Spider this host".

Nếu một hộp thoại xuất hiện thông báo "... Would you like to modify the scope to include these items?", nhấn vào Yes.

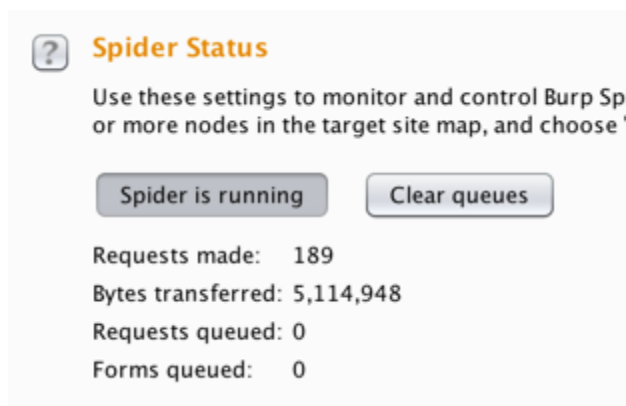
Trong chương trình Burp suite, nhấn vào tab Spider. Sau một vài giây, công cụ Burp suite tìm thấy một số form và một hộp thoại xuất hiện hỏi bạn có thể kiểm soát cách burp xử lý form trong tab tùy chọn Spider.



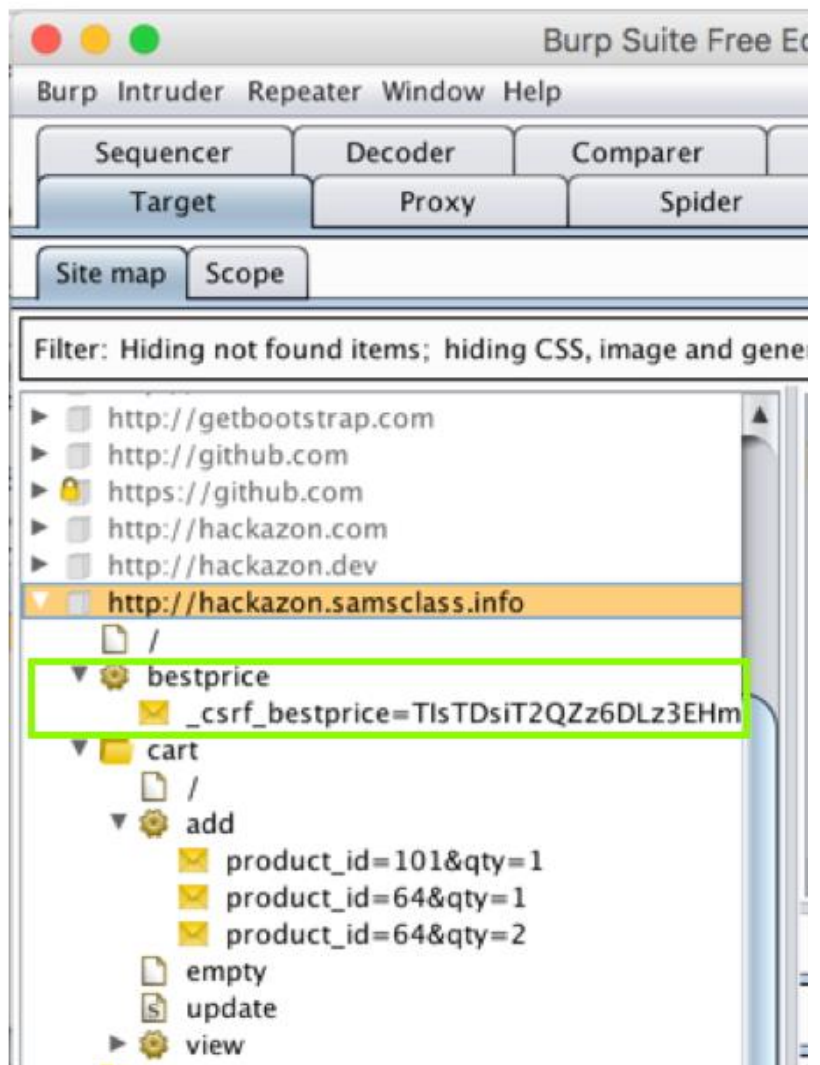
Nhấn vào "Ignore this form" trong hộp thoại này và tắt cả các hộp thoại xuất hiện khác. Chúng xuất hiện rất nhiều, có thể 15 lần.

Spider nên kết thúc trong vòng vài giây. Có thể nói nó được thực hiện bởi vì các giá trị yêu cầu xếp hàng đợi "Request queued" và form xếp hàng đợi "Forms queued" là 0, như hình dưới đây.

Nhấn vào nút "Spider is running" để dừng spidering.

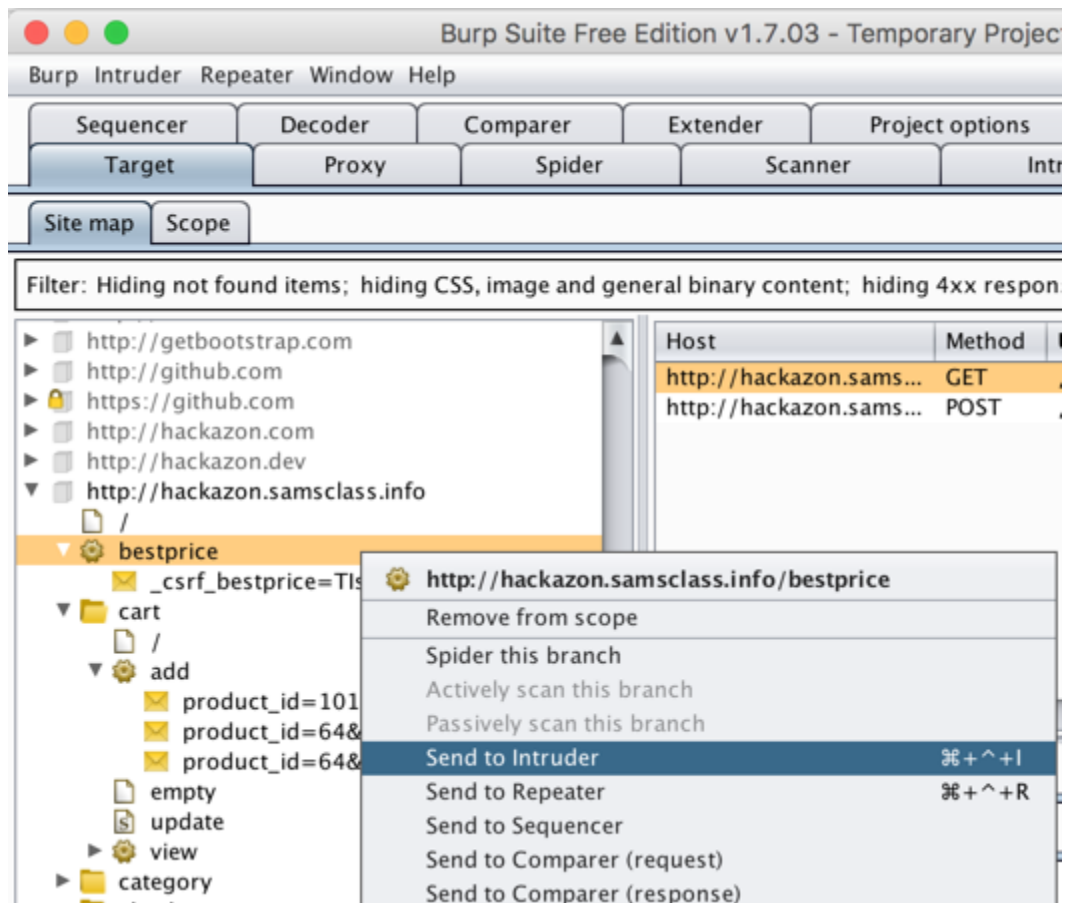


Trong phần mềm Burp suite, trên tab Target, trong tab phụ "Site map", mở rộng bestprice. Sẽ thấy một mặt hàng bắt đầu với _csrf_bestprice, như hình bên dưới. Đây là một phần của ứng dụng mà spider tìm thấy.

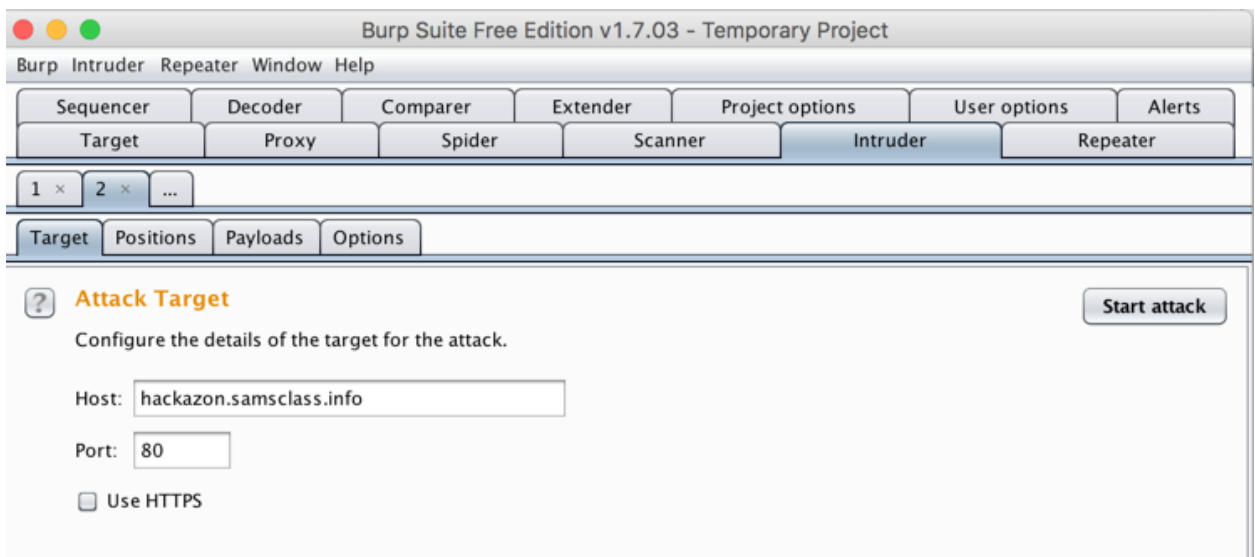


2.6 Sử dụng Burp Intruder để thực hiện tấn công brute force tìm kiếm thư mục

Trong chương trình Burp suite, trên tab Target, trong tab phụ "Site map", nhấn chuột phải vào bestprice. Trong menu ngữ cảnh, nhấn vào "Send to Intruder", như hình bên dưới.

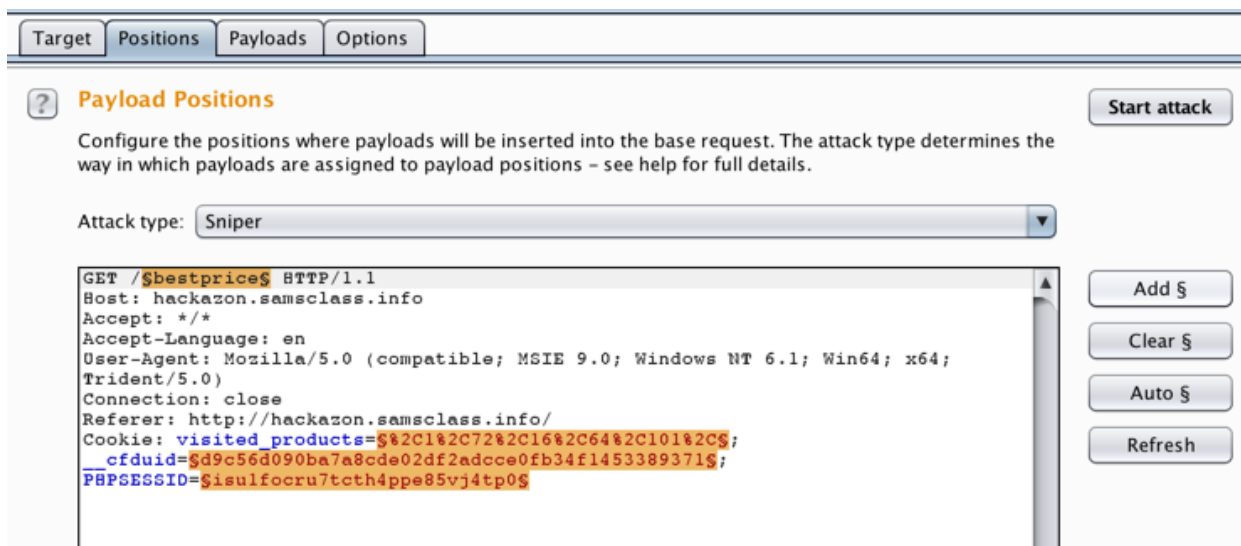


Trong chương trình Burp suite, nhấn vào tab Intruder. Trên tab phụ Target, Host: phải là "hackazon.samsclass.info", như hình dưới đây.

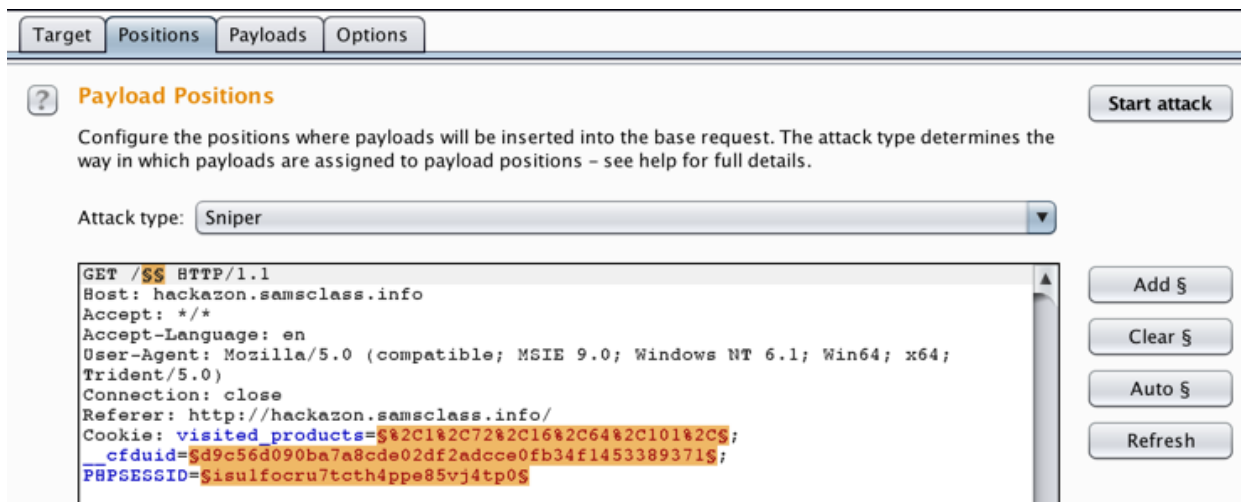


Nhấn vào tab phụ Positions. Trong dòng GET, nhấp đúp vào bestprice để đánh dấu nó. Ở phía bên phải, nhấn vào nút "Add §". Những "section marks" này chỉ ra nơi mà Burp Intruder sẽ chèn từ.

Màn hình trông giống như hình dưới đây.



Cẩn thận xóa từ bestprice, giữa các dấu \$, như hình dưới đây.



Nhấn vào nút "Start attack".

Một lỗi xuất hiện thông báo "Preset payload list is empty". Nhấn vào nút "Go back".

Trong chương trình Burp, nhấn vào tab phụ Payloads. Không có danh sách từ wordlists nào trong phiên bản miễn phí của Burp.

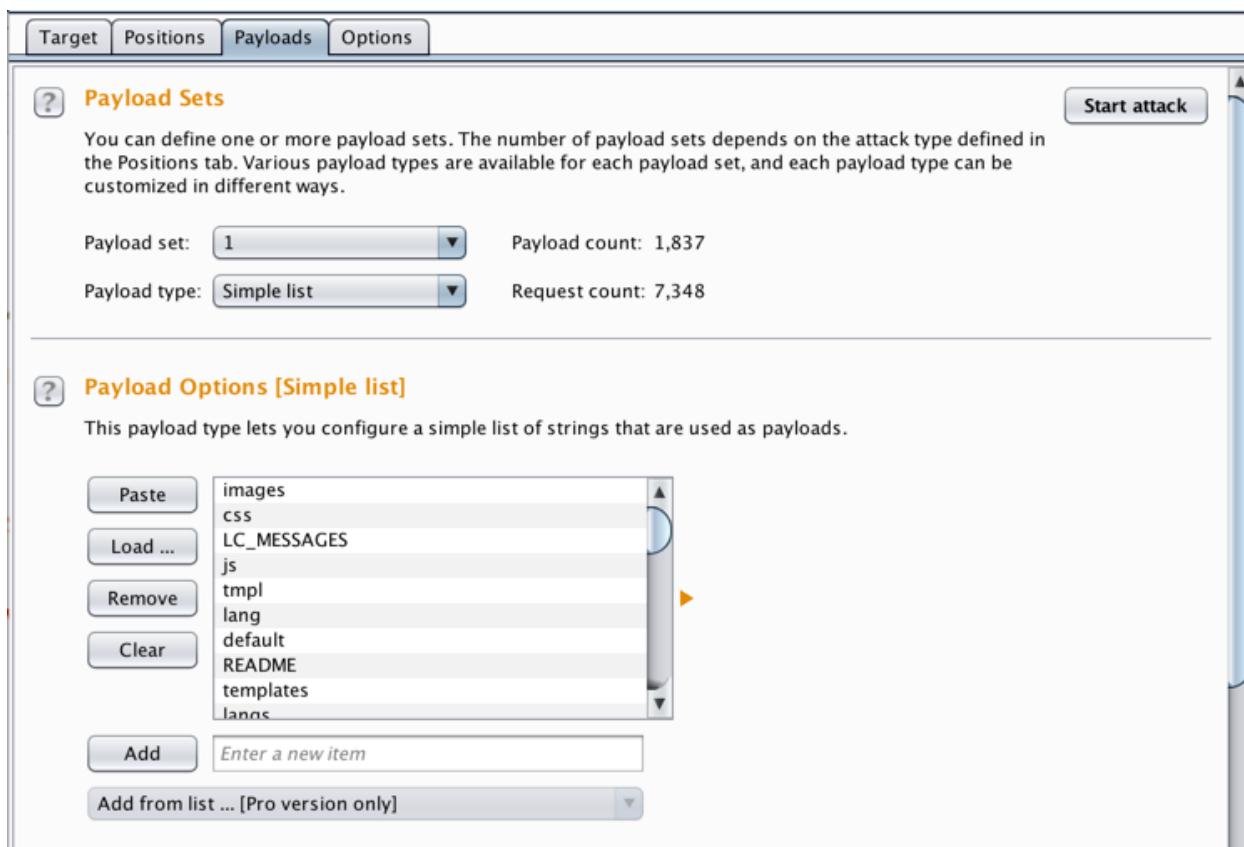
Nhấn chuột phải vào link bên dưới và lưu tập tin trên máy tính. Đây là danh sách tên thư mục nhận được từ trang được liệt kê trong phần Sources ở phần cuối của lab này.

[Directories_Common.wordlist](#)

Trong chương trình Burp suite, trong "Payload Options (Simple List)", nhấn vào nút Load...

Duyệt tới tập tin "Directories_Common.wordlist" trên máy tính và nhấp đúp vào nó.

Danh sách từ liệt kê, như hình dưới đây.



Nhấn vào nút "Start attack"

Một thông điệp cảnh báo rằng cuộc tấn công này bị hạn chế trong phiên bản miễn phí của Burp suite. Nhấn OK.

Một hộp thoại xuất hiện cho thấy cuộc tấn công đang diễn ra, như hình dưới đây. Nó rất chậm, nhưng nó hiển thị mã phản hồi HTTP cho mỗi yêu cầu.



Intruder attack 1						
Attack Save Columns						
Results Target Positions Payloads Options						
Filter: Showing all items						
Request	Position	Payload	Status	Error	Timeout	Length
0			200	<input type="checkbox"/>	<input type="checkbox"/>	74451
1	1	images	301	<input type="checkbox"/>	<input type="checkbox"/>	585
2	1	css	301	<input type="checkbox"/>	<input type="checkbox"/>	573
3	1	LC_MESSAGES	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
4	1	js	301	<input type="checkbox"/>	<input type="checkbox"/>	569
5	1	tmpl	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
6	1	lang	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
7	1	default	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
8	1	README	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
9	1	templates	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
10	1	langs	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
11	1	config	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
12	1	GNUmakefile	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
13	1	themes	404	<input type="checkbox"/>	<input type="checkbox"/>	22232
14	1	en	404	<input type="checkbox"/>	<input type="checkbox"/>	22232

26 of 7348

Trong cửa sổ "Intruder: attack 1", nhấn Attack, Pause. Khi cuộc tấn công tạm dừng đóng cửa sổ "Intruder: attack 1".

Yêu cầu

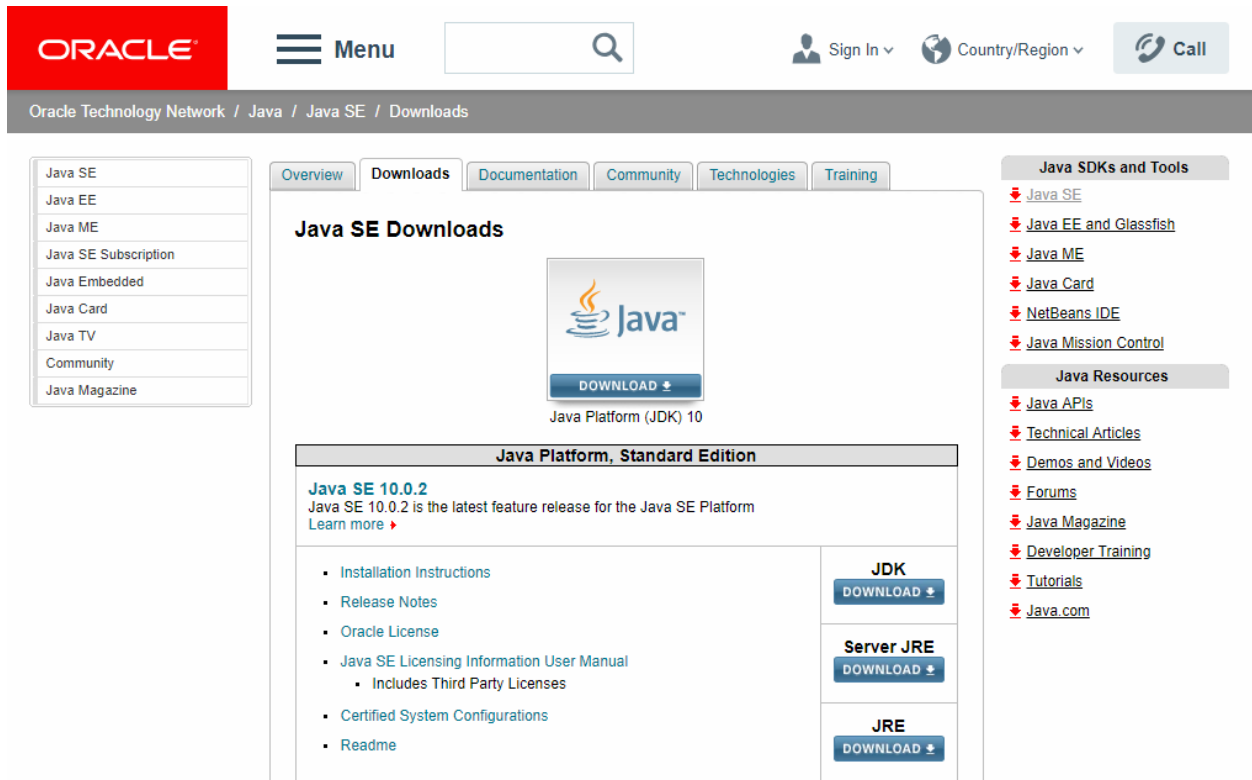
Máy Windows 7, 8 hoặc 10.

Mục đích

Giới thiệu công cụ WebGoat và hiểu cách HTTP request và responses hoạt động.

Cài đặt Java JDK

Mở một trình duyệt Web và truy cập <http://www.oracle.com/technetwork/java/javase/downloads/index.html> tải bản JDK mới nhất. Hiện tại là (10.0.2)



Cài đặt WebGoat

Mở trình duyệt Web và truy cập <https://github.com/WebGoat/WebGoat/releases>

Phiên bản hiện tại là v8.0.0.M21 ([webgoat-server-8.0.0.M21.jar](#))

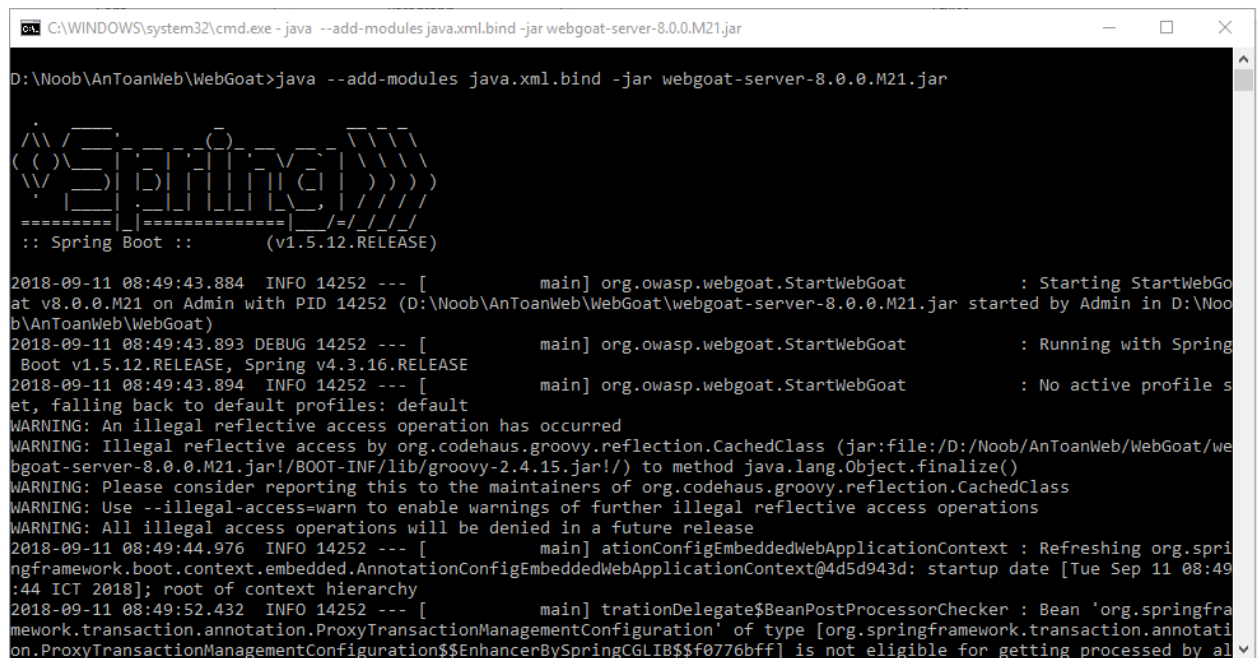
Mở cửa sổ Command Prompt hoặc Terminal truy cập vào thư mục chứa file [webgoat-server-8.0.0.M21.jar](#) và thực hiện các lệnh dưới đây.

```
java -jar webgoat-server-8.0.0.M21.jar [--server.port=8080] [--server.address=localhost]
```

Nếu bạn sử dụng phiên bản java từ 9 trở lên thì thực hiện lệnh sau :

```
Java --add-modules java.xml.bind -jar webgoat-server-8.0.0.M21.jar
```

Ở đây mình dùng lệnh dưới vì phiên bản java đang dùng là 10.0.2



```
C:\WINDOWS\system32\cmd.exe - java --add-modules java.xml.bind -jar webgoat-server-8.0.0.M21.jar

D:\Noob\AnToanWeb\WebGoat>java --add-modules java.xml.bind -jar webgoat-server-8.0.0.M21.jar

:: Spring Boot :: (v1.5.12.RELEASE)

2018-09-11 08:49:43.884 INFO 14252 --- [main] org.owasp.webgoat.StartWebGoat : Starting StartWebGoat
at v8.0.0.M21 on Admin with PID 14252 (D:\Noob\AnToanWeb\WebGoat\webgoat-server-8.0.0.M21.jar started by Admin in D:\Noob\AnToanWeb\WebGoat)
2018-09-11 08:49:43.893 DEBUG 14252 --- [main] org.owasp.webgoat.StartWebGoat : Running with Spring
Boot v1.5.12.RELEASE, Spring v4.3.16.RELEASE
2018-09-11 08:49:43.894 INFO 14252 --- [main] org.owasp.webgoat.StartWebGoat : No active profile s
et, falling back to default profiles: default
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by org.codehaus.groovy.reflection.CachedClass (jar:file:/D:/Noob/AnToanWeb/WebGoat/webgoat-server-8.0.0.M21.jar!/BOOT-INF/lib/groovy-2.4.15.jar!/) to method java.lang.Object.finalize()
WARNING: Please consider reporting this to the maintainers of org.codehaus.groovy.reflection.CachedClass
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
2018-09-11 08:49:44.976 INFO 14252 --- [main] ationConfigEmbeddedWebApplicationContext : Refreshing org.spr
ingframework.boot.context.embedded.AnnotationConfigEmbeddedWebApplicationContext@4d5d943d: startup date [Tue Sep 11 08:49
:44 ICT 2018]; root of context hierarchy
2018-09-11 08:49:52.432 INFO 14252 --- [main] trationDelegate$BeanPostProcessorChecker : Bean 'org.springfra
mework.transaction.annotation.ProxyTransactionManagementConfiguration' of type [org.springframework.transaction.annotati
on.ProxyTransactionManagementConfiguration$$EnhancerBySpringCGLIB$$f0776bff] is not eligible for getting processed by al
```

Giữ cửa sổ terminal không được tắt

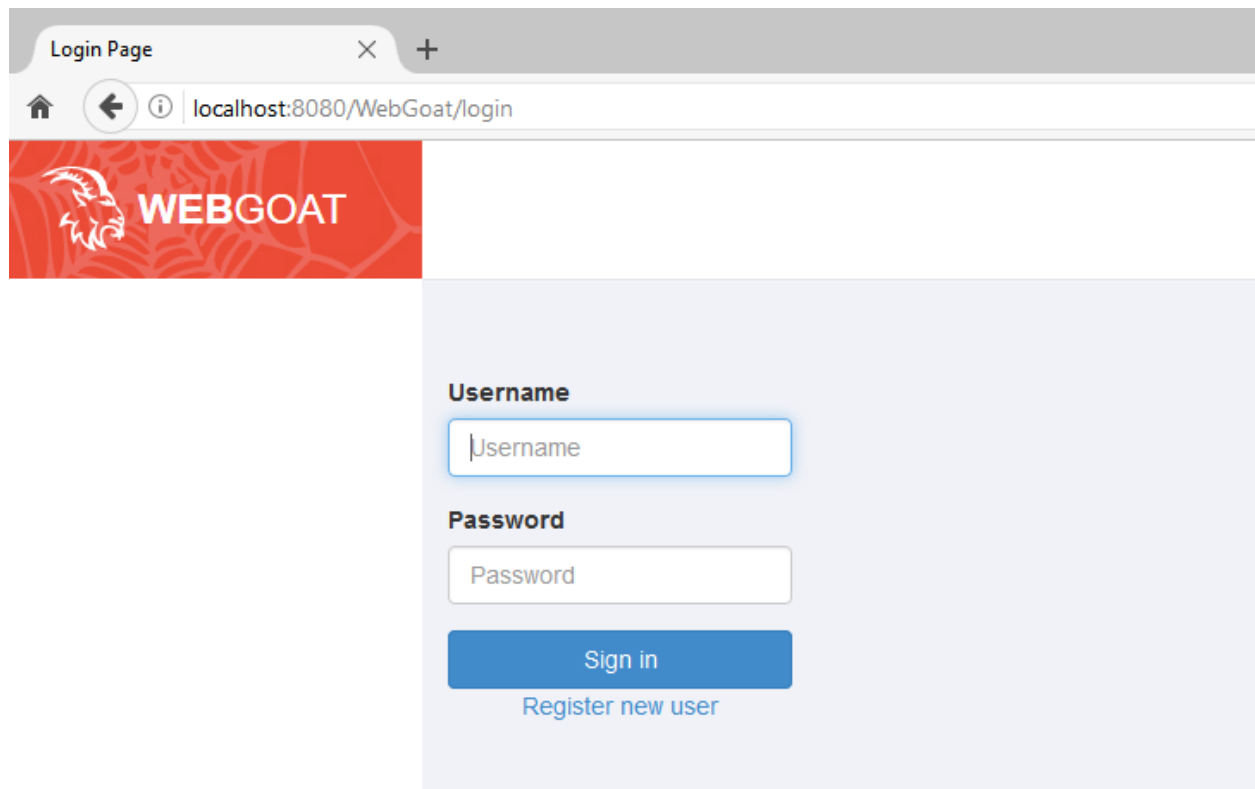
Khởi động Firefox

Nếu không có Firefox, hãy tải tại đây: <http://getfirefox.com>

Đăng nhập vào WebGoat

Trong Firefox, truy cập <http://localhost:8080/WebGoat>

Xuất hiện màn hình đăng nhập, như hình dưới đây.



Tạo một tài khoản đăng nhập mới

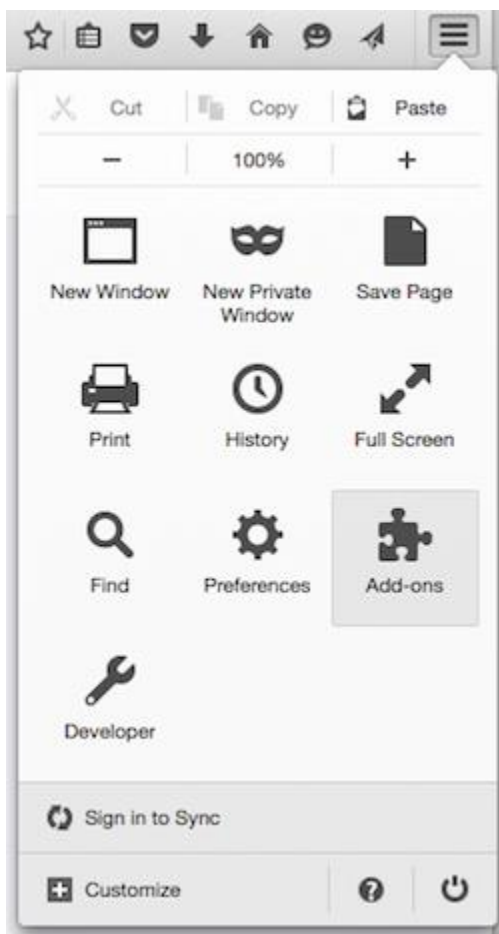
Register

Username	<input type="text" value="guest1"/>
Password	<input type="password" value="....."/>
Confirm password	<input type="password" value="..... "/>
Terms of use	<div><p>While running this program your machine will be extremely vulnerable to attack. You should disconnect from the Internet while using this program. WebGoat's default configuration binds to localhost to minimize the exposure.</p><p>This program is for educational purposes only. If you attempt these techniques without authorization, you are very likely to get caught. If you are caught engaging in unauthorized hacking, most companies will fire you. Claiming that you were doing security research will not work as that is the first thing that all hackers claim.</p></div>

☐ Agree with the terms and conditions

Cài đặt Tamper Data

Trong Firefox, ở trên cùng bên phải, nhấn vào biểu tượng ba thanh ngang.
Nhấn vào tiện ích **Add-ons**.



Trong trang trình quản lý tiện ích “Add-ons Manager”, tìm kiếm “**tamper data**”, như hình dưới đây.

Trong dòng “Tamper Data”, nhấn vào nút **Install**.

Một hộp thoại bật lên. Nhấn vào nút “**Accept and Install**”.



Tamper Data

Use tamperdata to view and modify HTTP/HTTPS headers and post parameters...

Adam Judson

Nếu install không được và nhận được thông báo là không tương thích với phiên bản Firefox hiện tại thì Install add-on **Disable Add-on Compatibility Checks** để tắt tính năng kiểm tra add-on khi cài đặt trên Firefox



Disable Add-on Compatibility Checks

by Kris Maglione

Not compatible with Firefox Quantum

Reinstates the extensions.checkCompatibility preference without respect to the current application version.

+ Add to Firefox

Sau đó cài lại Tamper data

Đóng Firefox và restart lại nó.

Trong Firefox, truy cập

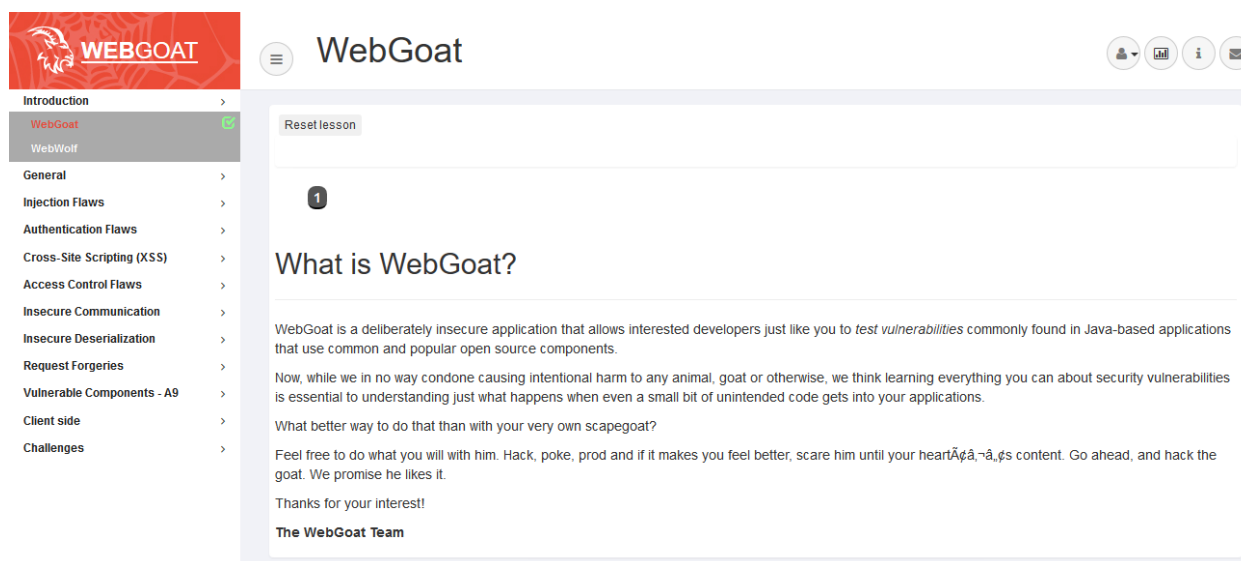
<http://localhost:8080/WebGoat>

Đăng nhập với username **guest** và mật khẩu **guest**.

a. Giới thiệu WebGoat

Ở phía bên trái cửa sổ WebGoat, nhấn vào giới thiệu **Introduction**.

Trong phần giới thiệu Introduction, nhấn vào "**WebGoat**", như hình dưới đây.



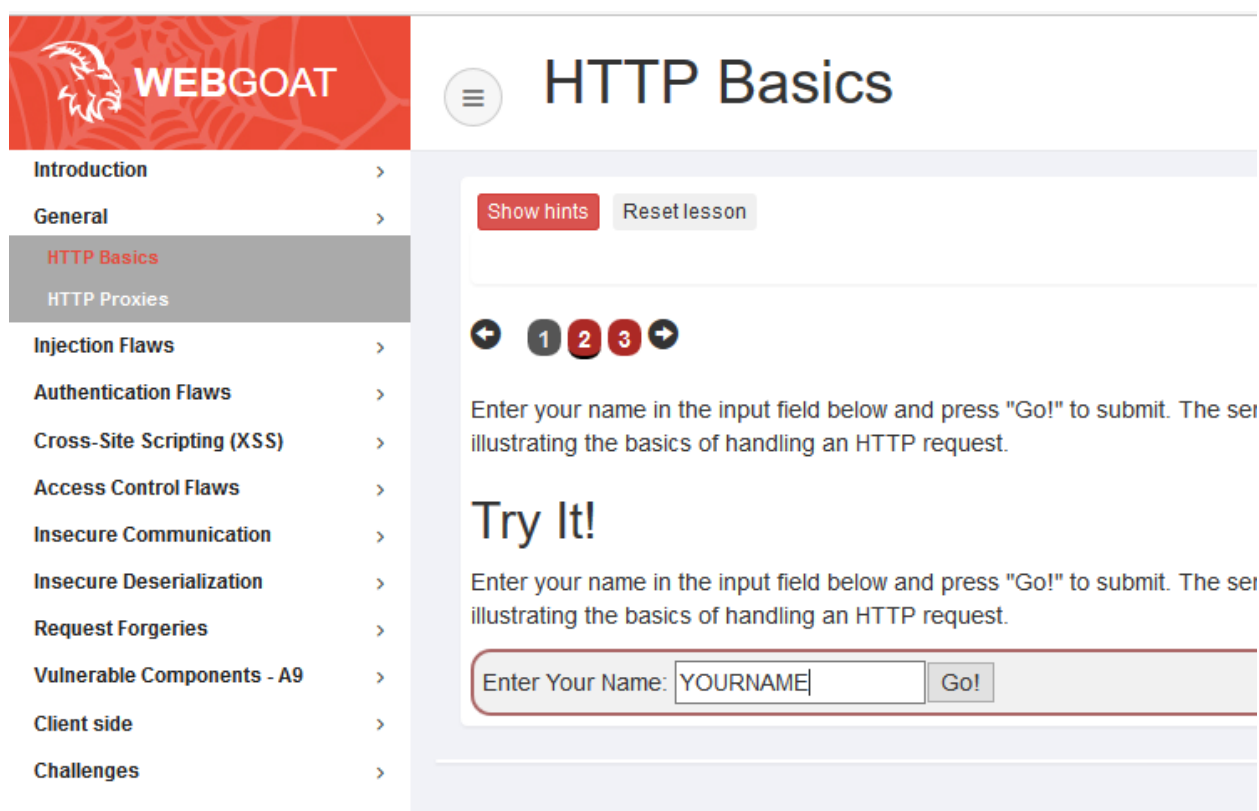
b. Http basics trong WebGoat

Mục đích của bài học này là tìm hiểu cách HTTP request và responses hoạt động.

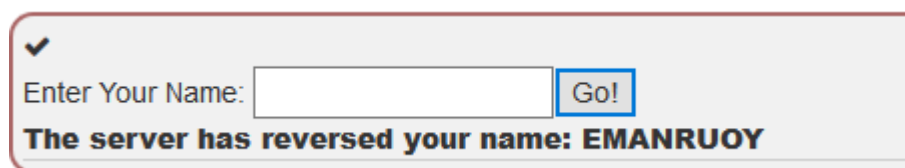
Ở phía bên trái của cửa sổ WebGoat, nhấn vào **General**.

Trong phần General, nhấn vào "**Http Basics**" Qua trang 2.

Nhập tên của bạn vào ô "Enter your name" và nhấn vào **Go!**, như hình dưới đây.



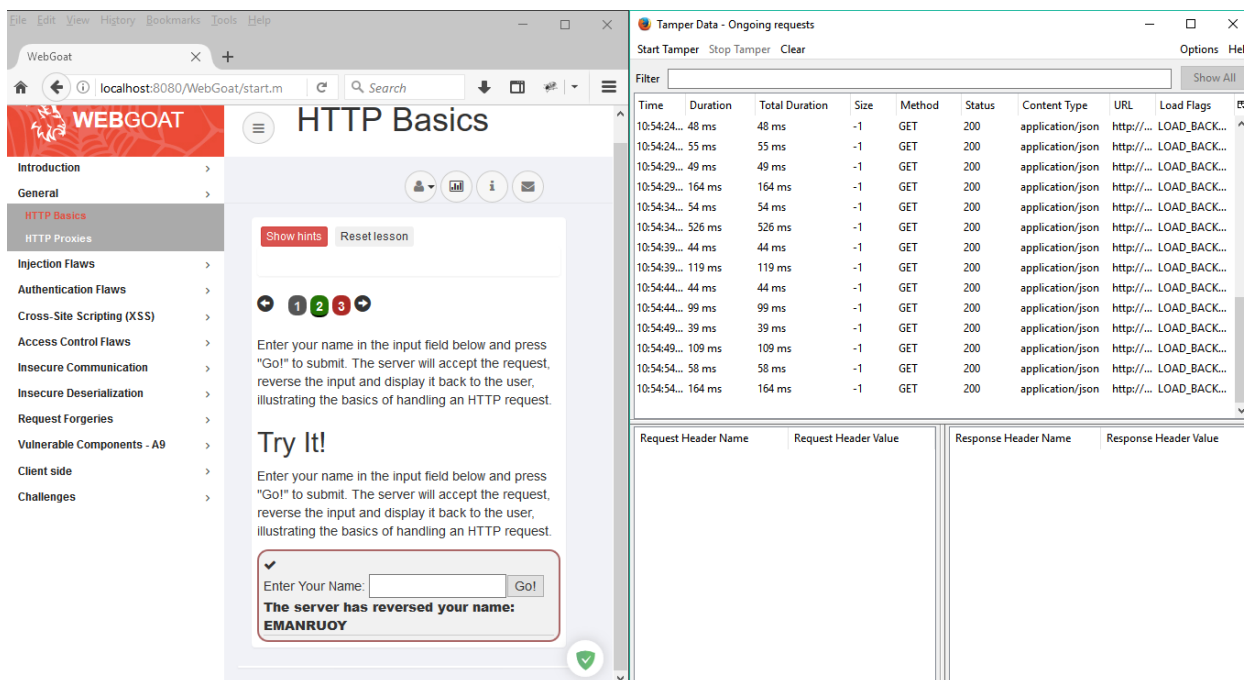
Thứ tự các chữ cái tên của bạn bị đảo ngược, như hình dưới đây.



Bây giờ chúng ta sẽ xem HTTP request làm điều đó như thế nào.

Từ cửa sổ Firefox, nhấn vào **Tools**, "**Tamper Data**".

Một cửa sổ “Tamper Data - Ongoing requests” sẽ mở ra, thay đổi kích thước cửa sổ Firefox và đặt nó bên cạnh cửa sổ Tamper Data để cả hai cửa sổ có thể nhìn thấy, như hình dưới đây.



Trong trang WebGoat, gõ lại tên của bạn và nhấn vào nút **Go!**.

Yêu cầu GET và POST xuất hiện trong hộp thoại Tamper Data, như được hiển thị ở trên.

Làm cho hộp thoại Tamper Data rộng hơn, và cuộn lên phía trên cùng của khung trên. Nhấp vào yêu cầu POST, khung dưới hiển thị đầy đủ các thông số.

Filter									Show All
Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags	
10:57:15.731	50 ms	50 ms	-1	POST	200	application/json	http://localhost:8080...	LOAD_BACKGROUND LOAD_B...	
10:57:15.808	48 ms	48 ms	-1	GET	200	application/json	http://localhost:8080...	LOAD_BACKGROUND LOAD_B...	
10:57:15.813	56 ms	56 ms	-1	GET	200	application/json	http://localhost:8080...	LOAD_BACKGROUND LOAD_B...	
10:57:19.317	25 ms	25 ms	-1	GET	200	application/json	http://localhost:8080...	LOAD_BACKGROUND LOAD_B...	
10:57:19.329	79 ms	79 ms	-1	GET	200	application/json	http://localhost:8080...	LOAD_BACKGROUND LOAD_B...	
10:57:24.319	38 ms	38 ms	-1	GET	200	application/json	http://localhost:8080...	LOAD_BACKGROUND LOAD_B...	
10:57:24.327	103 ms	103 ms	-1	GET	200	application/json	http://localhost:8080...	LOAD_BACKGROUND LOAD_B...	

Request Header Name	Request Header Value	Response Header Name	Response Header Value
Host	localhost:8080	Status	OK - 200
User-Agent	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0	X-Application-Context	application:8080
Accept	*/	X-Content-Type-Options	nosniff
Accept-Language	en-US,en;q=0.5	X-XSS-Protection	1; mode=block
Accept-Encoding	gzip, deflate	X-Frame-Options	DENY
Content-Type	application/x-www-form-urlencoded; charset=UTF-8	Content-Type	application/json; charset=UTF-8
X-Requested-With	XMLHttpRequest	Transfer-Encoding	chunked
Referer	http://localhost:8080/WebGoat/start.mvc	Date	Tue, 11 Sep 2018 03:57:15 GMT
Content-Length	15	X-Adguard-Filtered	AdGuard for Windows; version=6.3.1399.4073
Cookie	JSESSIONID=9047CBFC21DB72CEFCA8A1F079945C6F		
Connection	keep-alive		
POSTDATA	person=YOURNAME		

Khung bên trái phía dưới hiển thị yêu cầu POST được gửi đến máy chủ. Lưu ý những thành phần này:

- **Host:** Máy chủ đang yêu cầu dữ liệu
- **User-Agent:** Xác định loại trình duyệt
- **Referer:** Hiển thị trang truy cập đến
- **Cookie:** Xác định tài khoản của bạn
- **POSTDATA:** Mang dữ liệu bạn nhập vào form, bao gồm tên của bạn

Phía dưới bên phải cho thấy phản hồi từ máy chủ, có trạng thái Status: OK-200 nếu mọi thứ đều đúng.

