Table of Contents

Download Links

Initial Setup

Tools of the Trade

Miscellaneous

Attacking Web Applications using Burp Suite

26th October, 2018

Workshop at:
BSIDES DELHI 2018

Abstract

In this completely hands-on workshop, you would get to understand the techniques and methodologies that could be applied when performing a web application penetration testing. Throughout this workshop, you would be using Burp Suite tool, which is a conglomerate of distinct tools with powerful features. Apart from gaining familiarity with the tools and the techniques involved in application security testing, you would also get an opportunity to understand some of the common vulnerabilities from the OWASP Top 10 – 2017 list. We would provide you with a vulnerable website, and you would uncover security issues in it even if you h# Attacking Web Applications using Burp Suite

26th October, 2018

Workshop at:
BSIDES DELHI 2018

Abstract

In this completely hands-on workshop, you would get to understand the techniques and methodologies that could be applied when performing a web application penetration testing. Throughout this workshop, you would be using Burp Suite tool, which is a conglomerate of distinct tools with powerful features. Apart from gaining familiarity with the tools and the techniques involved in application security testing, you would also get an opportunity to understand some of the common vulnerabilities from the OWASP Top 10 – 2017 list. We would provide you with a vulnerable website, and you would uncover security issues in it even if you have never done this before!

Speaker Profile

Speaker-1

Riddhi Shree is working as Application Security Engineer at Appsecco. She is also one of the chapter leaders for null Community - Bangalore Chapter. She has over 9 years of experience in Software testing industry. She has delivered multiple talks and training sessions during open security meetups. She has, recently, conducted a 2-days workshop at c0c0n XI - Data Privacy, Cyber Security & Hacking Conference on "Burp Suite For Web and Mobile Security Testing".

Speaker-2

Vandana Verma is a Security Architect at IBM with over 12 years of experience specializing in web application, infrastructure and cloud security. She is part of security communities such as Volunteer Coordinator – Asia Pacific for OWASP Women in Appsec (WIA) & OWASP WIA Secretary, OWASP Chapter Leader and Heading InfoSecGirls. She has given talks and workshops at many colleges and security conferences including AppSec Europe, AppSec USA, NullCon and c0c0n.

Pre-Requisites

- Laptop with administrator access (mandatory)
- Minimum 4 GB RAM
- Atleast 10 GB of free hard disk space
- Oracle VirtualBox 5.x or later installed.
- Burp Suite Professional / Community Edition installed
- Make sure Burp Suite can start
- Firefox browser with FoxyProxy Standard add-on installed

Download Links

- Virtual Machine (bsides-workshop-vm.ova)
- Burp Suite Professional Edition
- Burp Suite Community Edition
- FoxyProxy Standard add-on ave never done this before!

Speaker Profile

Speaker-1

Riddhi Shree is working as Application Security Engineer at Appsecco. She is also one of the chapter leaders for null Community - Bangalore Chapter. She has over 9 years of experience in Software testing industry. She has delivered multiple talks and training sessions during open security meetups. She has, recently, conducted a 2-days workshop at c0c0n XI - Data Privacy, Cyber Security & Hacking Conference on "Burp Suite For Web and Mobile Security Testing".

Speaker-2

Vandana Verma is a Security Architect with over 12 years of experience specializing in web application, infrastructure and cloud security. She is part of security communities such as Volunteer Coordinator – Asia Pacific for OWASP Women in Appsec (WIA) & OWASP WIA Secretary, OWASP Chapter Leader and Heading InfoSecGirls. She has given talks and workshops at many colleges and security conferences including AppSec Europe, AppSec USA, NullCon and c0c0n.

Pre-Requisites

1. Download files from the provided download links (see section below).
2. Make sure you have done the initial setup by following the steps as described in the **Initial Setup** section.
3. Familiarize yourself with the Burp tools by following the steps mentioned in **Tools of the Trade** section.

Download Links

- Virtual Machine (bsides-workshop-vm.ova)
- Burp Suite Professional Edition
- Burp Suite Community Edition

Initial Setup

- Start Burp Suite Professional
- Import Virtual Machines

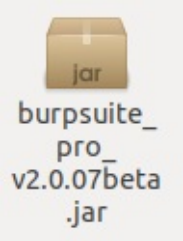
- Create New Firefox Profile
- Add FoxyProxy Addon
- Add New Proxy In FoxyProxy
- Configure Proxy Listener
- Install Burp's CA Certificate In Firefox
- Access Security Shepherd Application
- Remove Unnecessary Browser Traffic
- Setup Hotkeys

Tools of the Trade

- Target
- Proxy
- Scanner
- Intruder
- Repeater
- Sequencer
- Decoder
- Comparer
- Extender

Start Burp Suite Professional

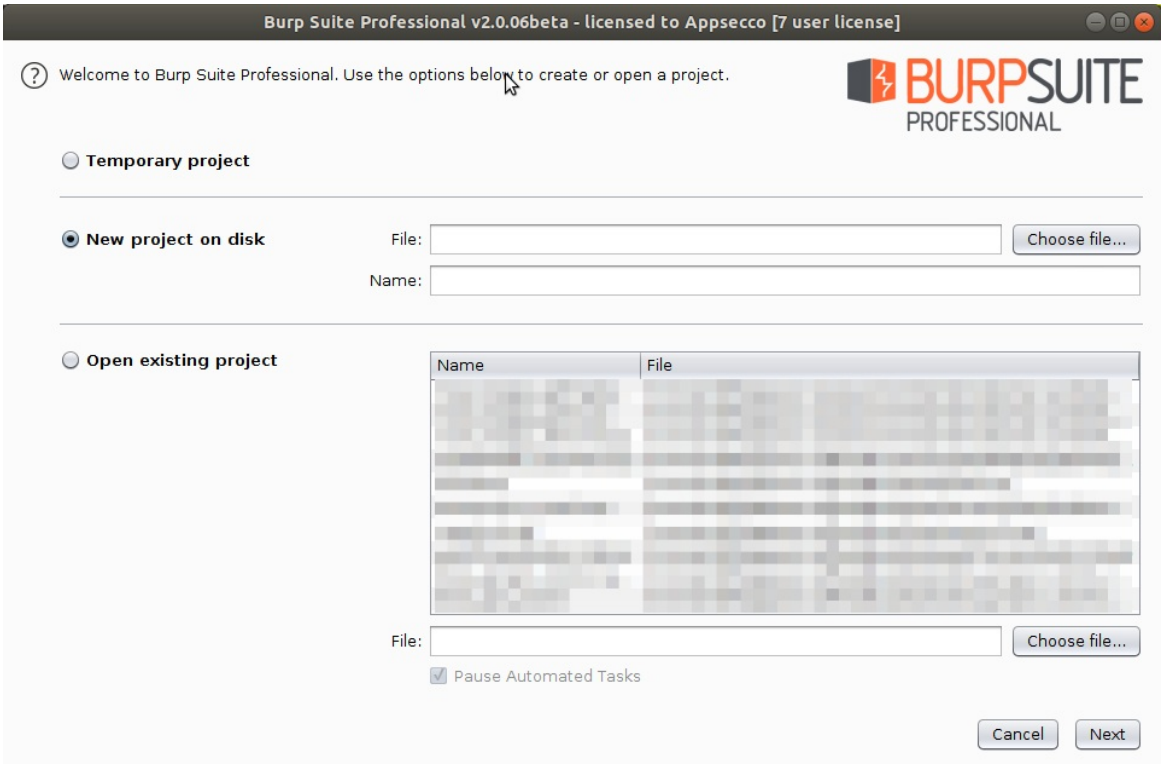
1. Download the JAR file for Burp Suite Professional.
2. Go to the folder containing the jar file "burpsuite_pro_v2.0.07beta.jar".



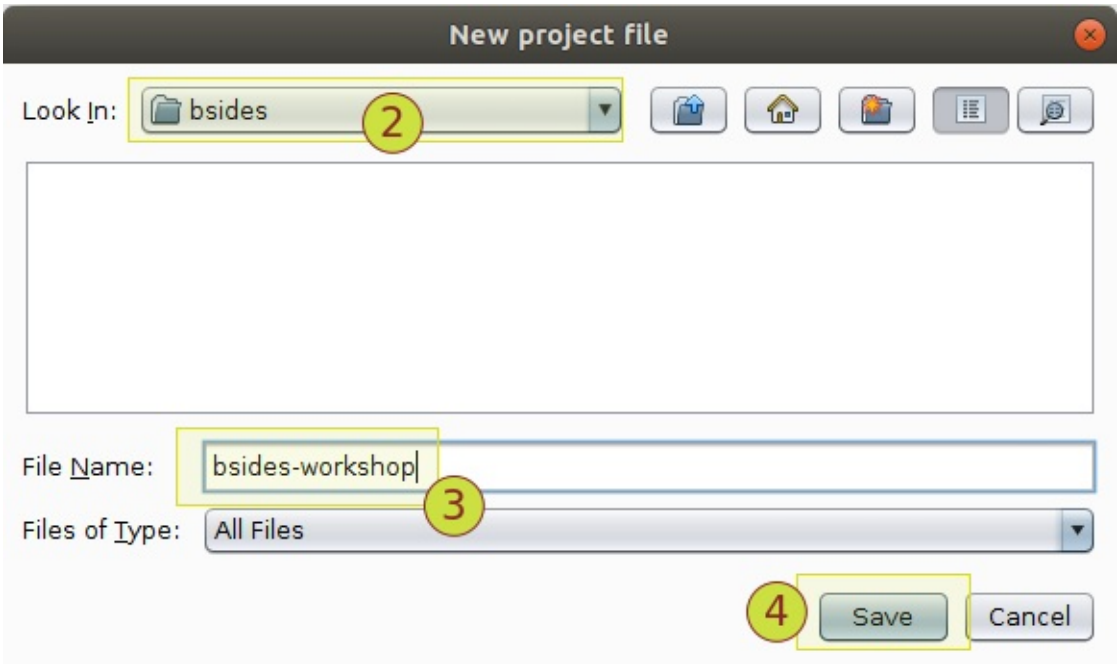
3. Run following command to start Burp Suite Professional Edition.

```
$ java -jar -Xmx2G burpsuite_pro_v2.0.07beta.jar
```

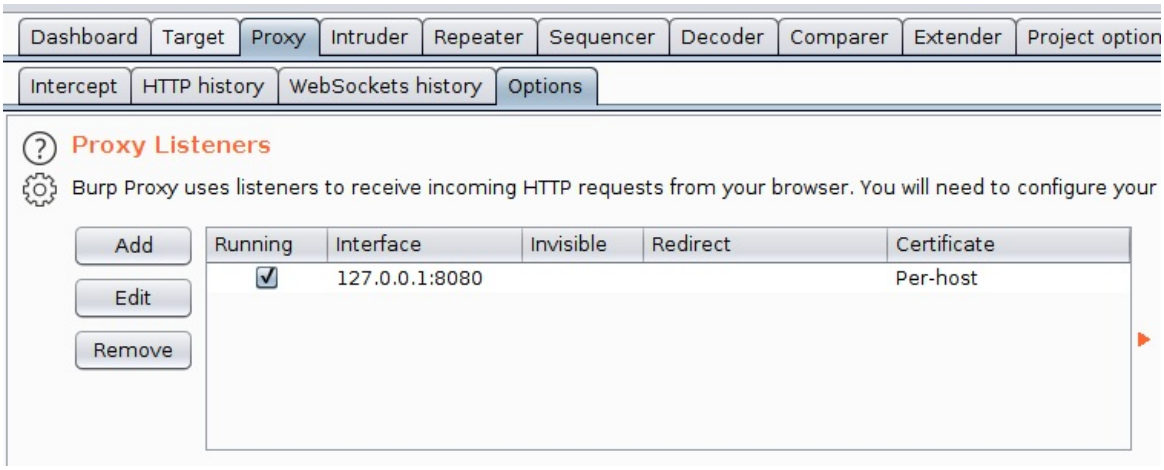
4. If you are prompted for licence, enter licence.
5. If you do not have a licence, switch to Burp Suite Community Edition, and skip to step #7.
6. Select "New project on disk" radio button.



7. Click on "Choose file" button, and choose a new location for creating a new project.



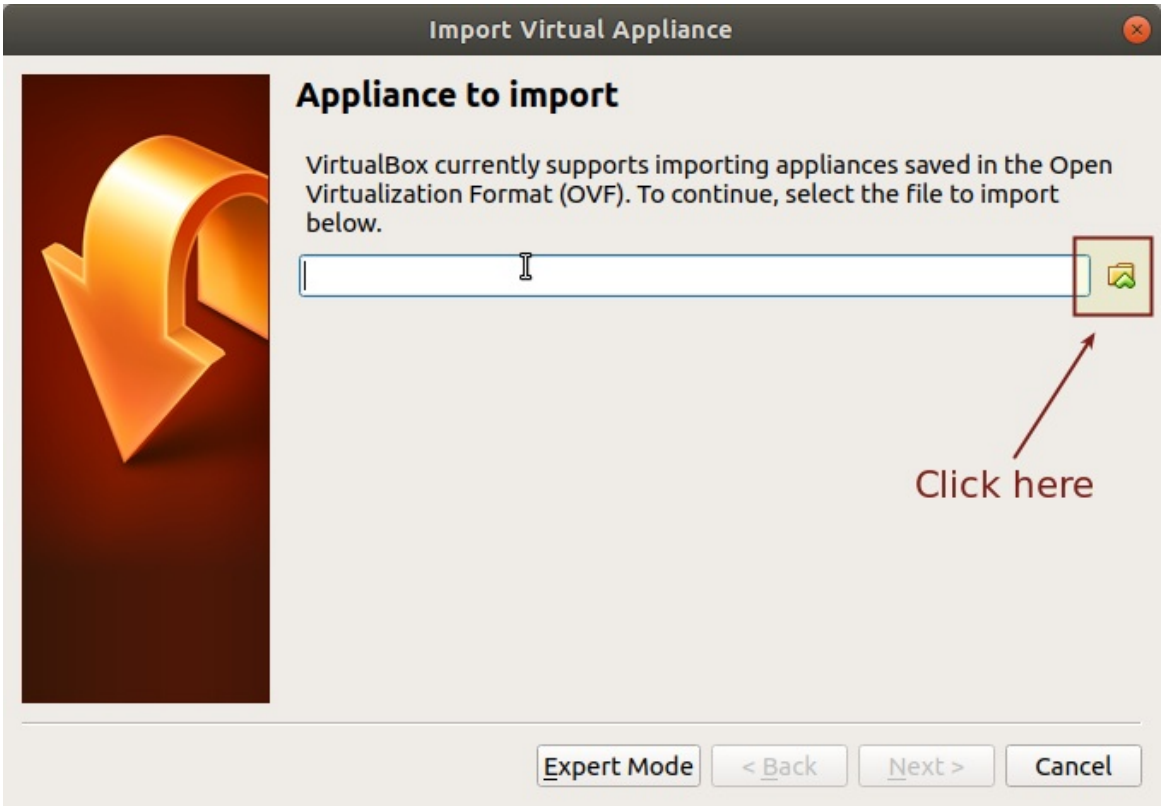
8. Click on "Next".
9. Click on "Start Burp".
10. Go to "Proxy" > "Options" > "Proxy Listeners", and validate the settings.



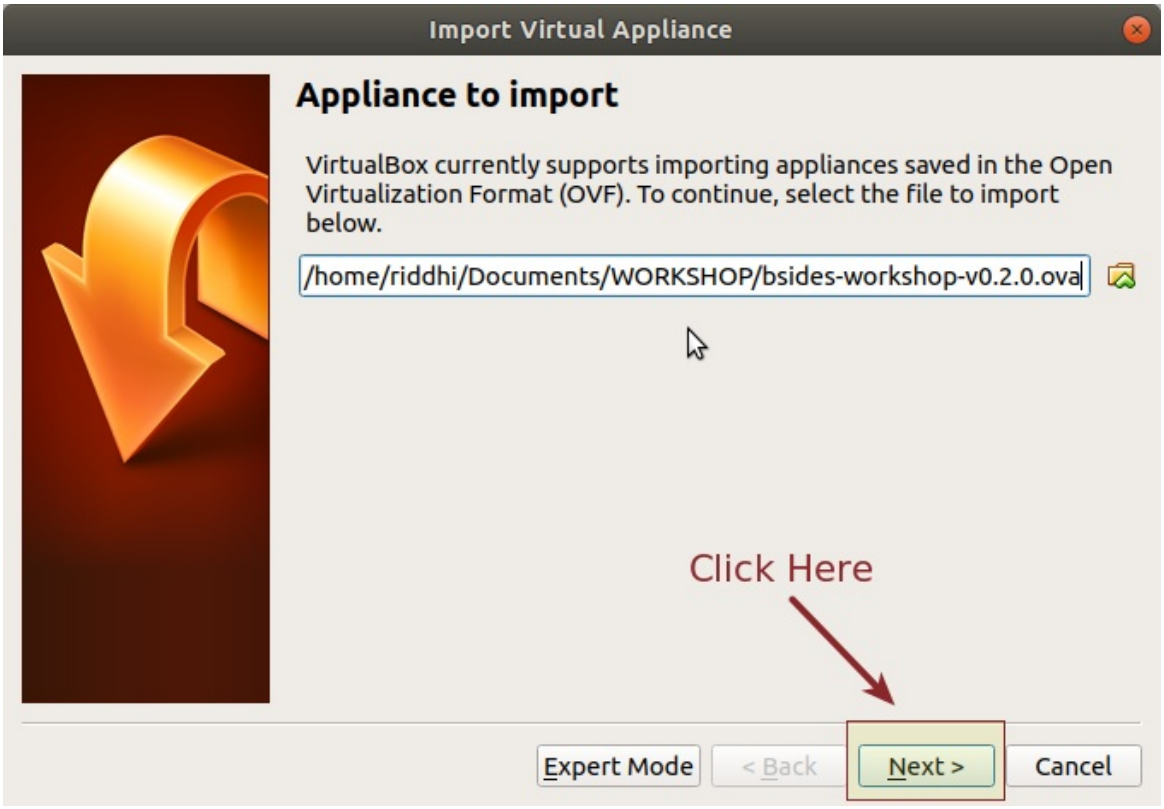
Import Virtual Machines

1. Download the OVA file named as bsides-workshop-vm.ova.
2. Open Virtual Box.
3. Click on "File" > "Import Appliance"

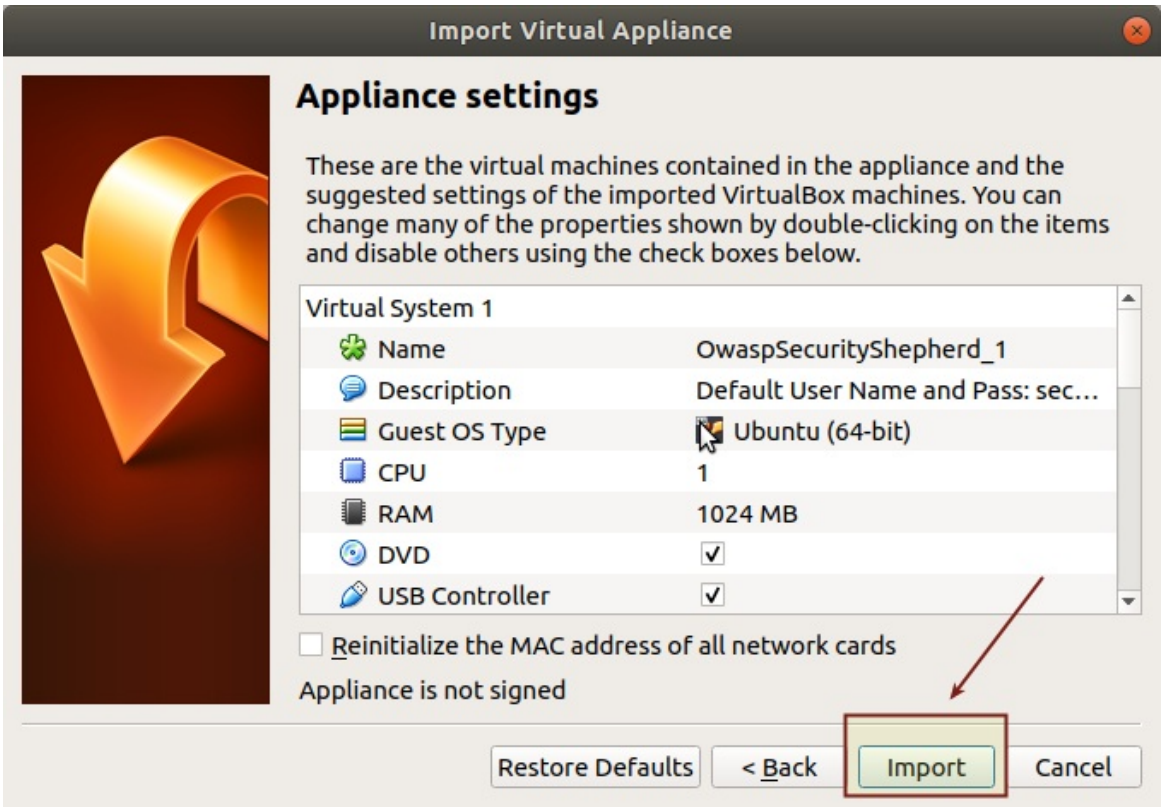
4. Locate and select the downloaded OVA file, i.e., "bsides-workshop-vm.ova".

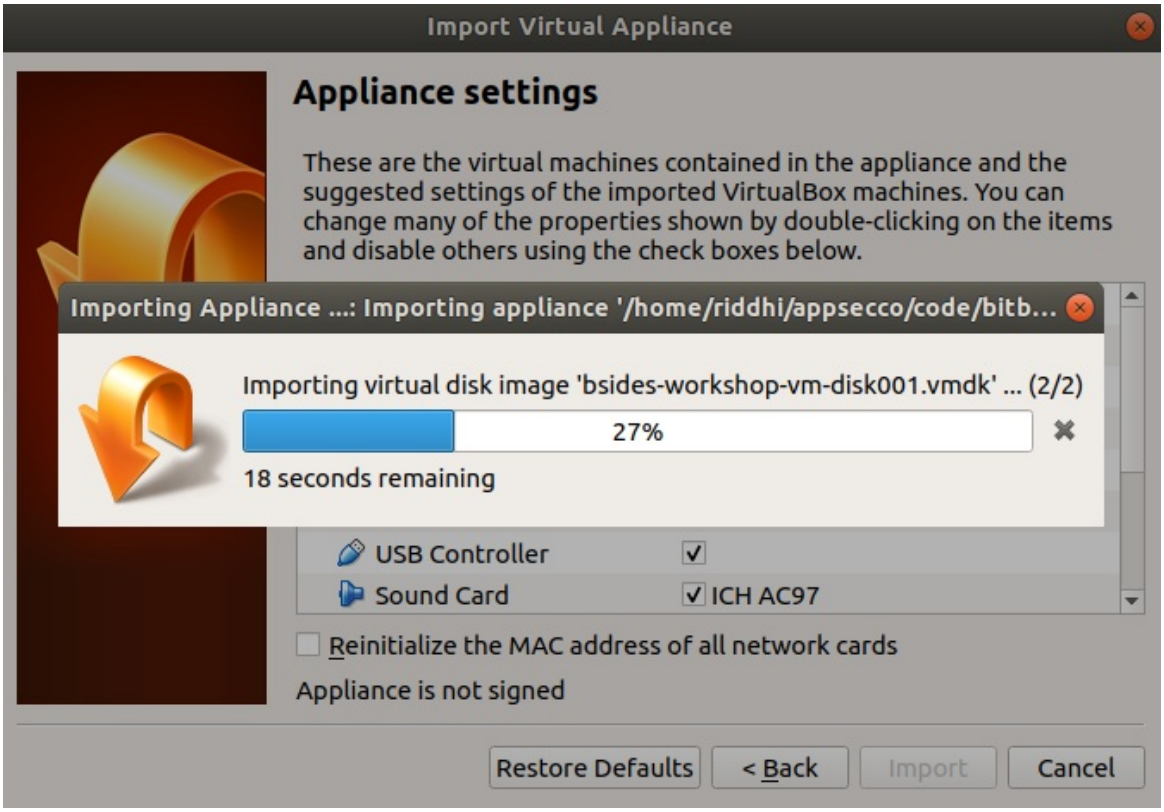


5. Click on "Next" button.

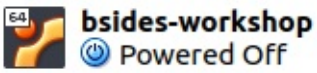


6. Import the OVA file by clicking on "Import" button.





7. You should see a virtual machine named as "bsides-workshop" imported successfully.



Create a new Firefox Profile

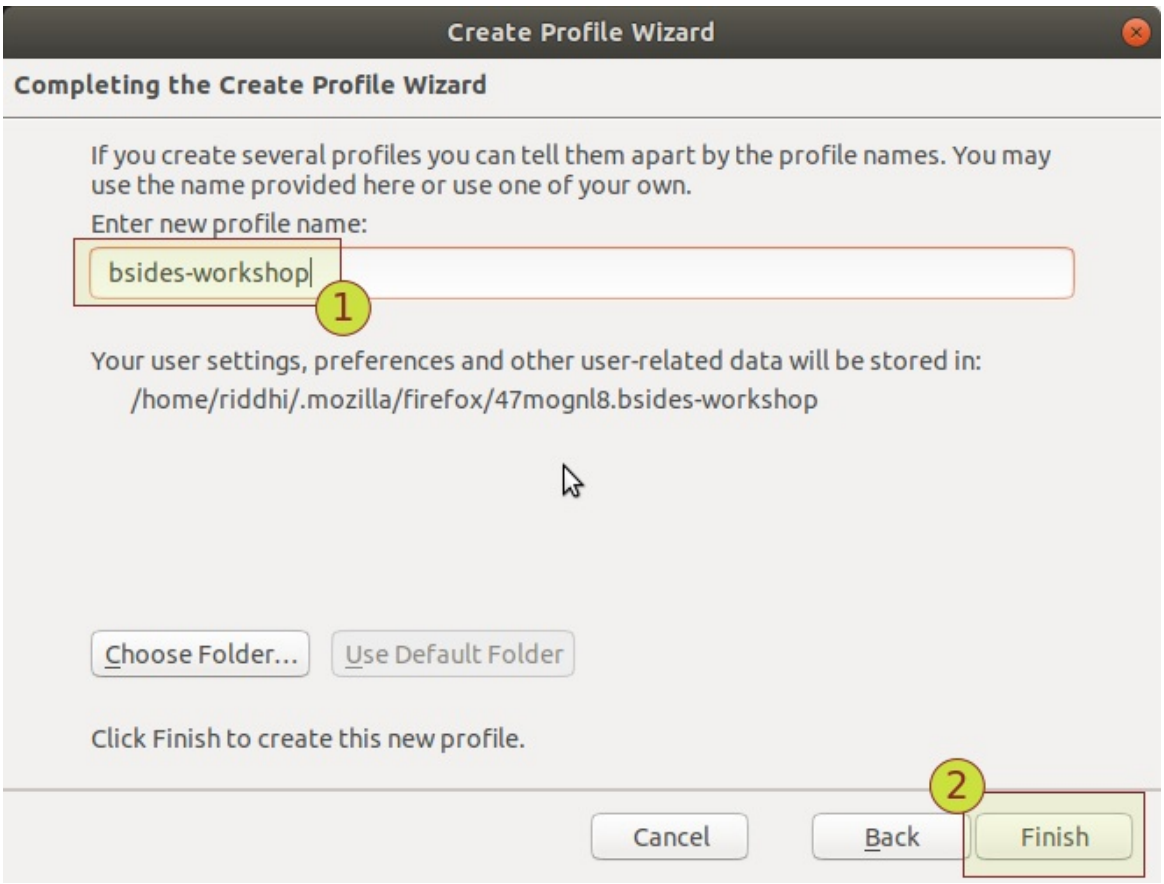
1. Close all running instances of Firefox browser.
2. Open a terminal in Ubuntu/Mac.
3. In Windows, press "Windows + R" to open the `Run` dialog.
4. Run the following command:

   Linux/MacOS: `firefox -p` / `firefox -P` / `firefox -ProfileManager`

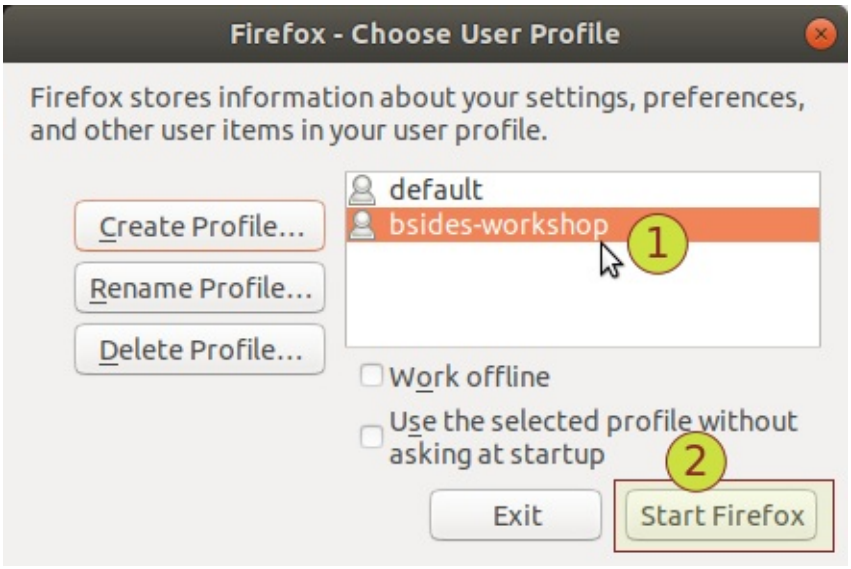
   Windows:
   `firefox.exe -P`

5. Click on "Create Profile".

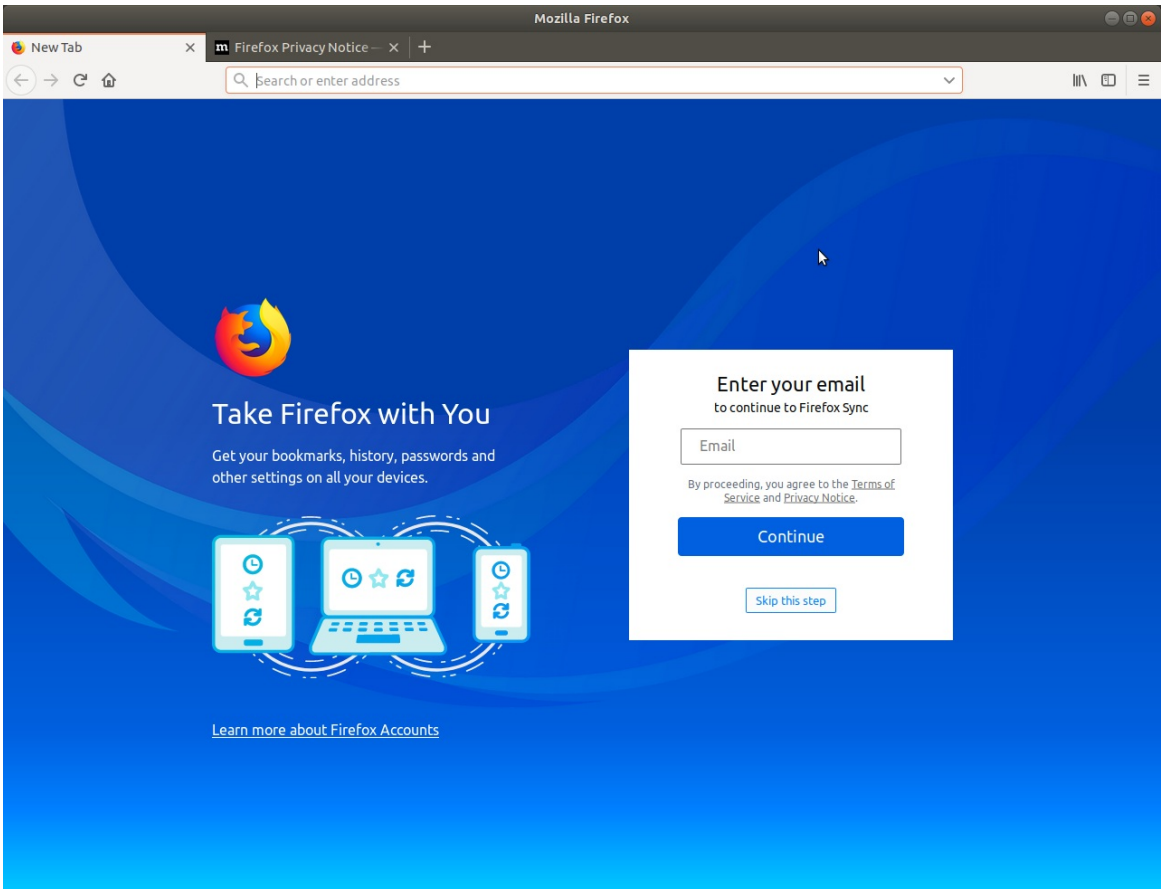
6. Give a name to your new firefox profile and click on "Finish" button.



7. Select the newly created profile and start firefox.

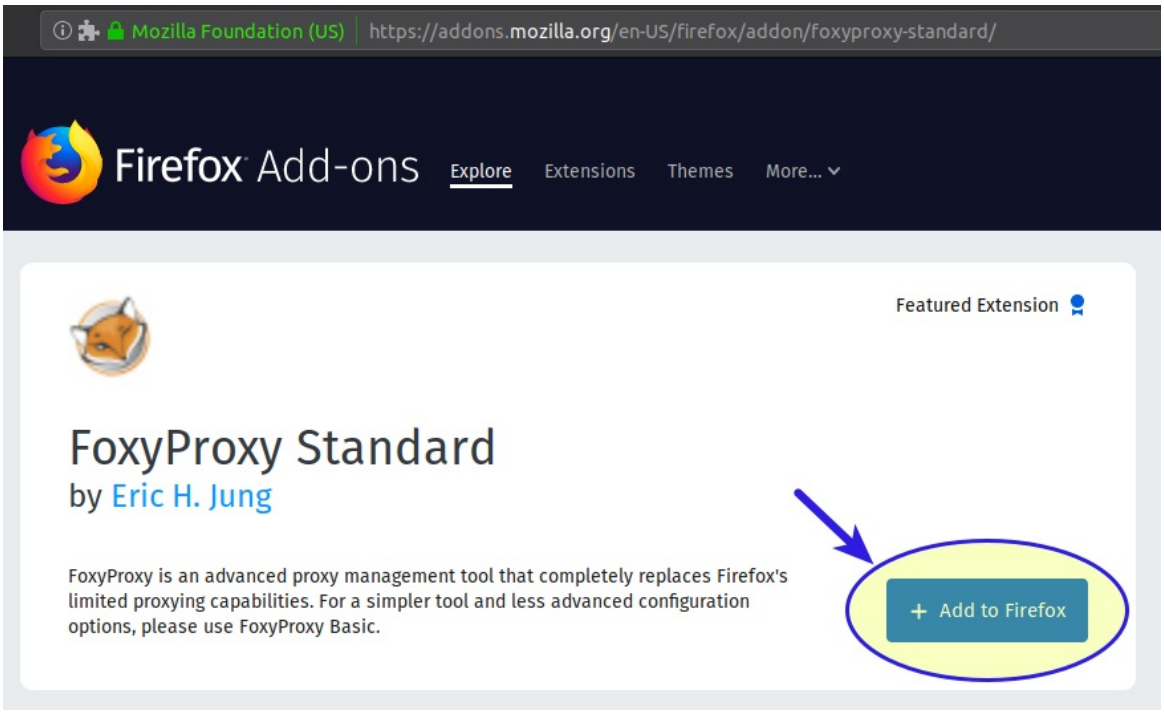


8. A fresh instance of Firefox browser should start with default browser settings.

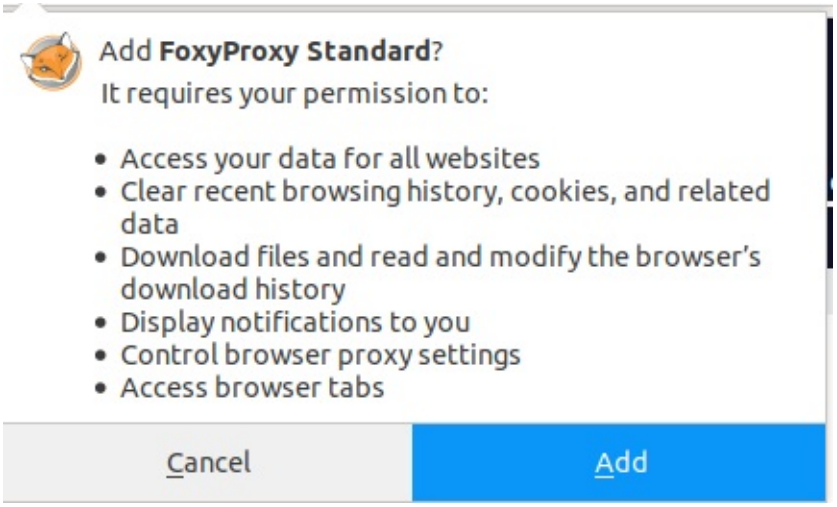


Add Foxy-Proxy Standard Add-on

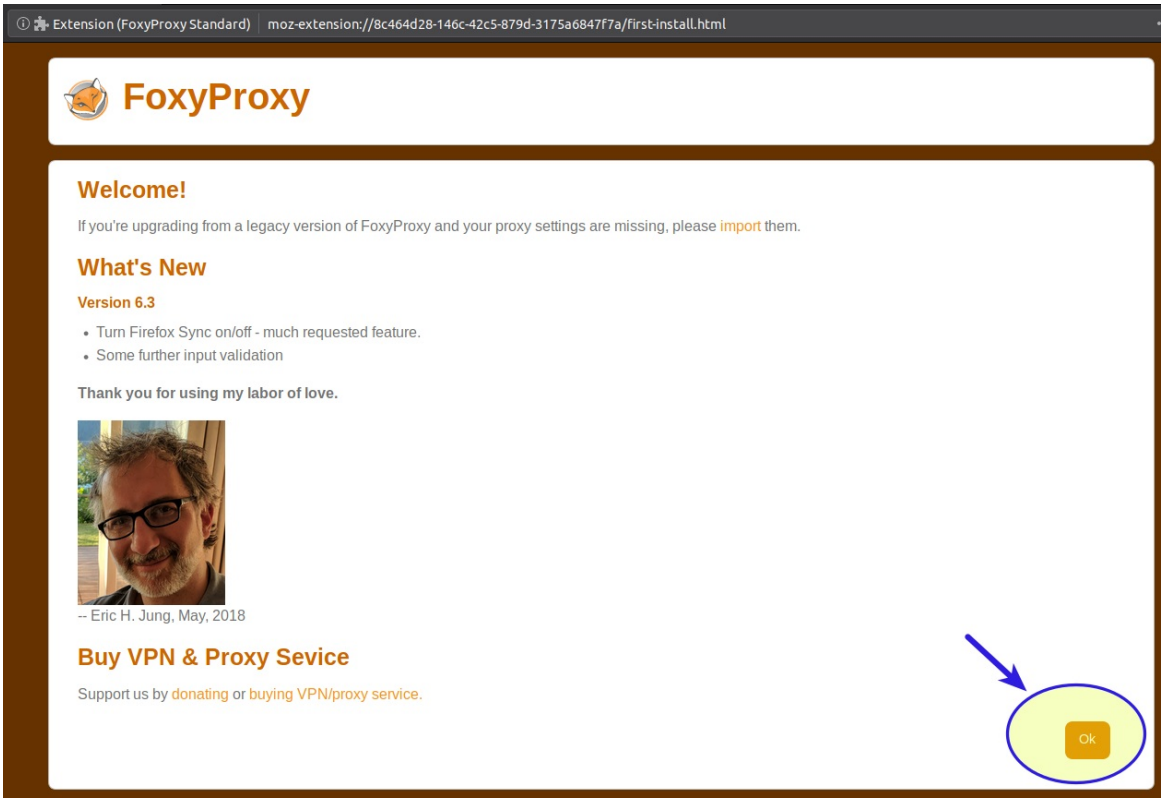
1. In Firfox browser, navigate to `https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/` .
2. Click on "Add to Firefox" button.

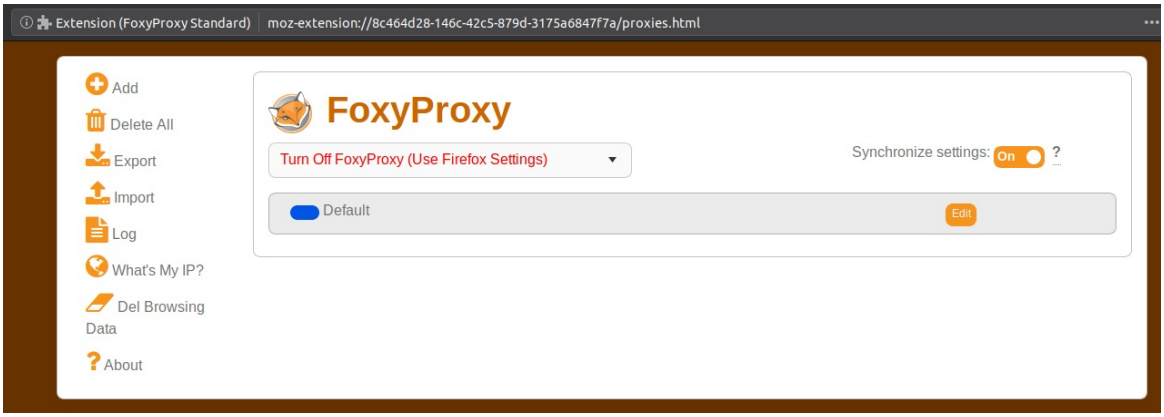


3. If permission is required, grant permission by clicking on "Add" button.



4. Click on "OK" button in the welcome screen.


Extension (FoxyProxy Standard)
moz-extension://8c464d28-146c-42c5-879d-3175a6847f7a/first-install.html
FoxyProxy
Welcome!
If you're upgrading from a legacy version of FoxyProxy and your proxy settings are missing, please import them.
What's New
Version 6.3
Turn Firefox Sync on/off - much requested feature.
Some further input validation
Thank you for using my labor of love.
-- Eric H. Jung, May, 2018
Buy VPN & Proxy Sevice
Support us by donating or buying VPN/proxy service.
Ok

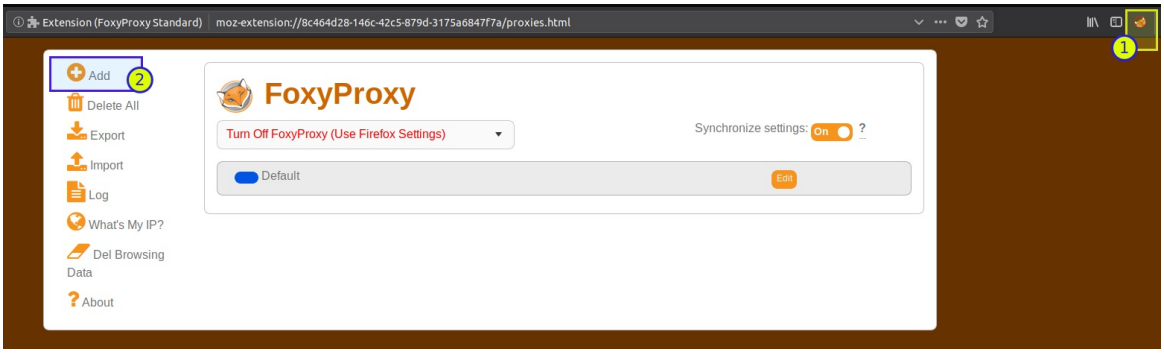

Extension (FoxyProxy Standard)
moz-extension://8c464d28-146c-42c5-879d-3175a6847f7a/proxies.html
Add
Delete All
Export
Import
Log
What's My IP?
Del Browsing Data
About
FoxyProxy
Turn Off FoxyProxy (Use Firefox Settings)
Synchronize settings:
On
?
Default
Edit

Add a New Proxy in FoxyProxy

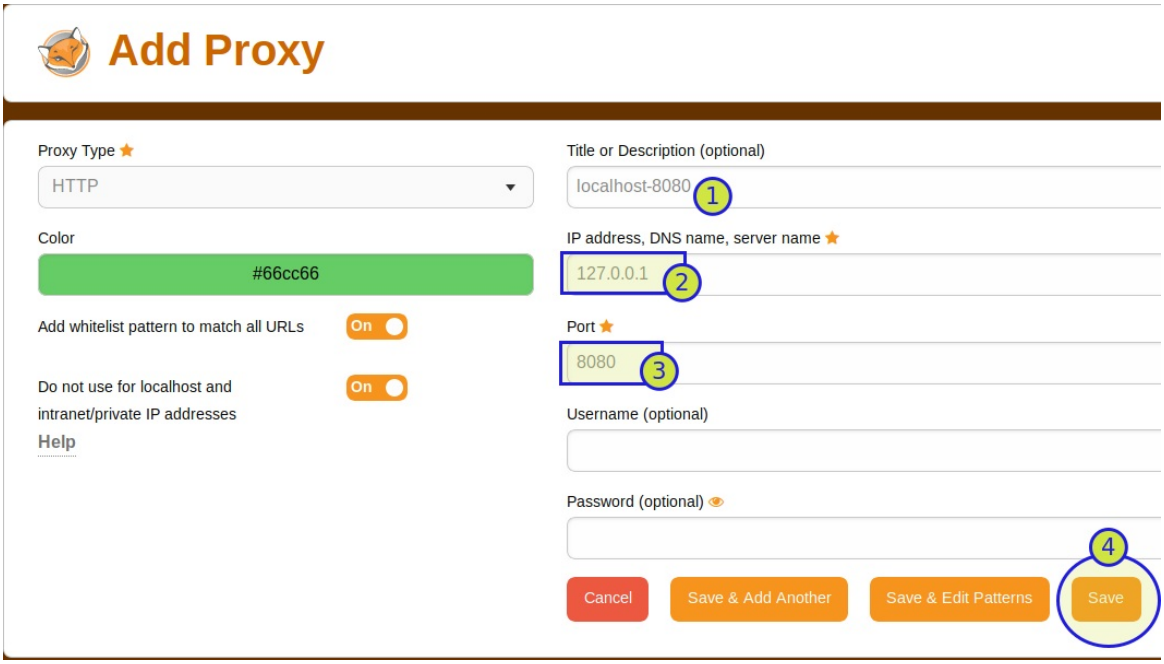
1. Go to the Firefox browser.
2. Click on `FoxyProxy` icon in the top-right corner of the browser.

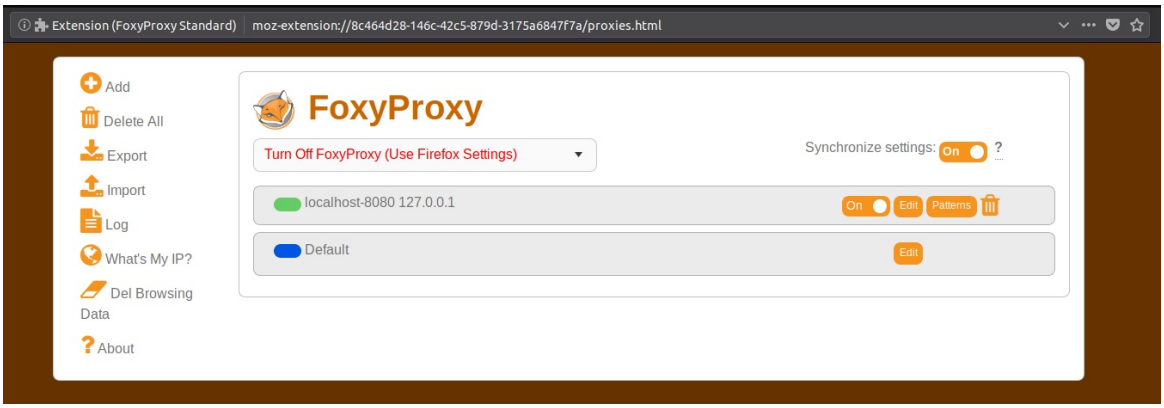
3. Select `Options` from the dropdown menu.

4. Click on `Add` button to add a new **proxy**.

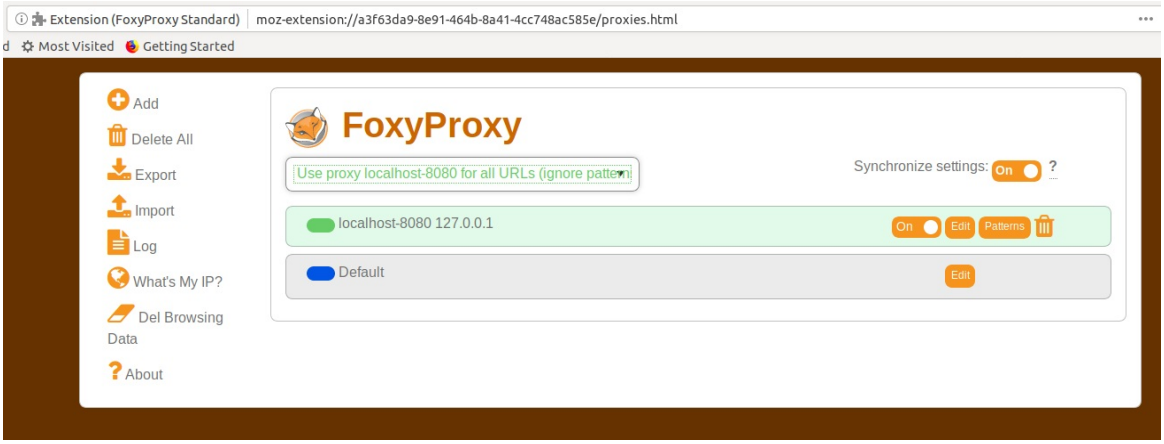


5. Enter title as `localhost-8080` (or anything of your choice), IP address as `127.0.0.1`, port as `8080`, and click on the `Save` button.



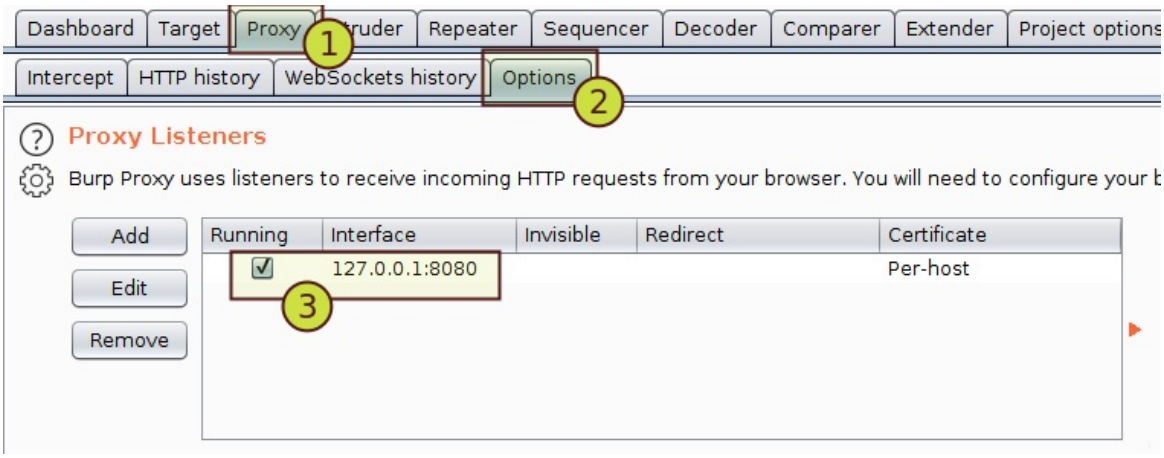


6. Enable proxy settings by selecting the option "**Use proxy localhost-8080 for all URLs (ignore patterns)**".

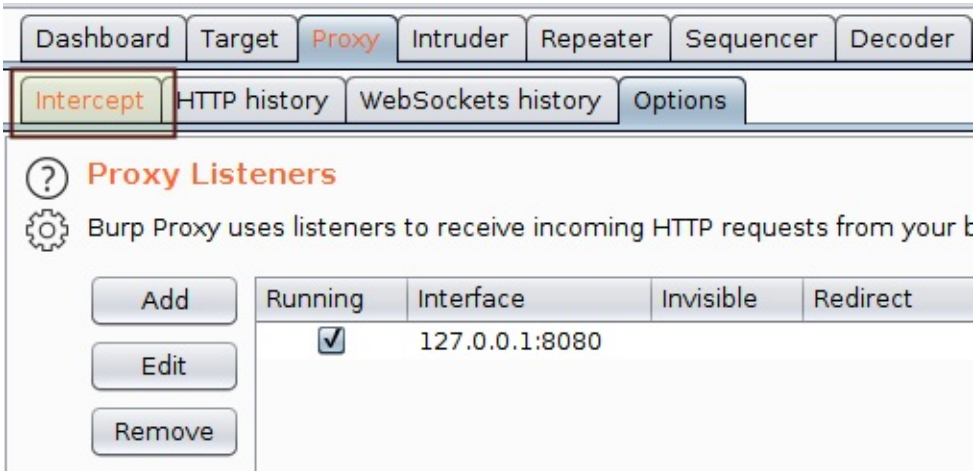


Configure Proxy Listener in Burp Suite

1. In Burp Suite, go to '**Proxy**' tab > '**Options**' sub-tab > '**Proxy Listeners**' section, and validate the proxy listener settings. It should be same as that set in the Firefox browser, i.e., enable a proxy listener for localhost (`127.0.0.1`) on port `8080` .

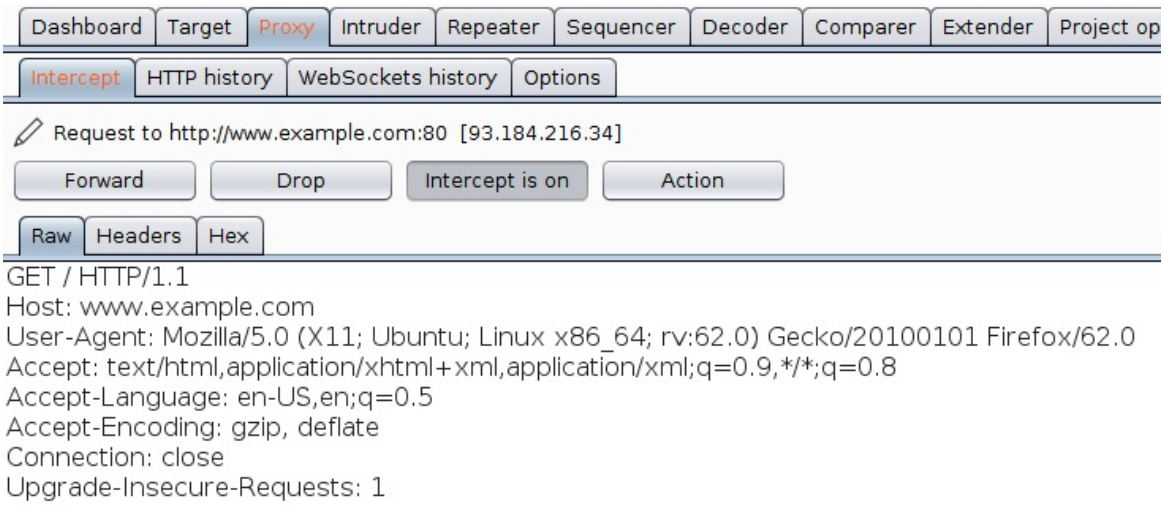


2. Switch to your Firefox browser and navigate to `www.example.com`

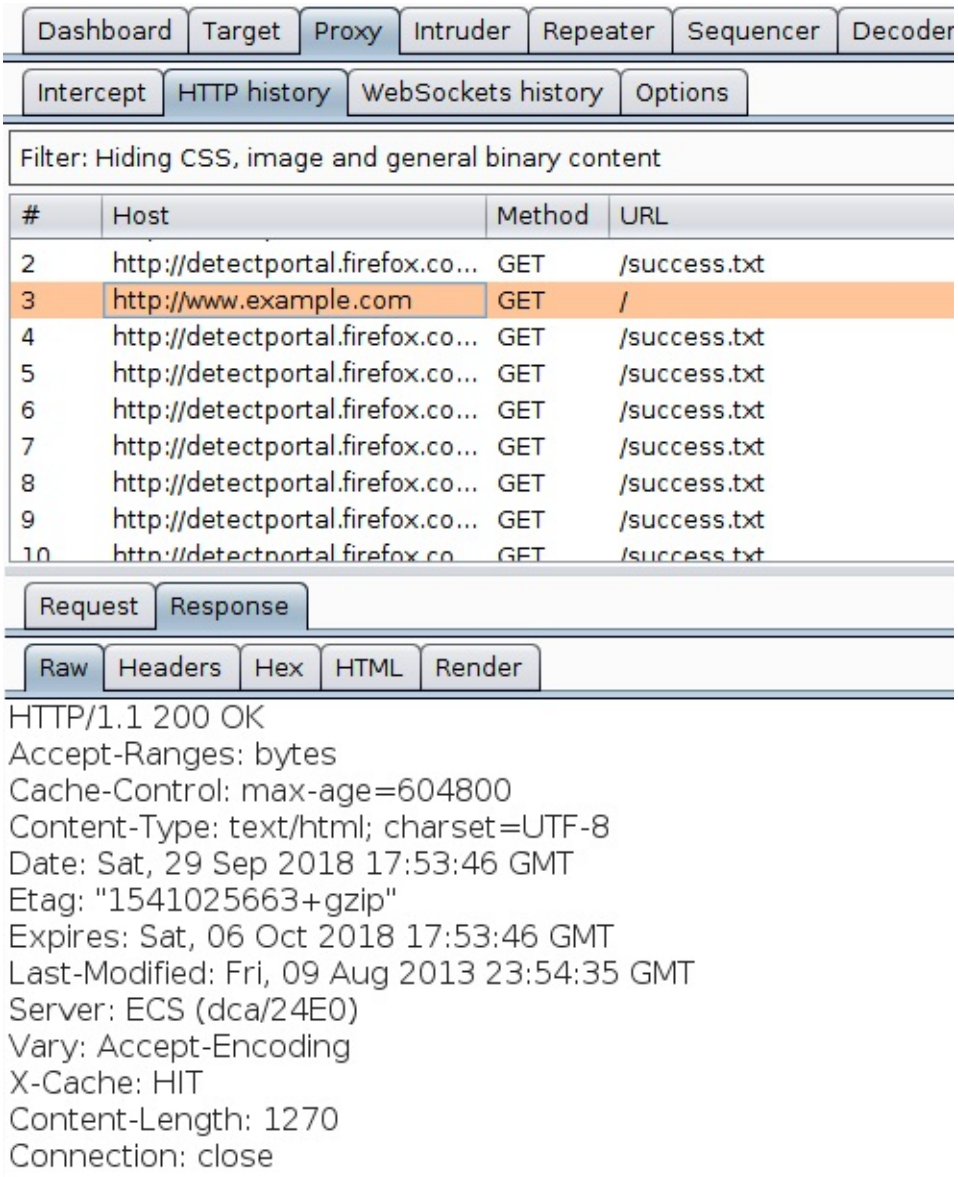


3. Switch back to Burp and navigate to the "Intercept" tab.

4. Forward the intercepted request.



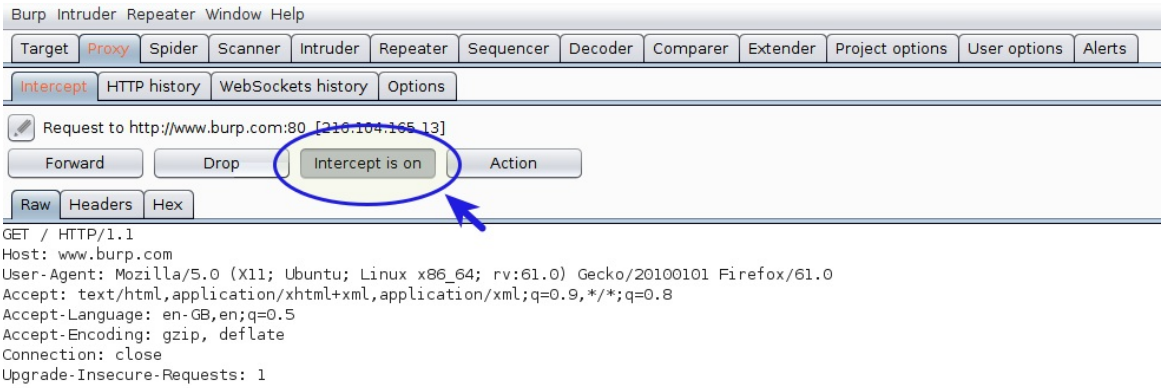
5. Switch to "Proxy" > "HTTP History" tab.

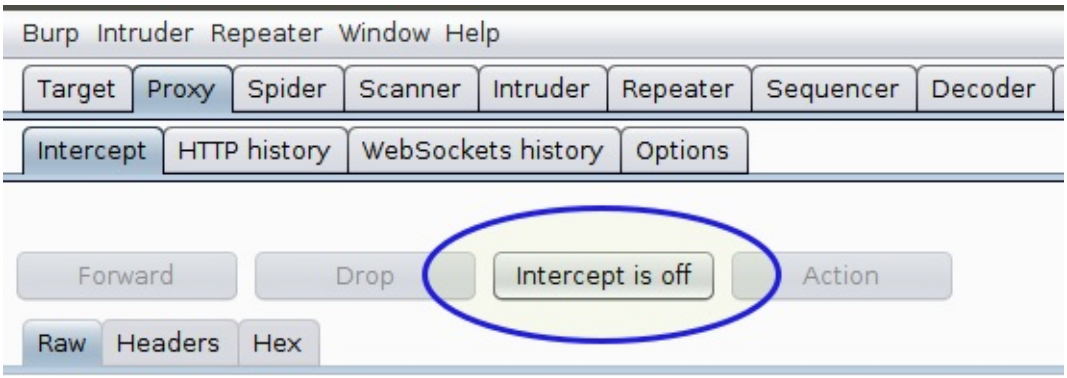


6. You should see the traffic from Firefox browser getting populated in Burp's HTTP history table.

Install Burp's CA Certificate

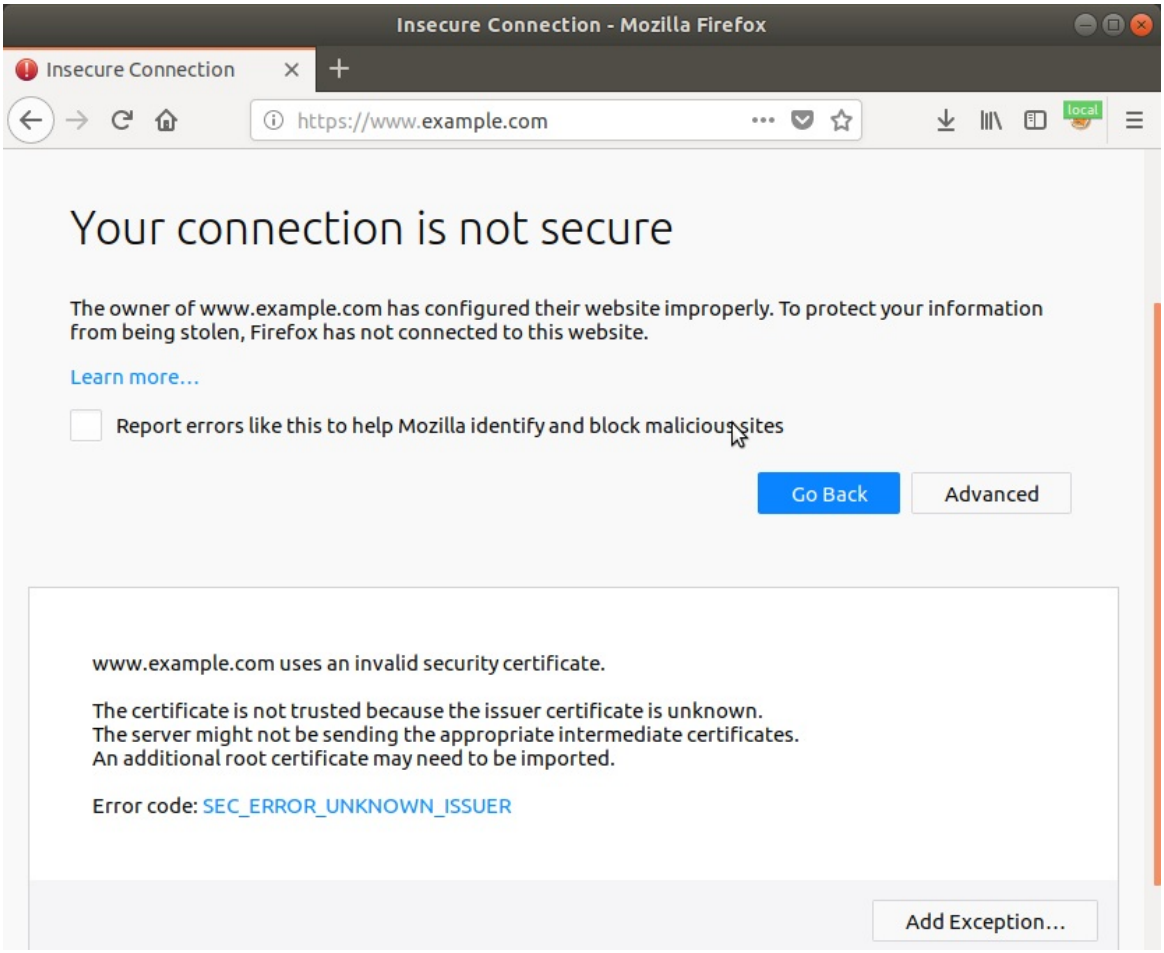
1. In Burp Suite, go to **Proxy** > **Intercept** tab and disable intercept mode by clicking on the "**Intercept is on**" button.



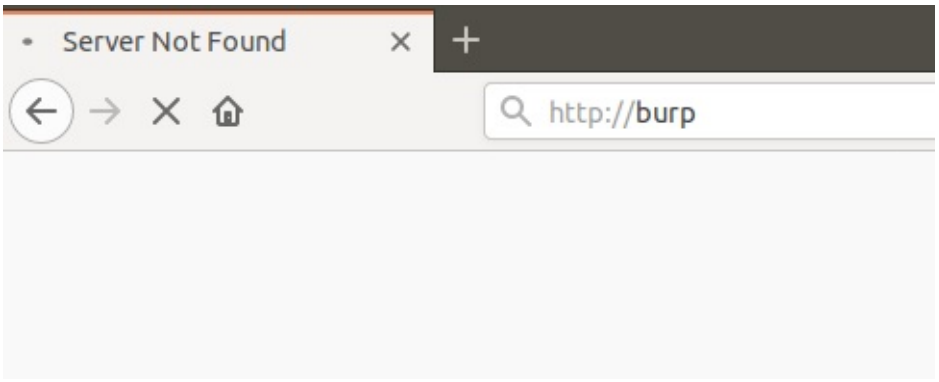


2. In Firefox, navigate to a secure website, e.g., `https://www.example.com`.

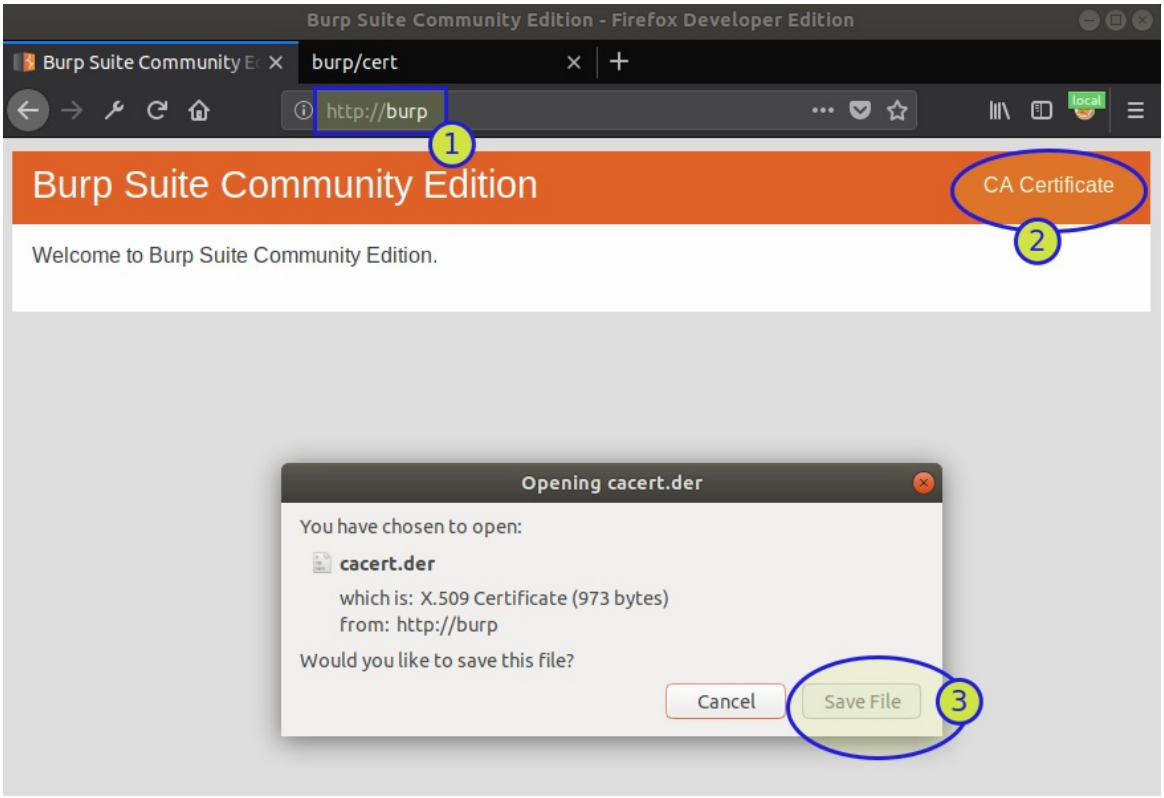
   If you have configured Burp's proxy listener correctly, and you haven't installed Burp's self-signed Certificate Authority (CA) certificate, yet, then the browser may throw an "invalid security certificate" error with the message "*...issuer certificate is unknown*". Click on the "Advanced" button to see error details.



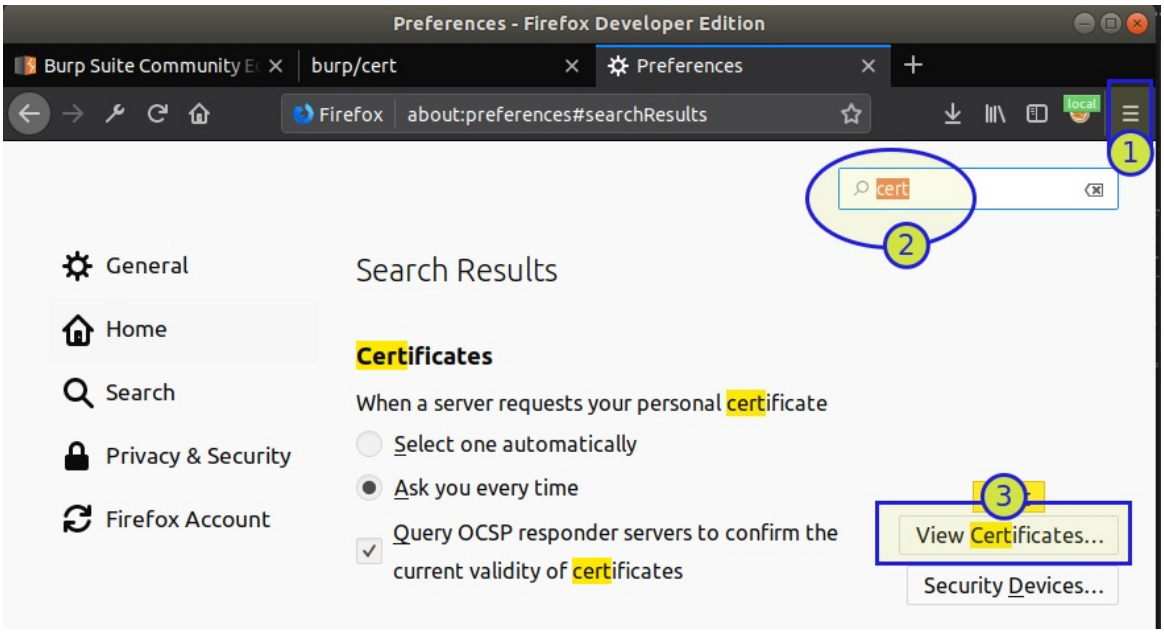
3. If you received "SEC_ERROR_UNKNOWN_ISSUER" error from the browser, navigate to `http://burp`.



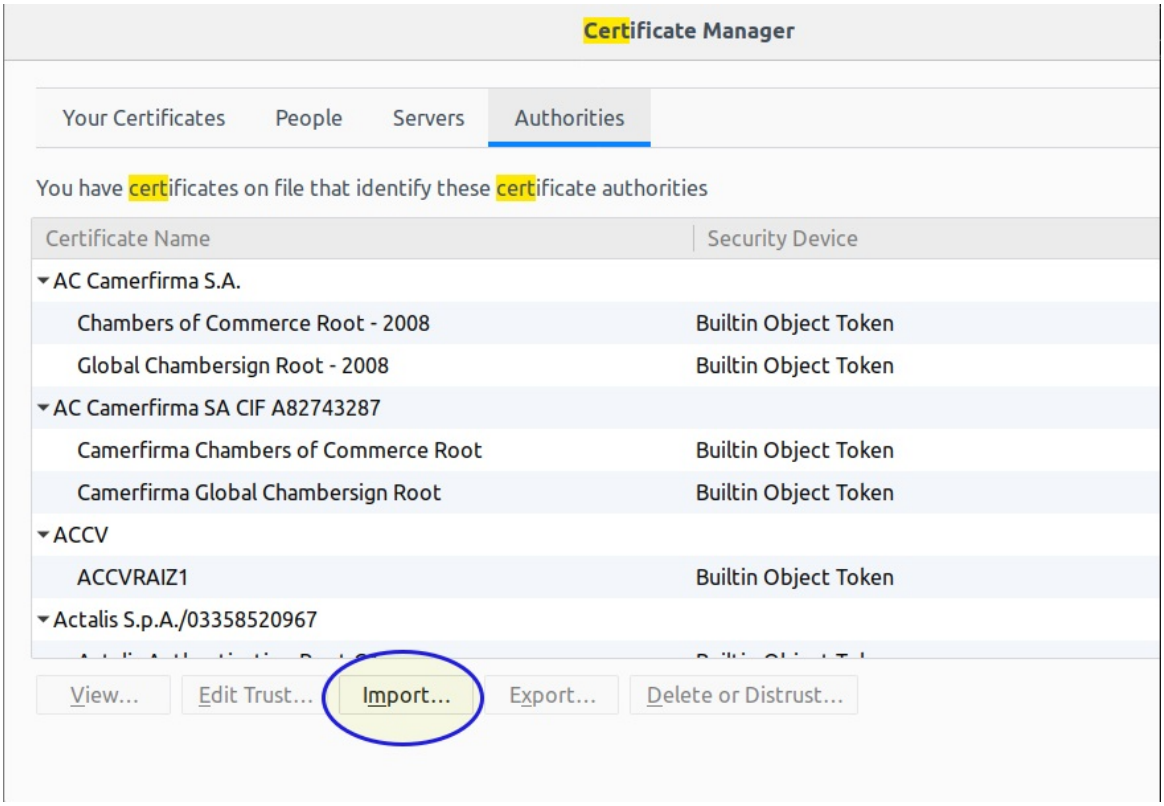
4. Click on "CA Certificate" link to download the "cacert.der" file.



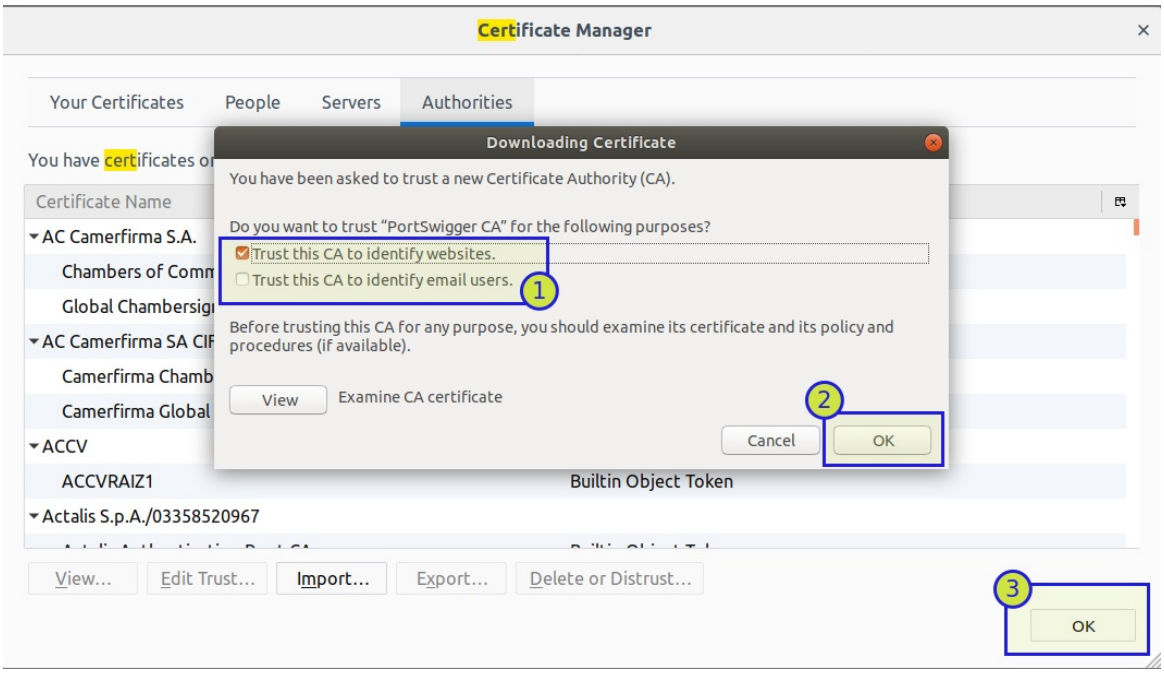
5. In the Firefox browser, go to "Preferences", search for the term "certificate", and click on "View Certificates" button.



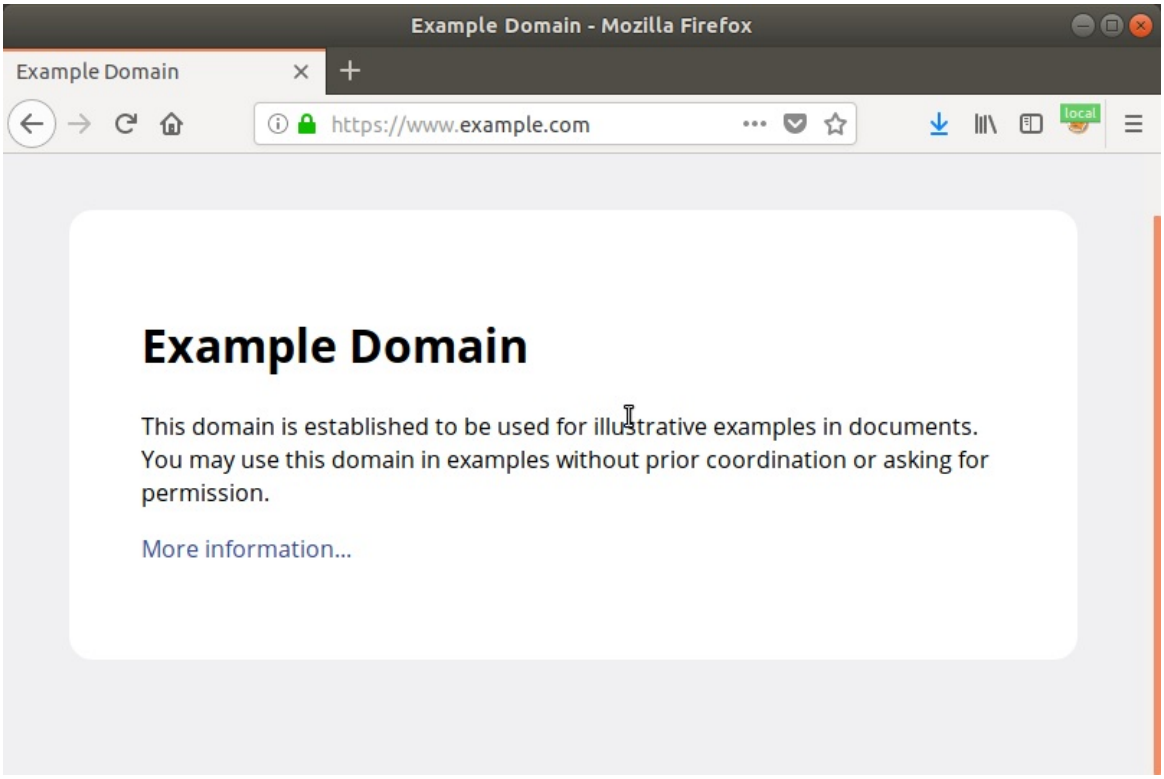
6. In the "Certificate Manager" window, click on "Import" button and select the downloaded "cacert.der" file.



7. In the "Downloading Certificate" window prompt, select checkboxes as shown in following image and click on "Ok".

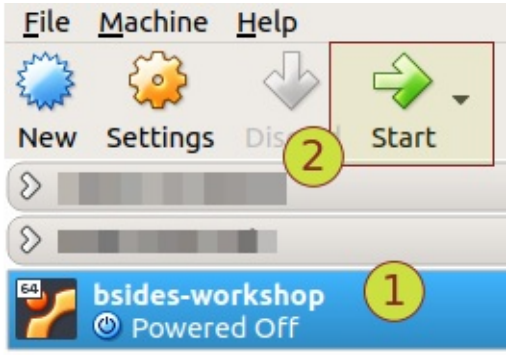


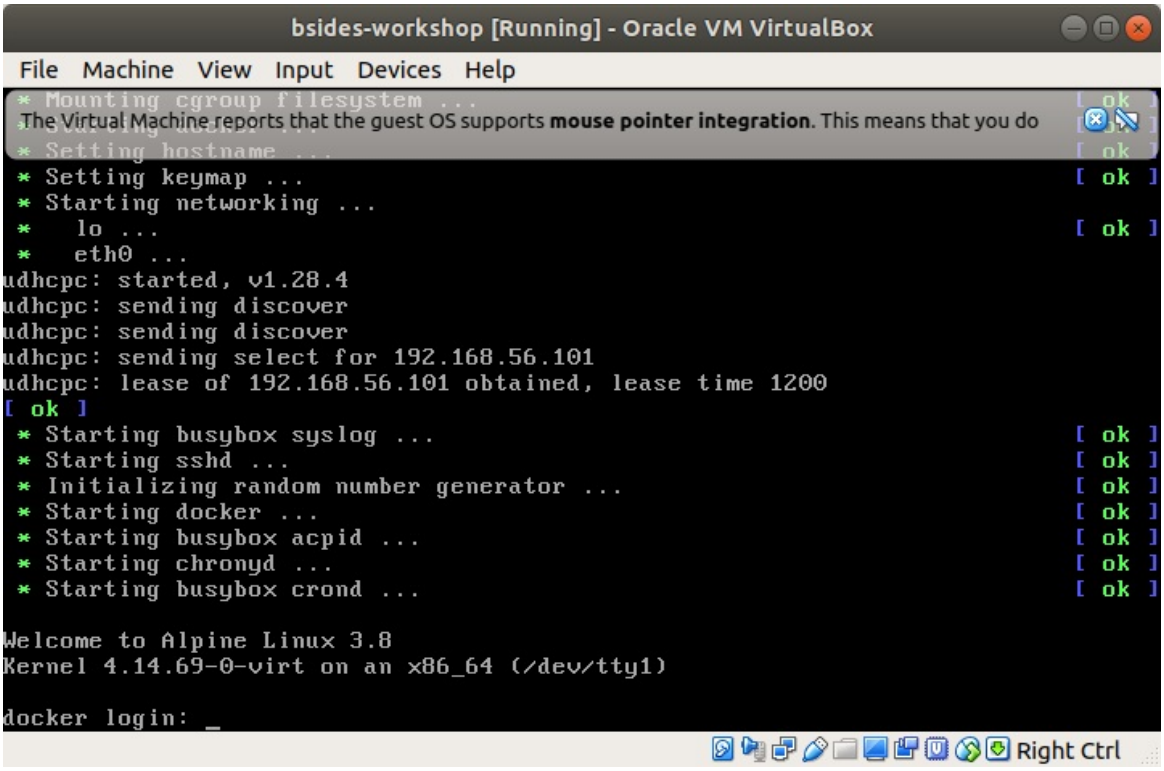
8. Access secure websites, e.g., "https://www.example.com", without encountering the "SEC_ERROR_UNKNOWN_ISSUER" error.


Example Domain - Mozilla Firefox
Example Domain
https://www.example.com
Example Domain
This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.
More information...

Access Security Shepherd Web Application

1. Start the virtual machine named as "bsides-workshop", by selecting "bsides-workshop" and clicking on the "Start" button.





2. Login to the Virtual Machine using the following credentials: **Username**: `root` **Password**: `Docker@321`

3. Obtain the IP address of the virtual machine by running `ifconfig eth0` command on the terminal.

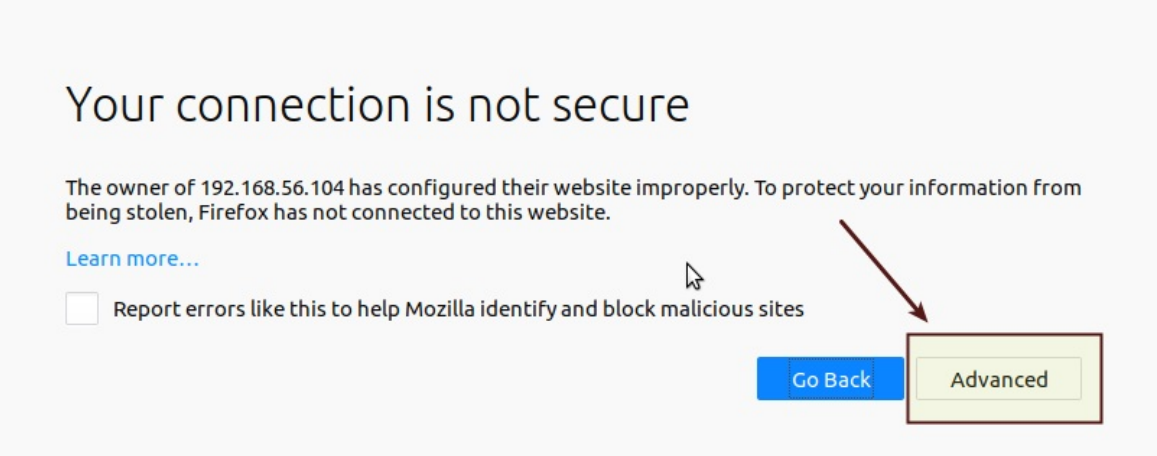
4. In my case, I got the IP address as `192.168.56.101` .

5. Run following commands to start Security Shepherd application:

```
# cd SecurityShepherd/
# docker-compose up -d
```

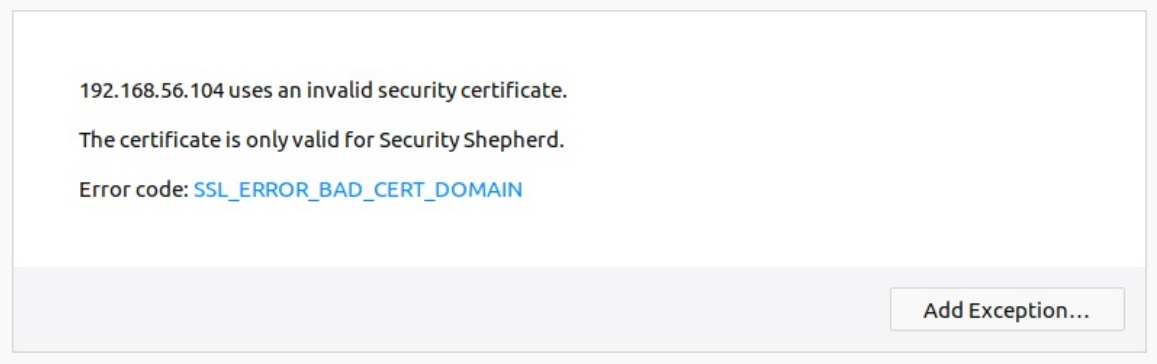
6. In Firefox, access the URL `http://192.168.56.101` .

7. If the browser throws an error saying "Your connection is not secure", click on the "Advanced" button to see error details.

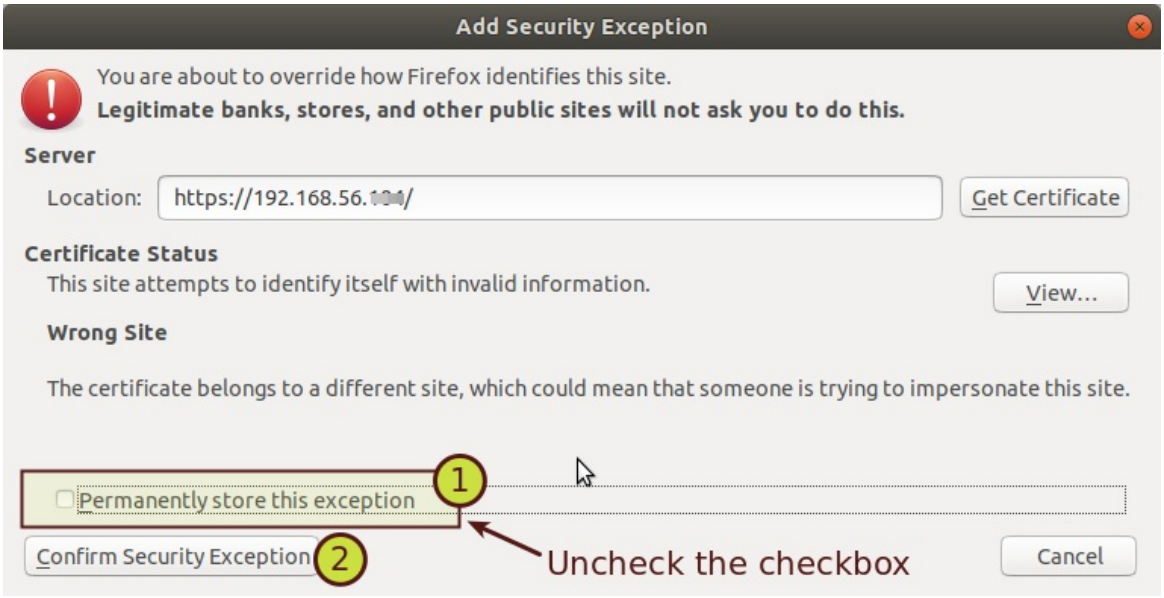


8. This time the error is not "SEC_ERROR_UNKNOWN_ISSUER", but it is "SSL_ERROR_BAD_CERT_DOMAIN" instead.

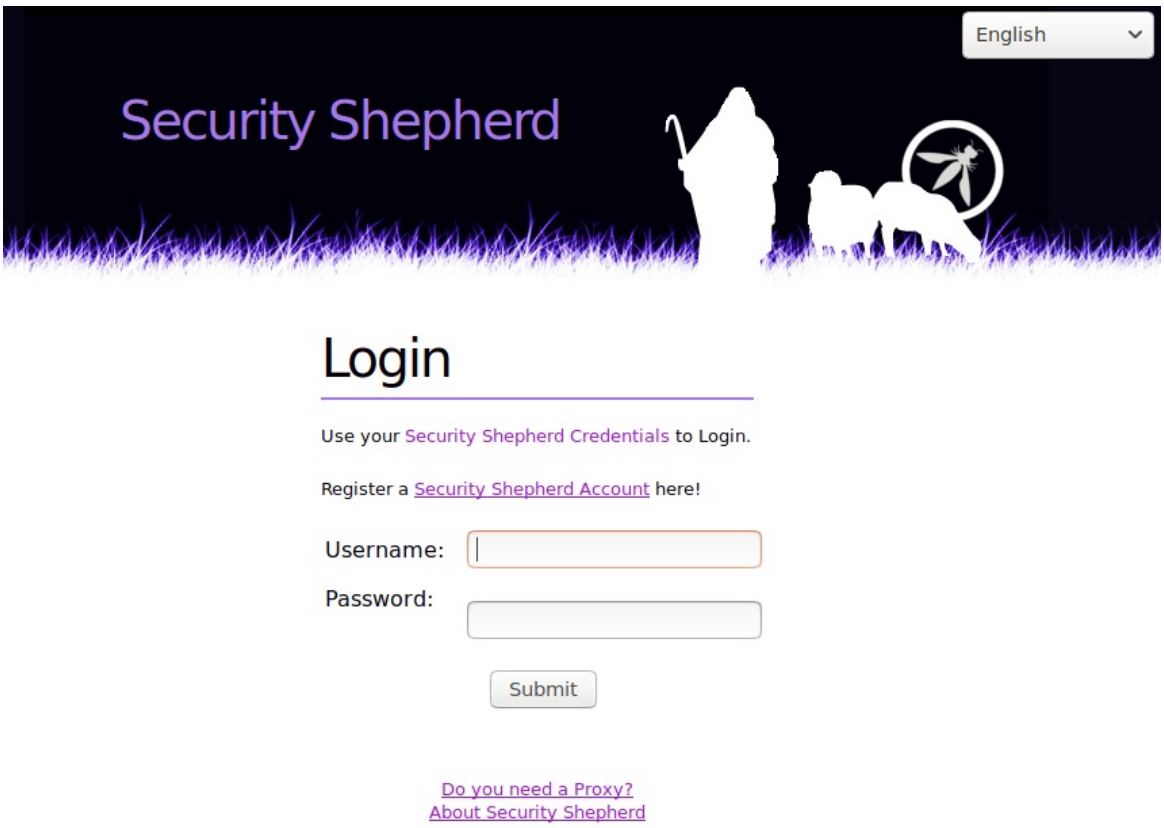
9. Click on "Add Exception" button.



10. Uncheck the "Permanently store this exception" checkbox, and click on "Confirm Security Exception" button.

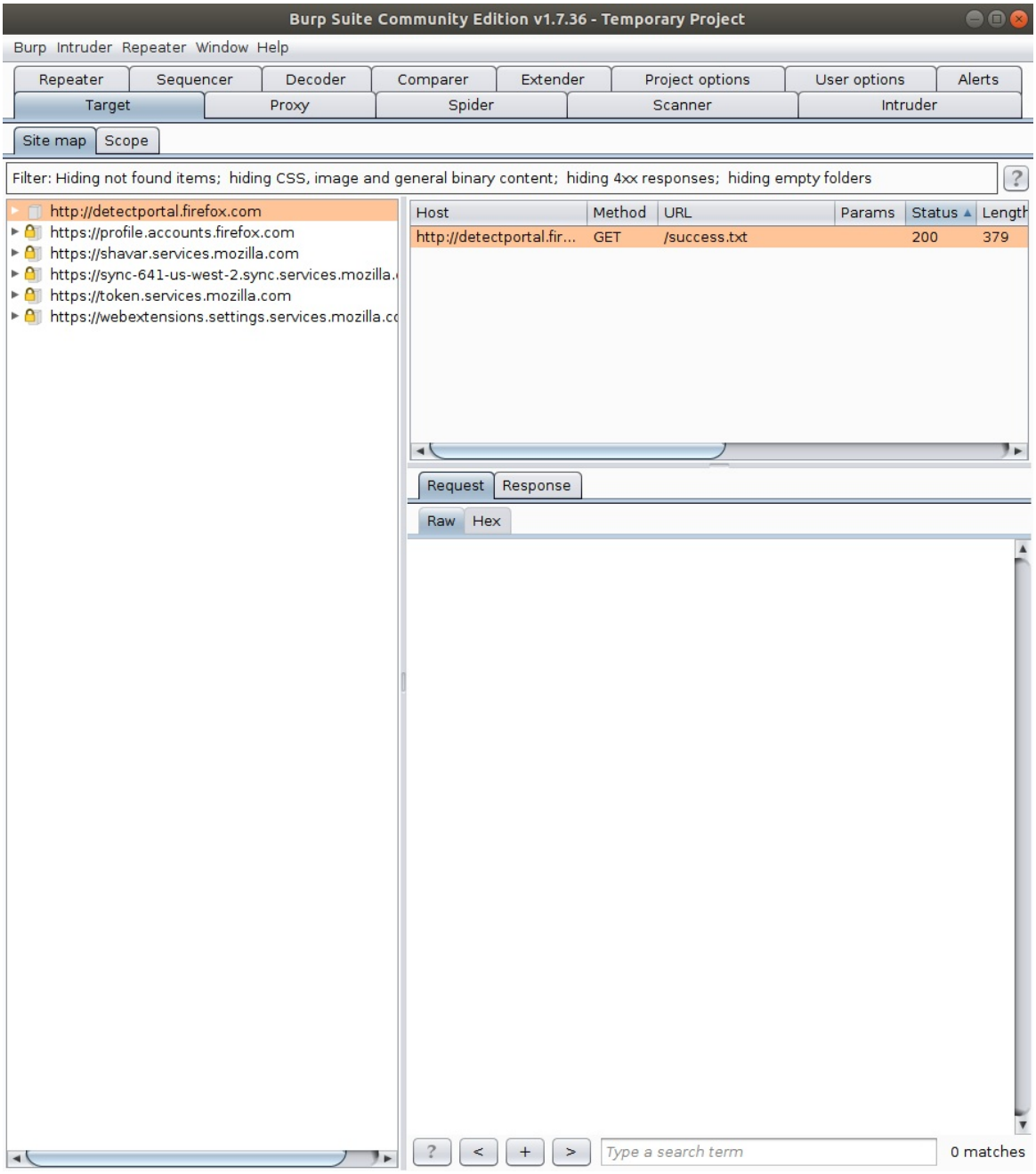


11. You should see the login page of Security Shepherd web application.



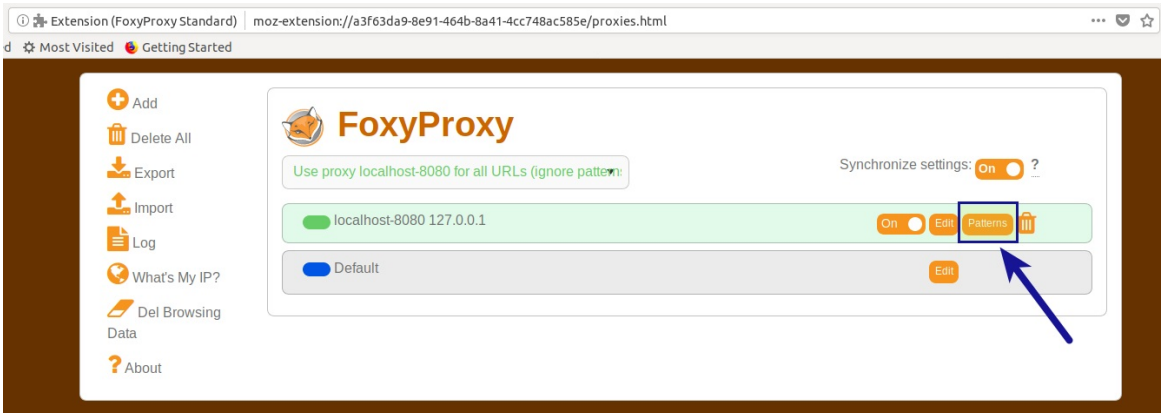
Getting Rid of Unnecessary Browser Traffic

1. In Burp, go to "Target" > "Site map" tab.
2. Do you see unnecessary traffic in your site map? Are they originating from Firefox browser itself? We need to get rid of these noise.



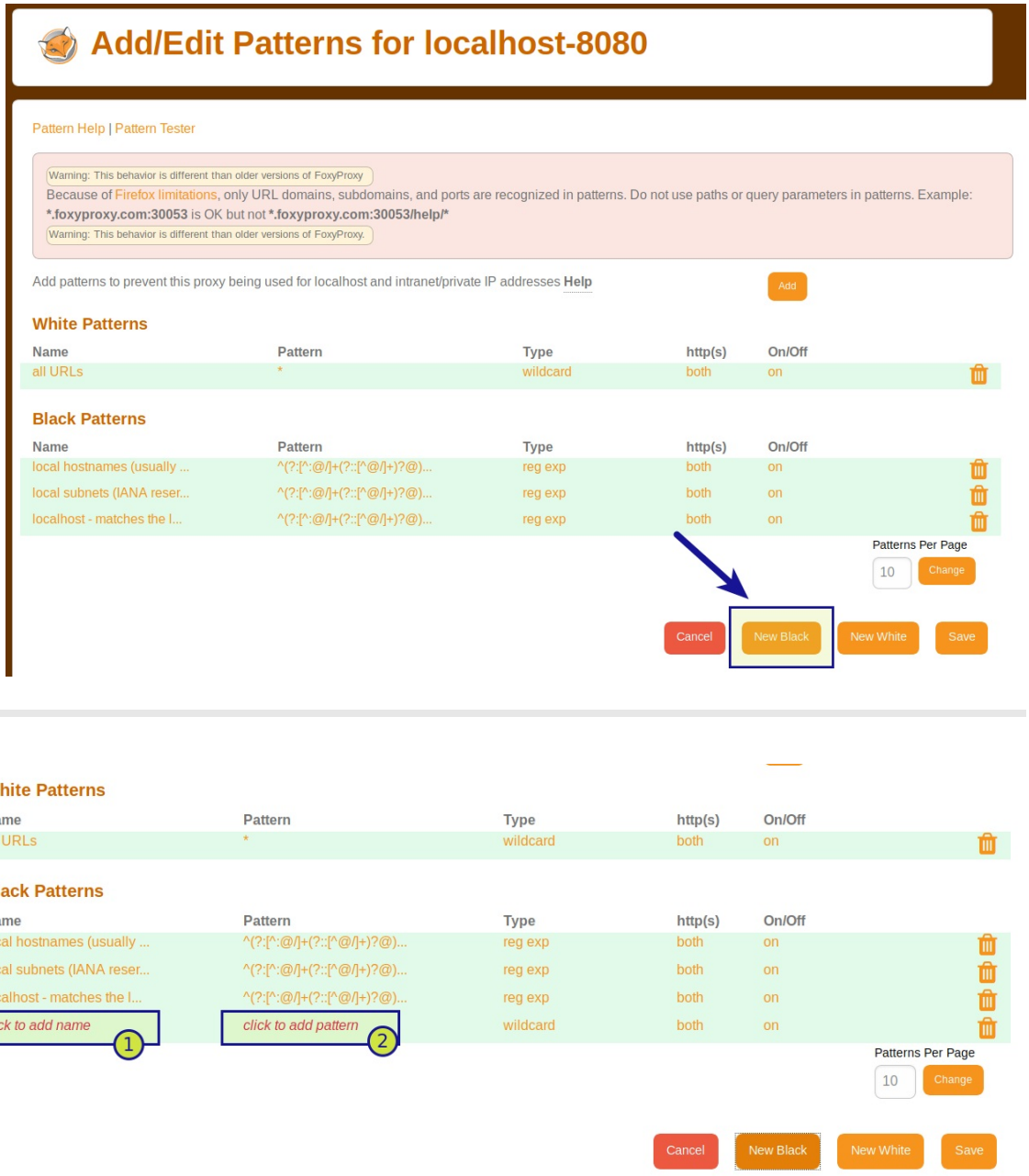
3. To disable capturing of unnecessary browser traffic, analyze the traffic in the "Site map" and identify URL patterns that need to be excluded. In the current scenario, we observe that most of the noise is originating from following two domains:
    - `firefox.com`
    - `mozilla.com`
4. In your Firefox browser, click on "FoxyProxy" icon and select "**Options**"

5. Choose the recently created proxy (named as, "localhost-8080") and click on "**Patterns**" button.

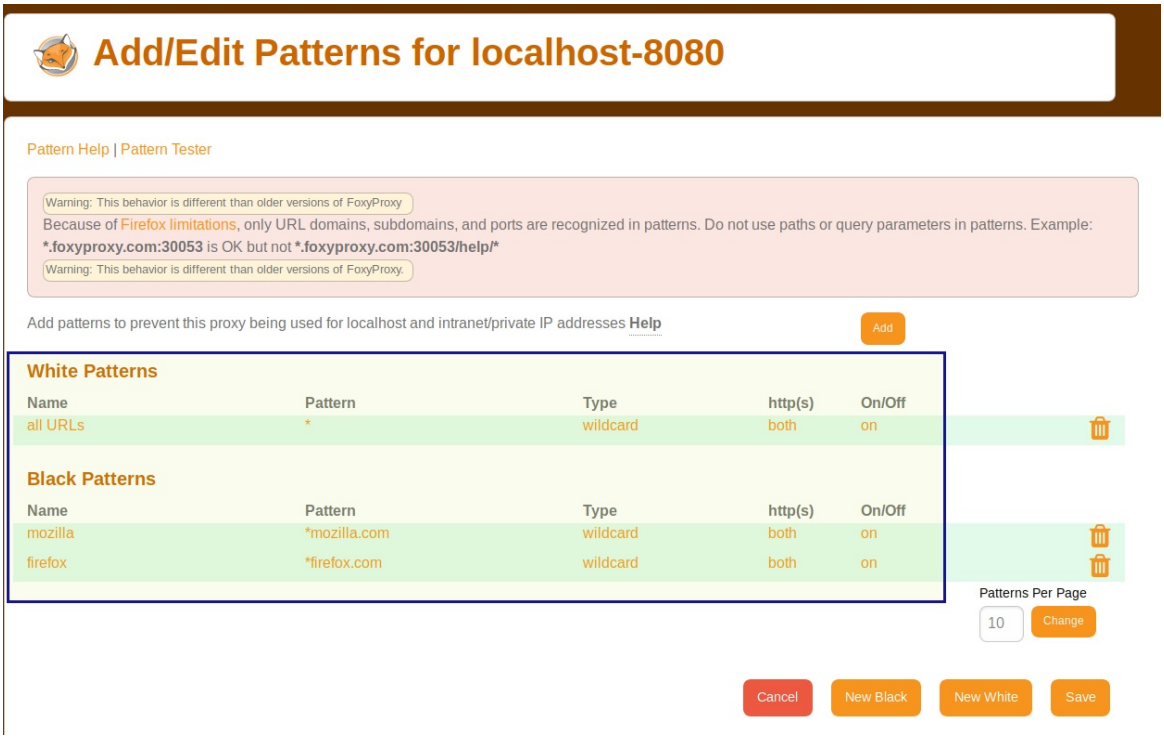


6. In the "Add/Edit Patterns for localhost-8080" window, click on "**New Black**" button, and edit the "Name" and "Pattern" fields as shown below:

   - **1st Black Pattern**:
     - Name: `firefox.com`
     - Pattern: `*.firefox.com`
   - **2nd Black Pattern**:
     - Name: `mozilla.com`
     - Pattern: `*.mozilla.com`

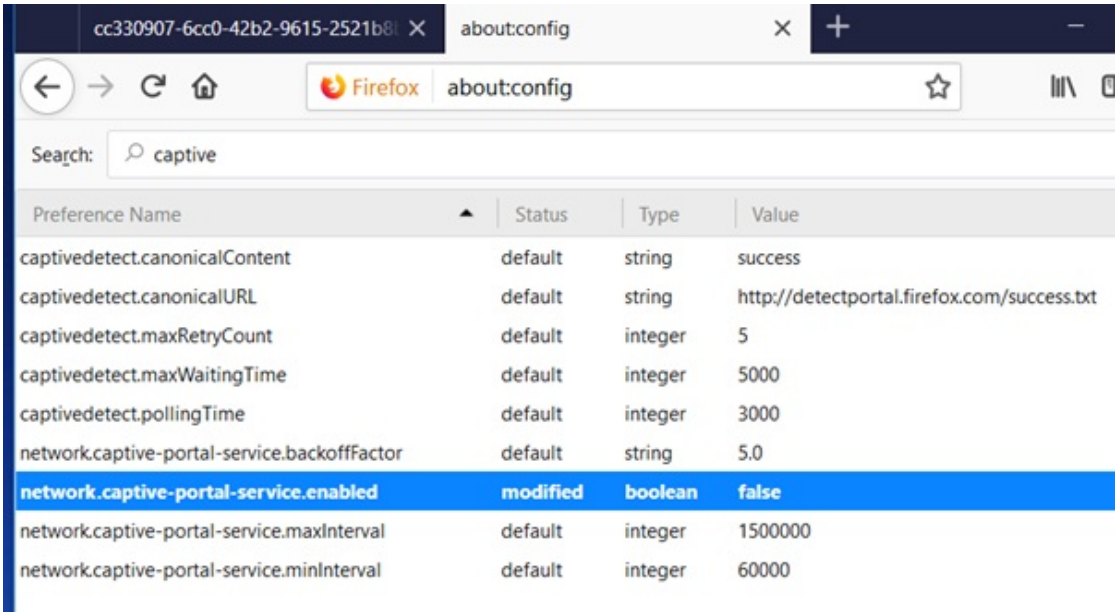


7. Delete the other (default) patterns listed under "Black Patterns". The final screen should look similar to:



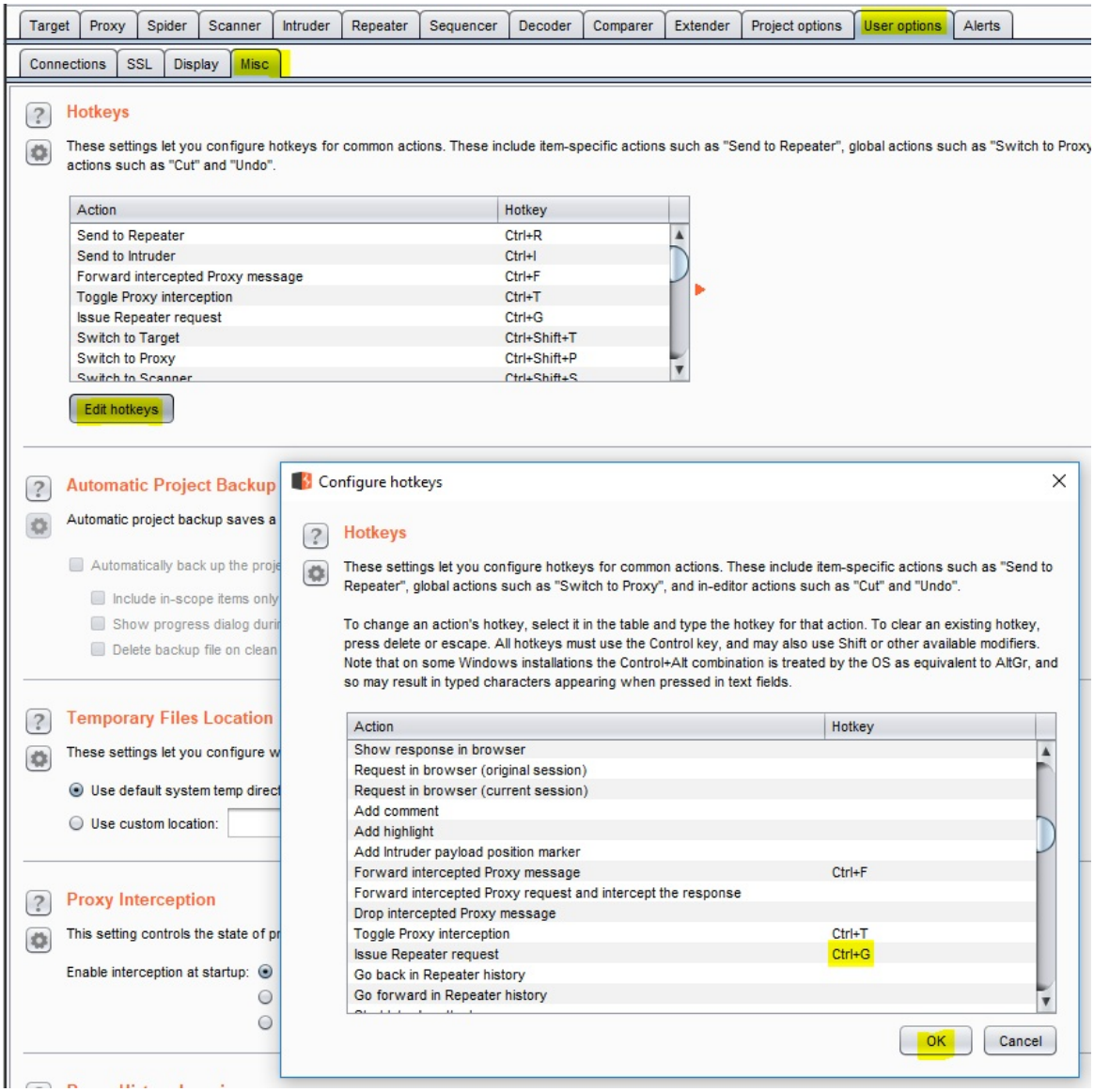
8. Click on "Save" button and select the option "**Use Enabled Proxies By Patterns and Priority**".

9. Access `about:config` in the address bar of your Firefox browser.
10. Disable following browser configuration by double-clicking on the respective preference name.
    - `network.captive-portal-service.enabled`


cc330907-6cc0-42b2-9615-2521b8
about:config
Firefox
about:config
Search:
captive
Preference Name
Status
Type
Value
captivedetect.canonicalContent
default
string
success
captivedetect.canonicalURL
default
string
http://detectportal.firefox.com/success.txt
captivedetect.maxRetryCount
default
integer
5
captivedetect.maxWaitingTime
default
integer
5000
captivedetect.pollingTime
default
integer
3000
network.captive-portal-service.backoffFactor
default
string
5.0
network.captive-portal-service.enabled
modified
boolean
false
network.captive-portal-service.maxInterval
default
integer
1500000
network.captive-portal-service.minInterval
default
integer
60000

Setup Hotkeys

1. In Burp, go to "User Options" > "Misc" tab.
2. Under "Hotkeys" section, click on the "Edit hotkeys" button.
3. Set shortcuts for triggereing actions in Burp.
4. Example:



Action	Hotkey
Send to Repeater	Ctrl+R
Send to Intruder	Ctrl+I
Send to Spider	
Do an active scan	
Do a passive scan	
Send to Comparer	Ctrl+Alt+C
Send request to Comparer	Ctrl+Alt+1
Send response to Comparer	Ctrl+Alt+2
Send to Decoder	Ctrl+E
Send to Sequencer	Ctrl+Q
Find references	Ctrl+3
Add to scope	
Remove from scope	
Discover content	Ctrl+4
Schedule task	
Generate CSRF PoC	
Copy URL	Ctrl+5
Copy as curl command	
Copy links	
Delete item(s)	
Save item(s)	
Save history	
Add to site map	
Show response in browser	Ctrl+6
Request in browser (original session)	Ctrl+7
Request in browser (current session)	Ctrl+8
Add comment	Ctrl+2
Add highlight	Ctrl+1
Add Intruder payload position marker	Ctrl+9
Forward intercepted Proxy message	Ctrl+F
Forward intercepted Proxy request and intercept the response	Ctrl+Alt+F
Drop intercepted Proxy message	Ctrl+Shift+Delete
Toggle Proxy interception	Ctrl+T
Issue Repeater request	Ctrl+G
Go back in Repeater history	Ctrl+Shift+G
Go forward in Repeater history	Ctrl+Alt+G
Start Intruder attack	Ctrl+K
Switch to Target	Ctrl+Shift+T
Switch to Proxy	Ctrl+Shift+P
Switch to Spider	

Action	Hotkey
Switch to Proxy	Ctrl+Shift+P
Switch to Spider	
Switch to Scanner	
Switch to Intruder	Ctrl+Shift+I
Switch to Repeater	Ctrl+Shift+R
Switch to Sequencer	Ctrl+Shift+Q
Switch to Decoder	Ctrl+Shift+E
Switch to Comparer	Ctrl+Shift+C
Switch to Project options	Ctrl+Shift+O
Switch to User options	Ctrl+Alt+U
Switch to Alerts tab	Ctrl+Shift+A
Go to previous tab	Ctrl+Minus
Go to next tab	Ctrl+Equals
Editor: Cut	Ctrl+X
Editor: Copy	Ctrl+C
Editor: Paste	Ctrl+V
Editor: Copy to file	
Editor: Paste from file	
Editor: Paste URL as request	
Editor: Undo	Ctrl+Z
Editor: Redo	Ctrl+Y
Editor: Select all	Ctrl+A
Editor: Search	Ctrl+S
Editor: Go to previous search match	Ctrl+Comma
Editor: Go to next search match	Ctrl+Period
Editor: Change request method	Ctrl+M
Editor: Change body encoding	
Editor: URL-decode	Ctrl+Shift+U
Editor: URL-encode key characters	Ctrl+U
Editor: URL-encode all characters	
Editor: URL-encode all characters (Unicode)	
Editor: Toggle URL-encoding as you type	
Editor: HTML-decode	Ctrl+Shift+H
Editor: HTML-encode key characters	Ctrl+H
Editor: HTML-encode all characters	
Editor: HTML-encode all characters (numeric entities)	
Editor: HTML-encode all characters (hex entities)	
Editor: Base64-decode	Ctrl+Shift+B
Editor: Base64-encode	Ctrl+B
Editor: Construct string in JavaScript	

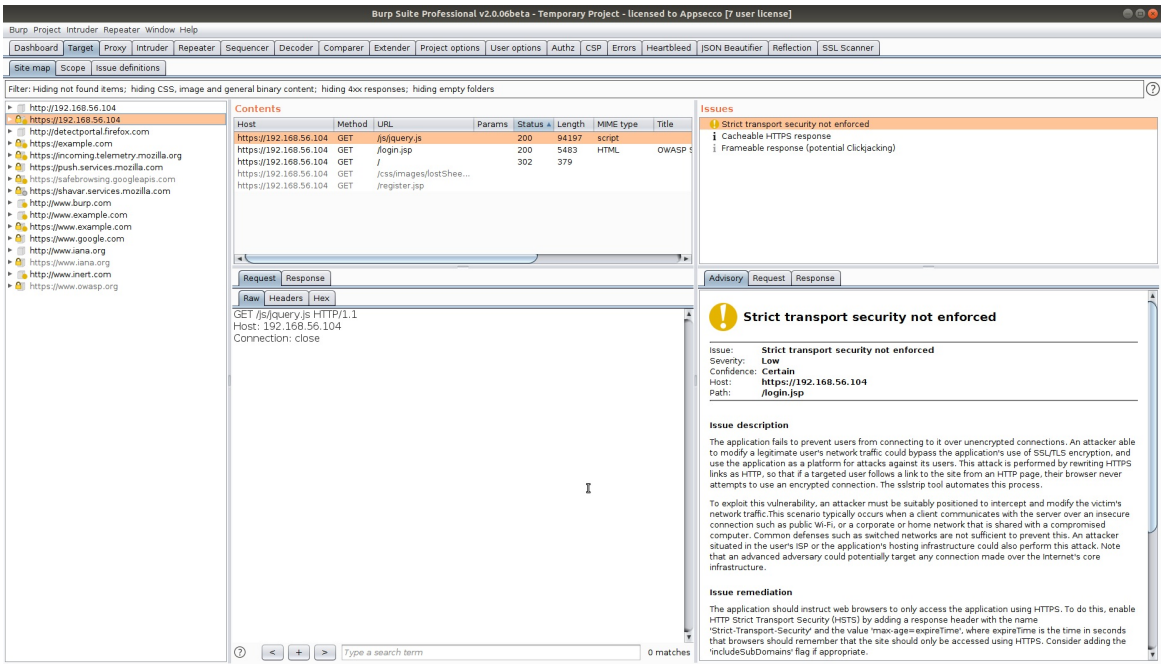
Editor: Base64-encode	Ctrl+B
Editor: Construct string in JavaScript	
Editor: Construct string in Microsoft SQL Server	
Editor: Construct string in Oracle	
Editor: Construct string in MySQL	
Editor: Backspace word	Ctrl+Backspace
Editor: Delete word	Ctrl+Delete
Editor: Delete line	Ctrl+D
Editor: Go to previous word	Ctrl+Left
Editor: Go to previous word (extend selection)	Ctrl+Shift+Left
Editor: Go to next word	Ctrl+Right
Editor: Go to next word (extend selection)	Ctrl+Shift+Right
Editor: Go to previous paragraph	Ctrl+Up
Editor: Go to previous paragraph (extend selection)	Ctrl+Shift+Up
Editor: Go to next paragraph	Ctrl+Down
Editor: Go to next paragraph (extend selection)	Ctrl+Shift+Down
Editor: Go to start of document	Ctrl+Home
Editor: Go to start of document (extend selection)	Ctrl+Shift+Home
Editor: Go to end of document	Ctrl+End
Editor: Go to end of document (extend selection)	Ctrl+Shift+End

Target (15 Minutes)

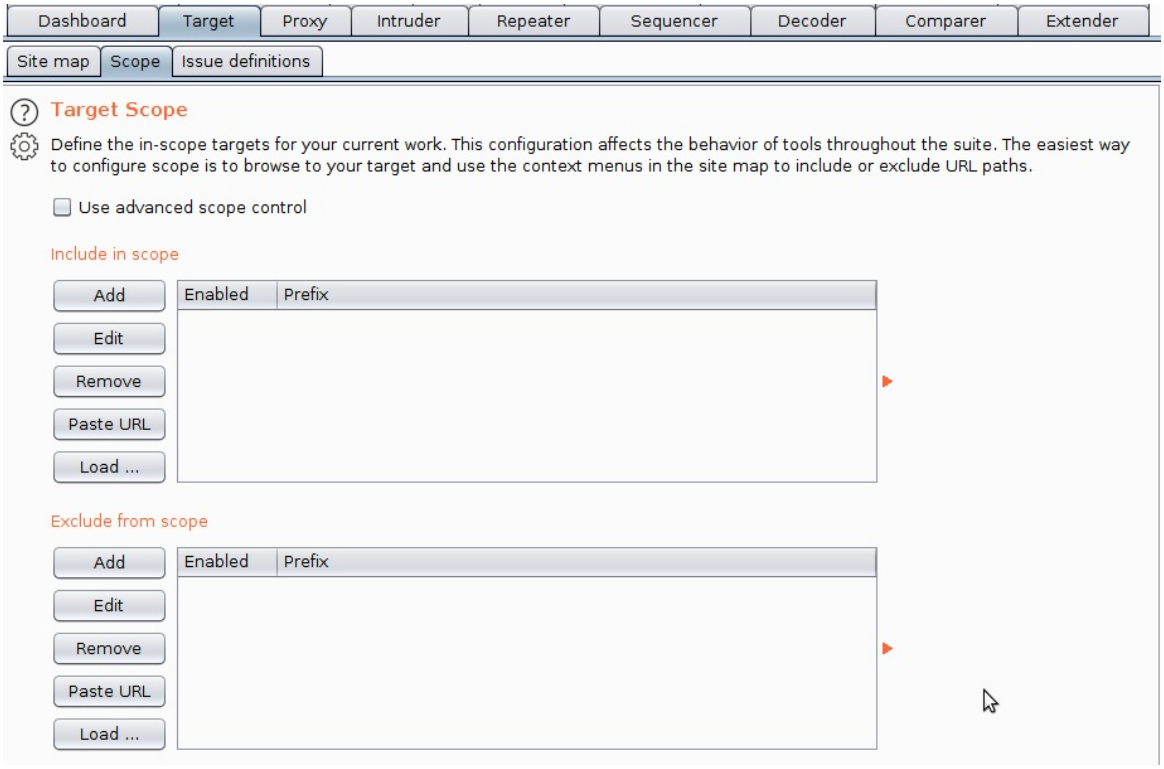
This tool contains detailed information about your target applications, and lets you drive the process of testing for vulnerabilities.

Site map

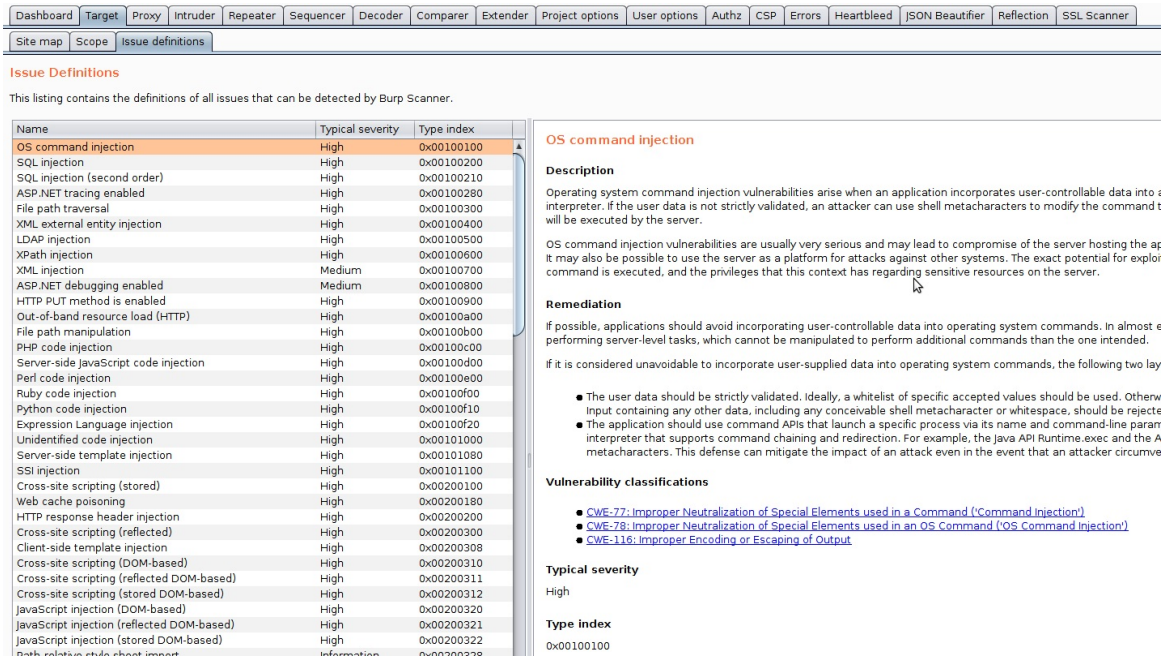
1. In Burp, go to "Target" > "Site map" tab, and get familiar with the user interface.



2. Switch to "Target" > "Scope" tab.

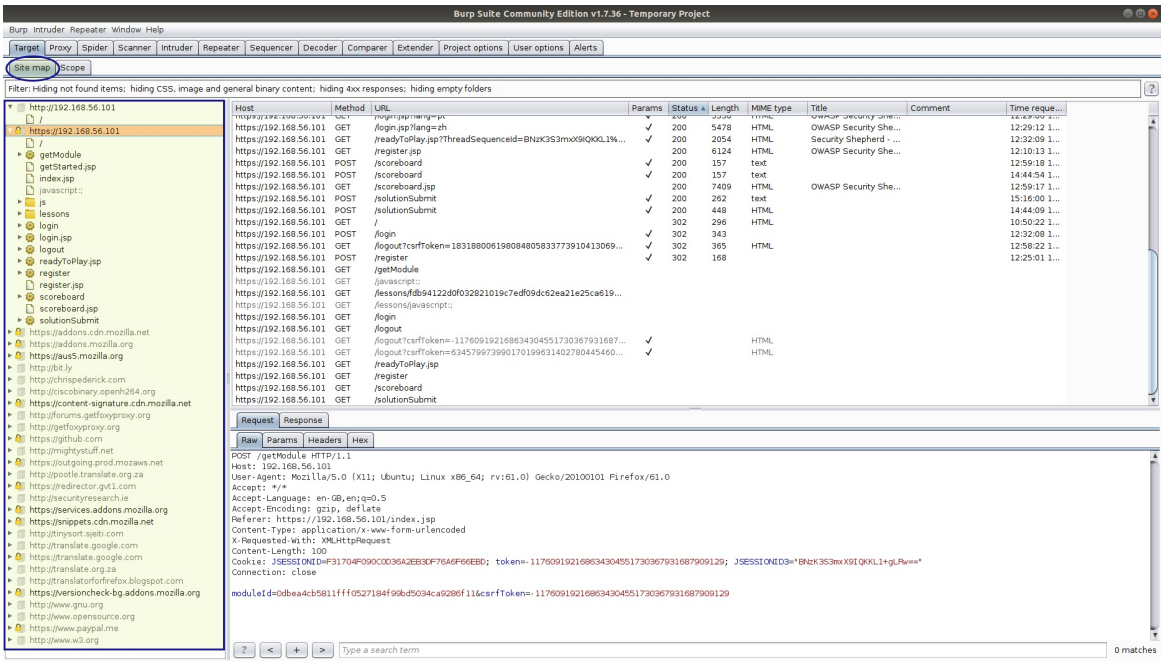


3. Switch to "Target" > "Issue definitions" tab.



4. In Firefox, explore the Security Shepherd web application by following links and submitting forms.

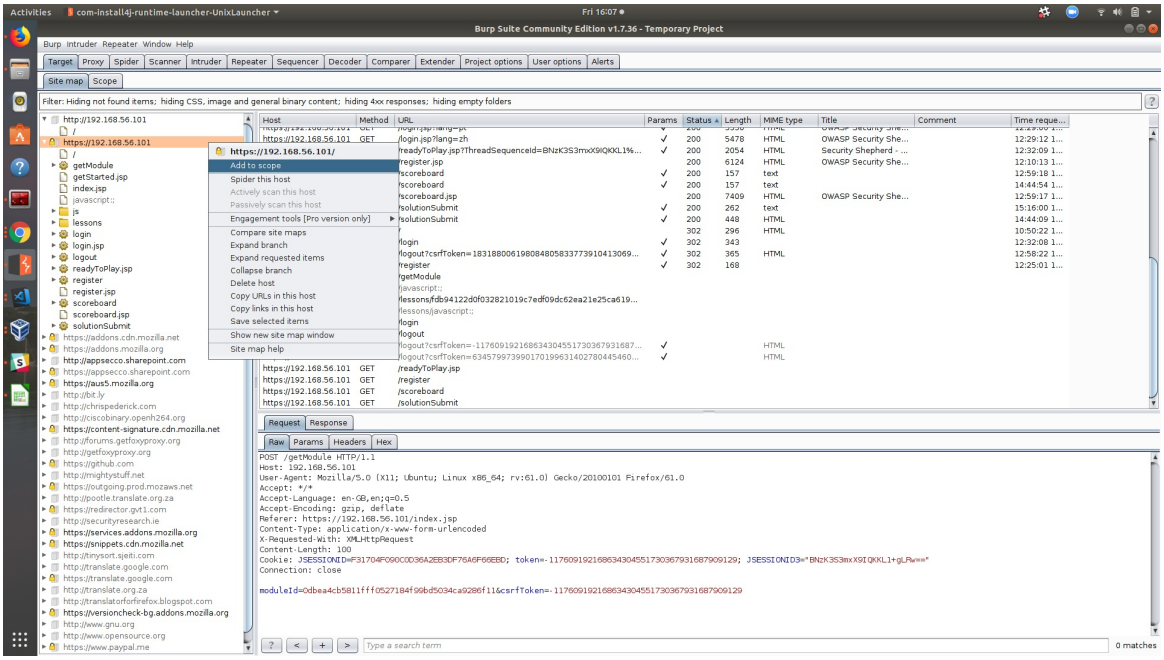
5. Observe the site map getting populated with URLs as you explore the target website. In site map, the items that have been manually requested in browser appear in **black**, while other items appear in **gray**.



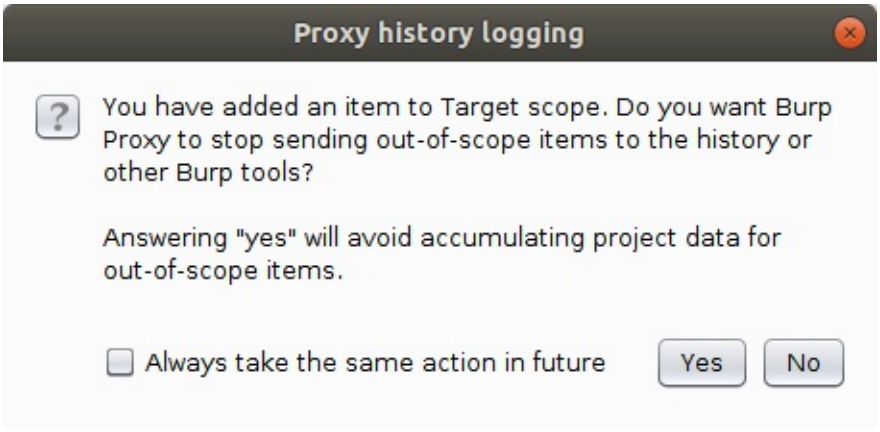
Scope

1. Select a URL in the "Target" > "Site map" tab.

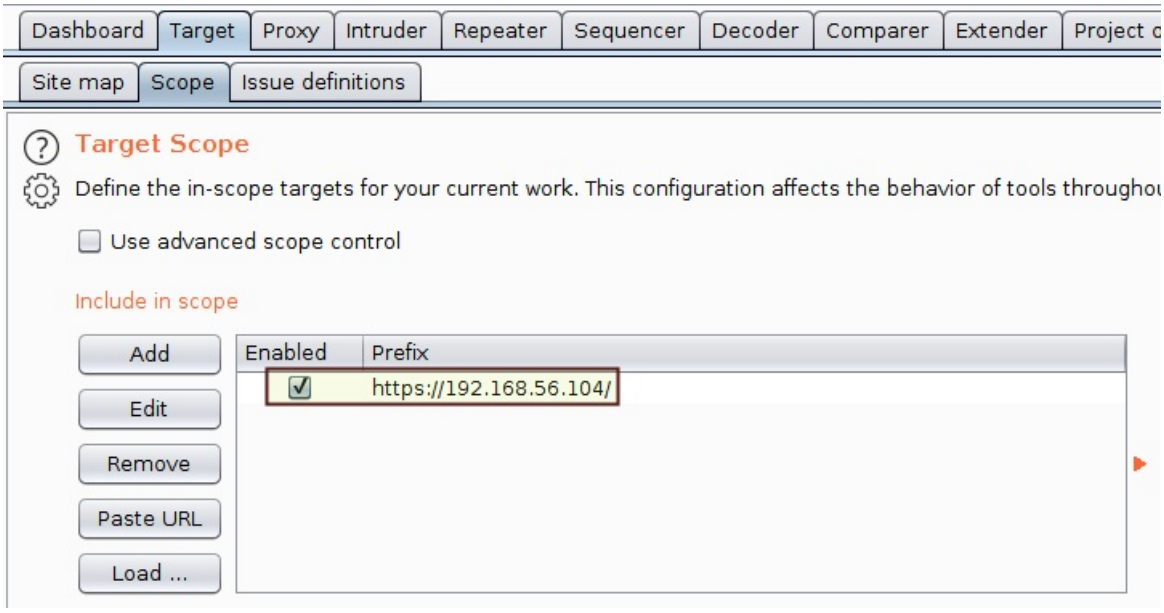
2. Right click on the chosen URL and select "**Add to scope**" option from the context menu.



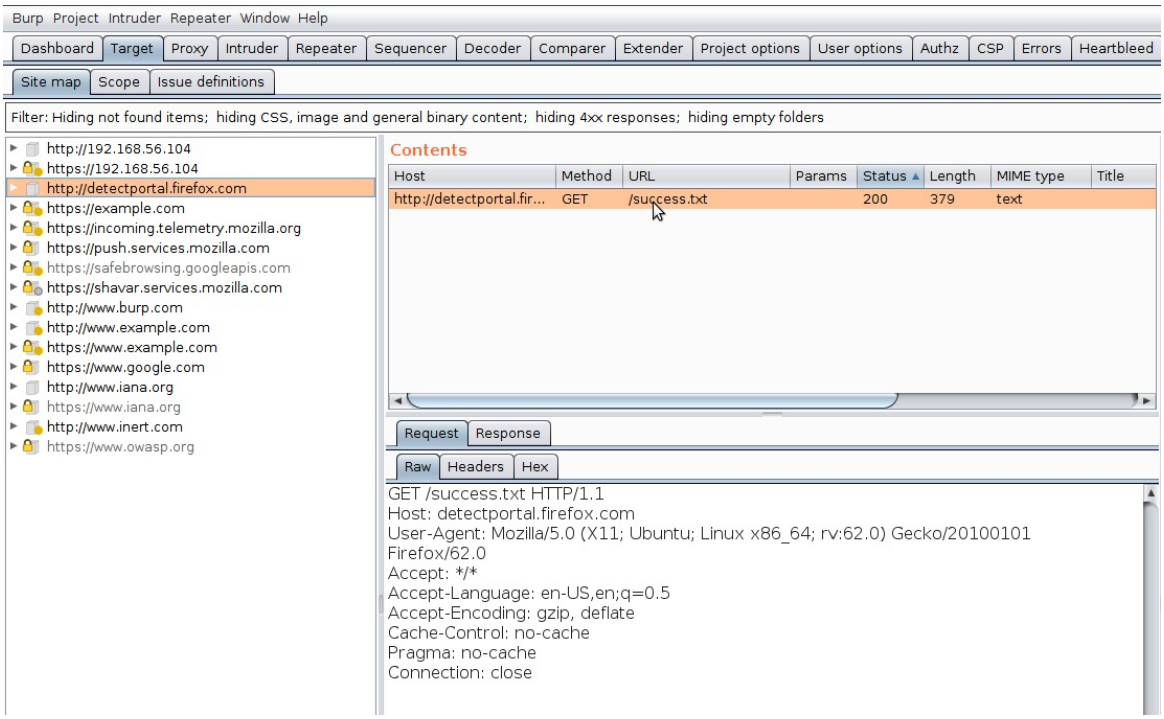
3. Select "**No**" in the "Proxy history logging" prompt. This is because we want to see all requests (in or out of scope) that are made while accessing the target web application.



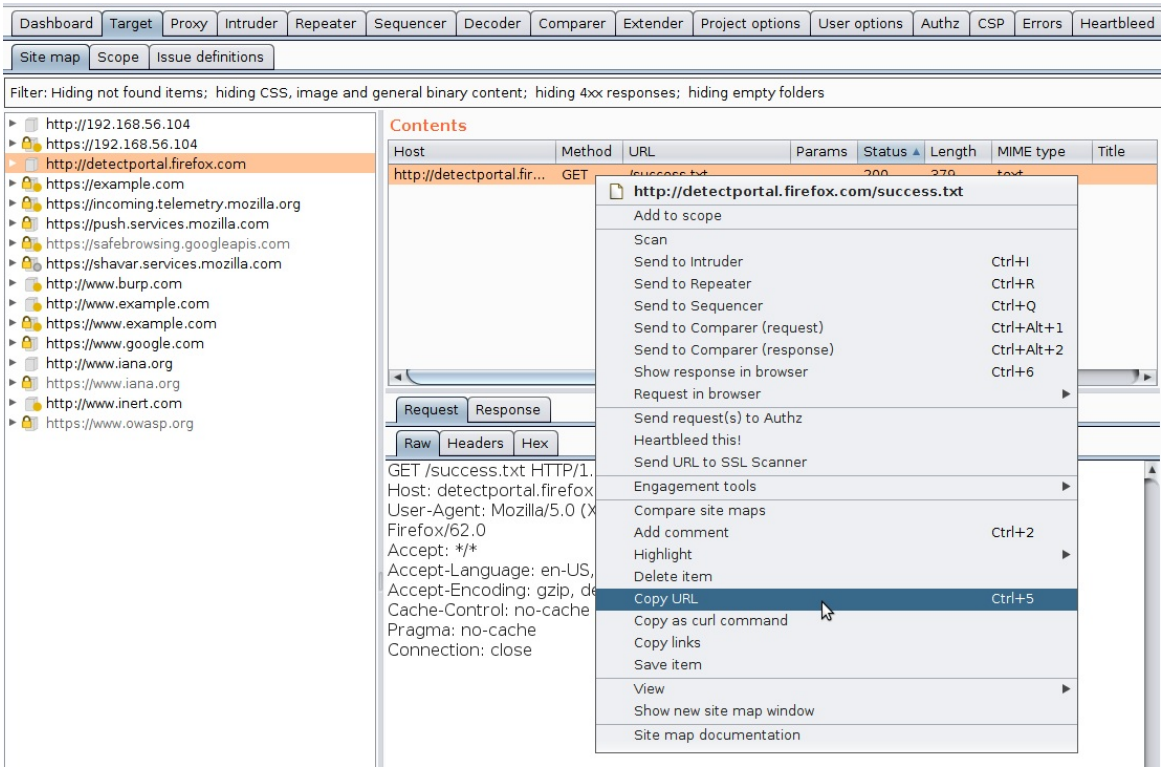
4. Go to "Target" > "Scope" tab to verify if the chosen URL was included in scope.



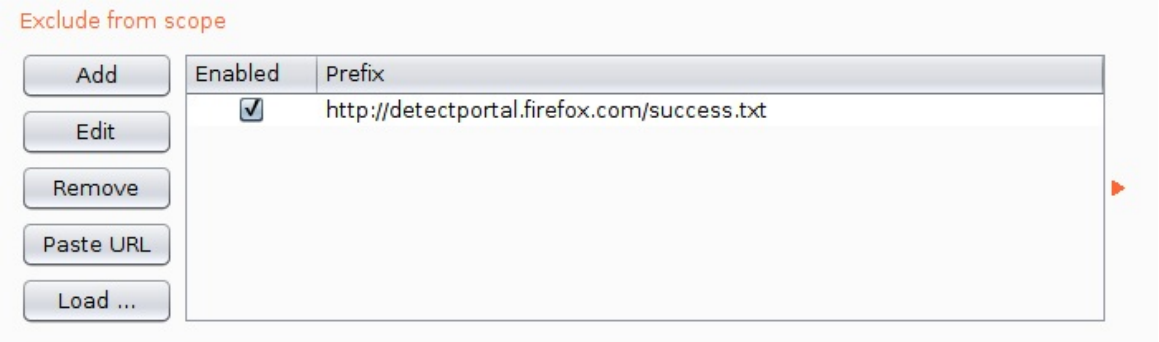
5. Return to "Target" > "Site map" tab, and select a different URL in the "Contents" section.



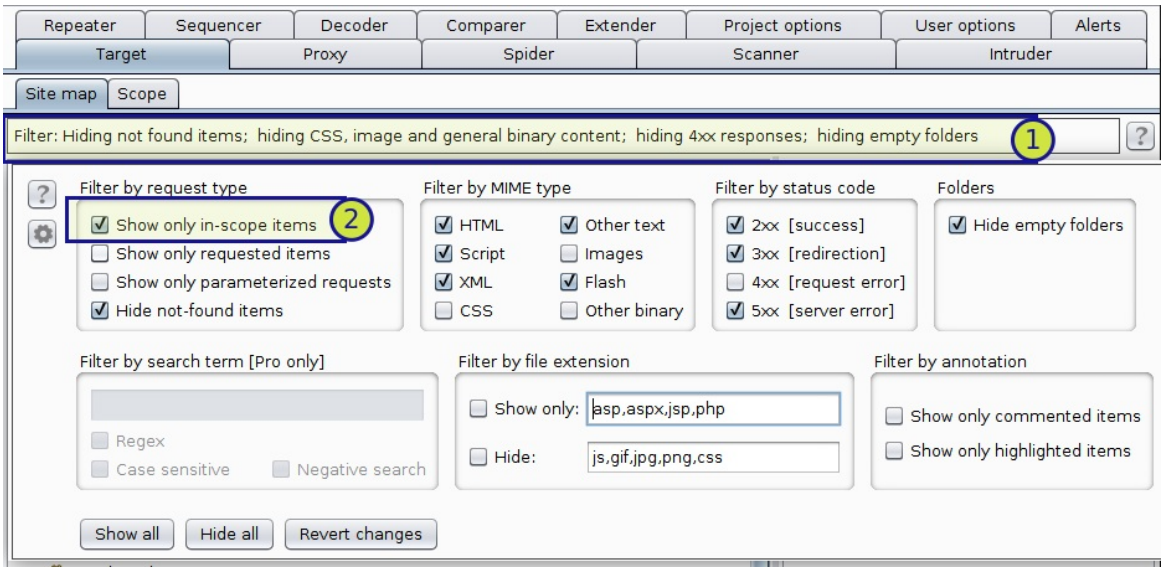
6. Right click on the chosen URL and select "**Copy URL**" option from the context menu.



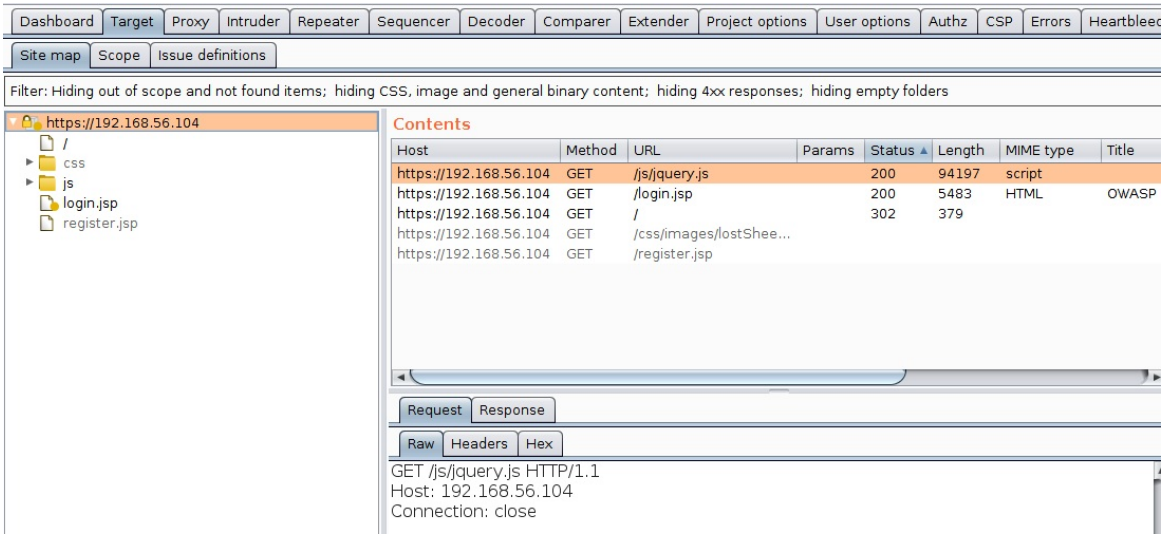
7. Go to "Target" > "Scope" tab, and click on "Paste URL" button under the "Exclude from scope" section.



8. You could, now, configure suitable **display filters** on the site map and Proxy history tabs, to hide from view items that you are not currently interested in.
9. Go to "Target" > "Site map" tab.
10. Click on the `Filter` bar.
11. Select the checkbox labeled as `Show only in-scope items`.
12. Click anywhere outside of the filter-box.



13. Only in-scope items should be visible in the site map, now.

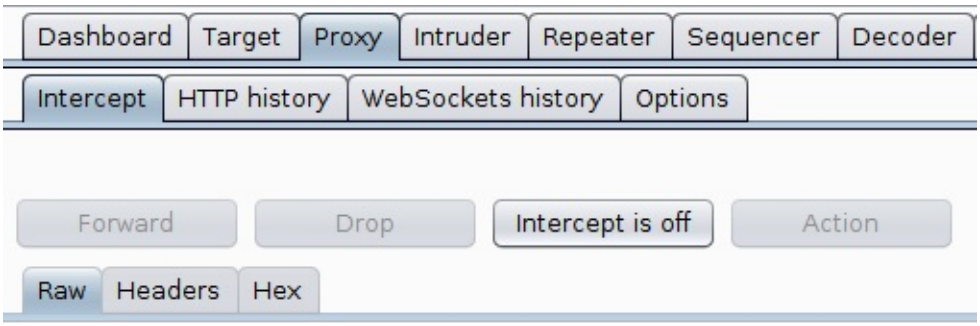


Proxy (30 Minutes)

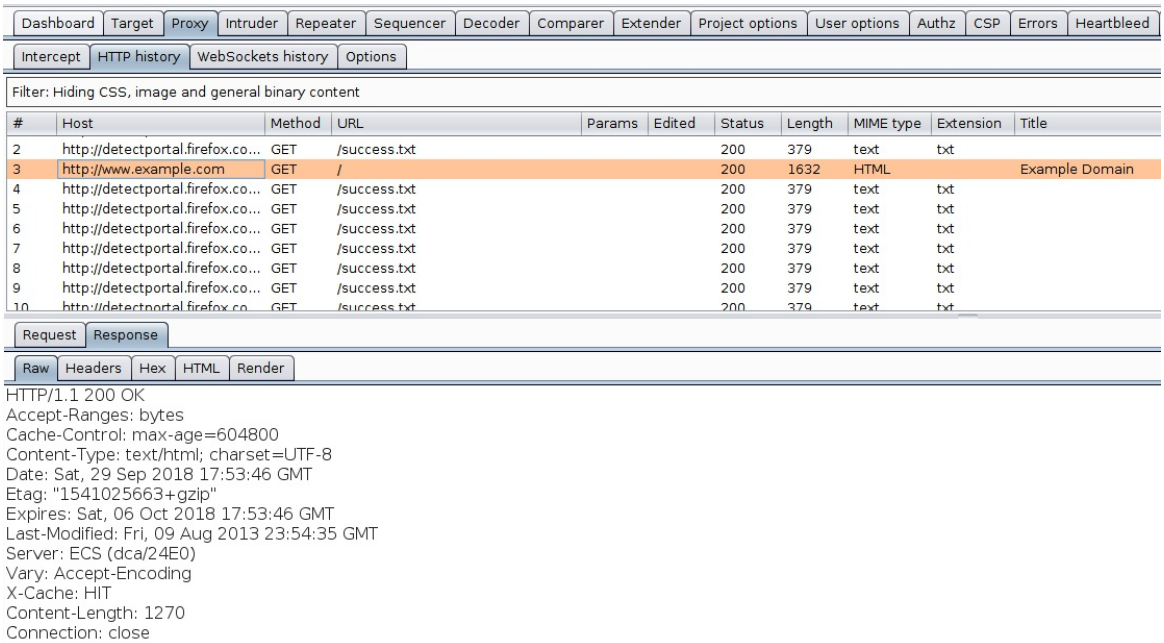
This is an intercepting web proxy that operates as a man-in-the-middle between the end browser and the target web application. It lets you intercept, inspect and modify the raw traffic passing in both directions.

Intercept

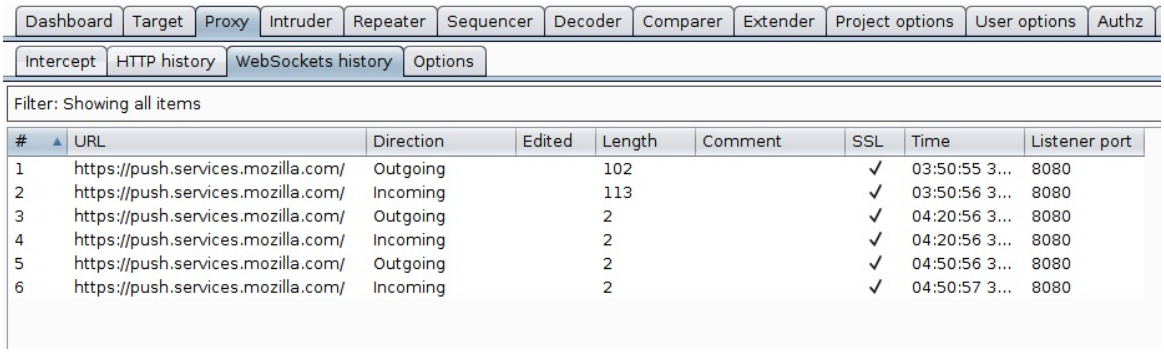
1. In Burp, go to "Proxy" > "Intercept" tab, and get familiar with the user interface.



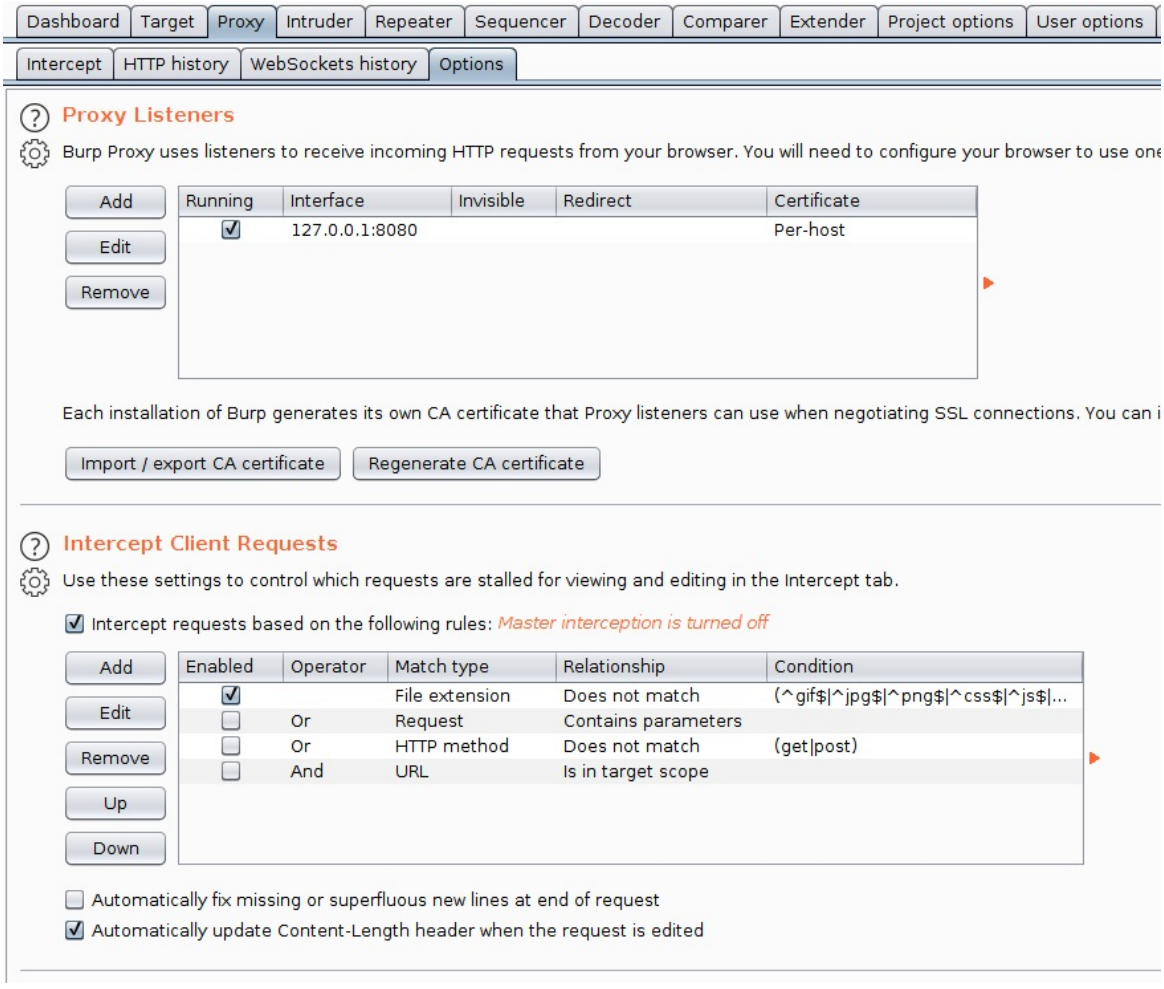
2. Switch to "Proxy" > "HTTP history" tab.



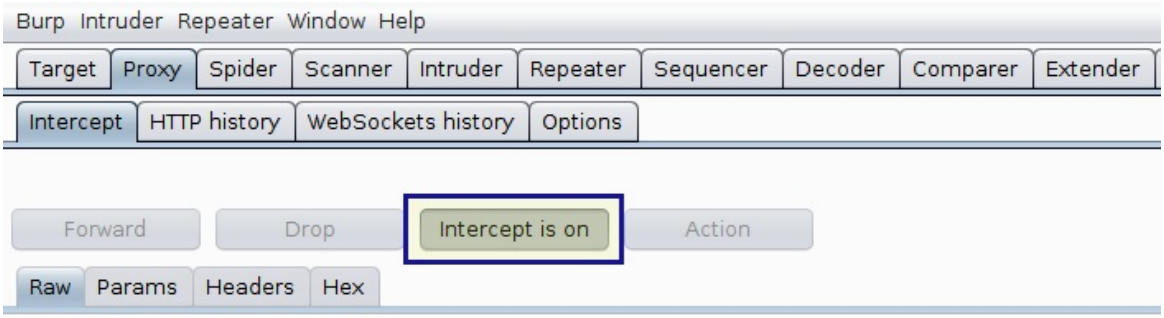
3. Switch to "Proxy" > "Websockets history" tab.



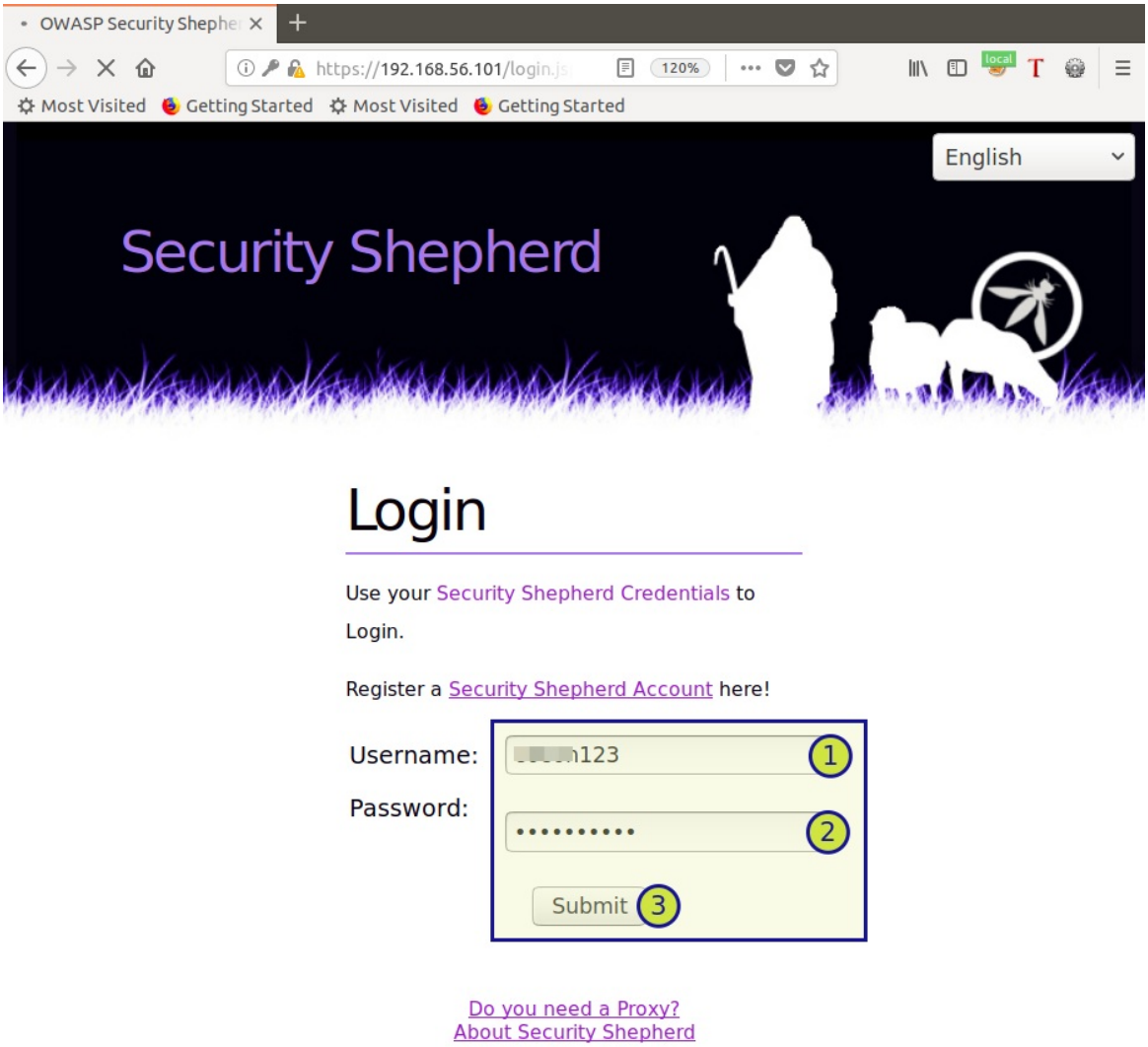
4. Switch to "Proxy" > "Options" tab, and look at the different options available.



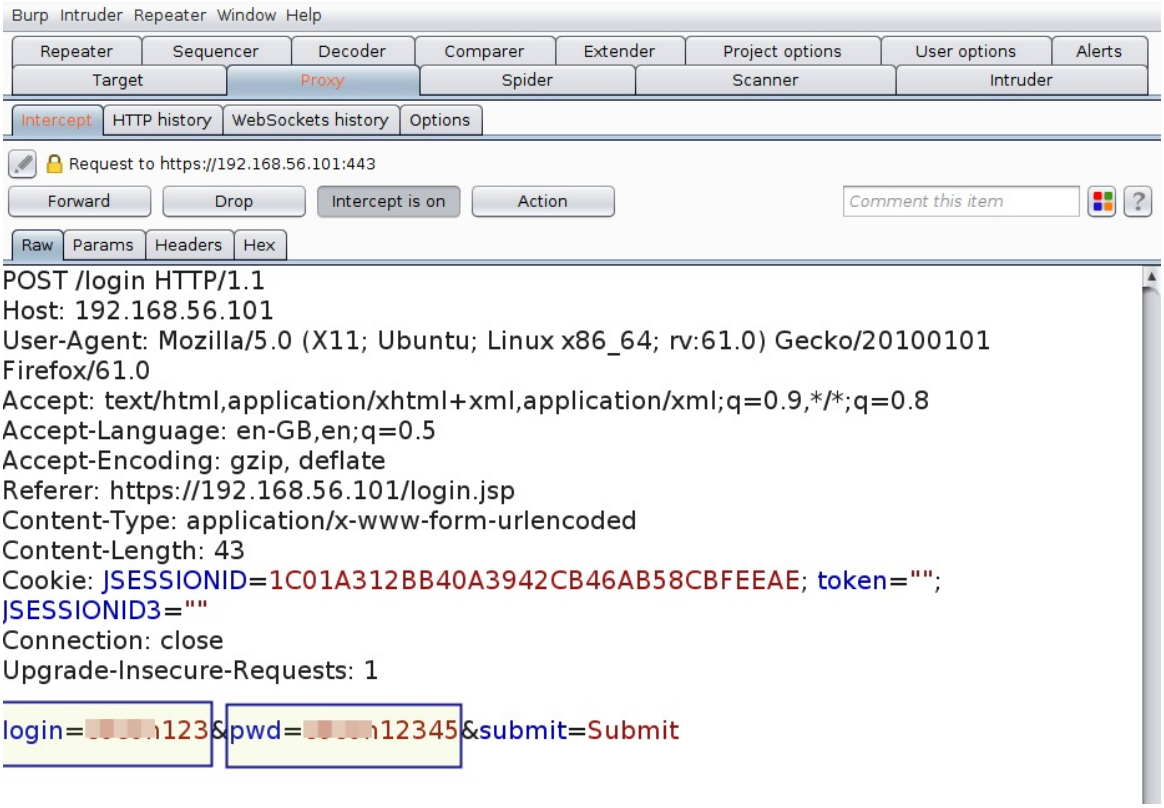
5. In Burp, go to "Proxy" > "Intercept" tab, and ensure that interception mode is turned **on**. If the intercept control button says "Intercept is off", then click on it to toggle the interception status.



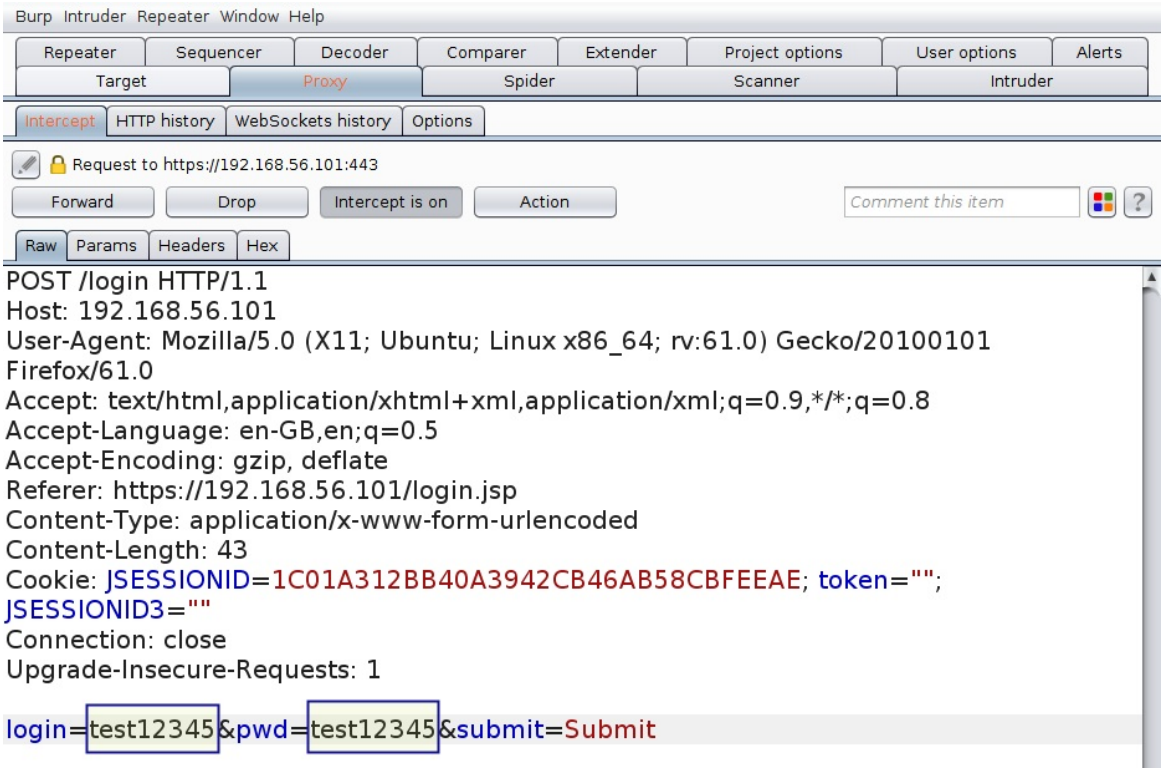
6. With the intercept mode enabled in Burp Suite, fill and submit the login form of the Security Shepherd application.



7. Switch to "Proxy" > "Intercept" tab and observe that the submitted request has been intercepted. At this point, it is possible to modify the request parameters before forwarding the request to the origin server.
8. Analyze the intercepted request, and observe the parameters passed in POST request body.

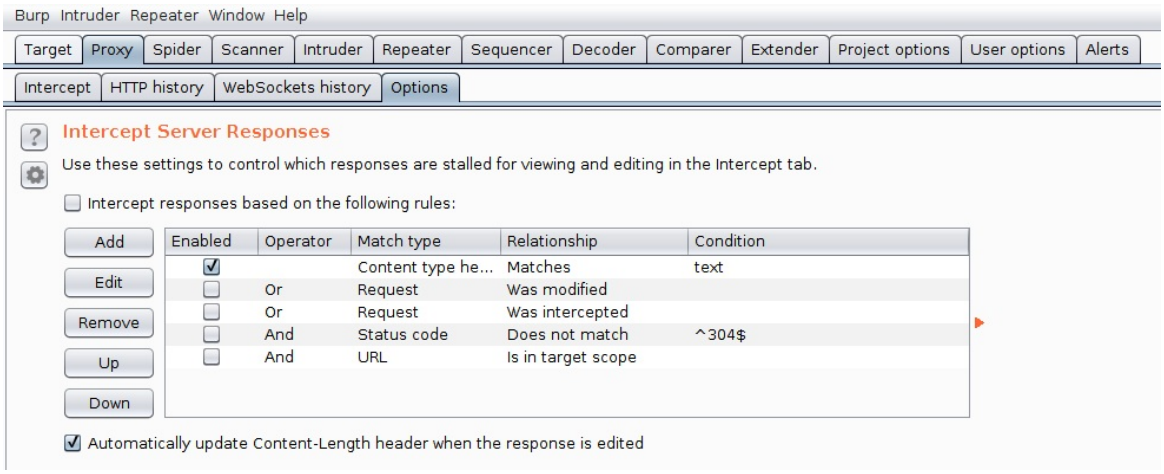


9. Tamper with the input parameters, i.e., change values for `login` and `pwd` parameters.

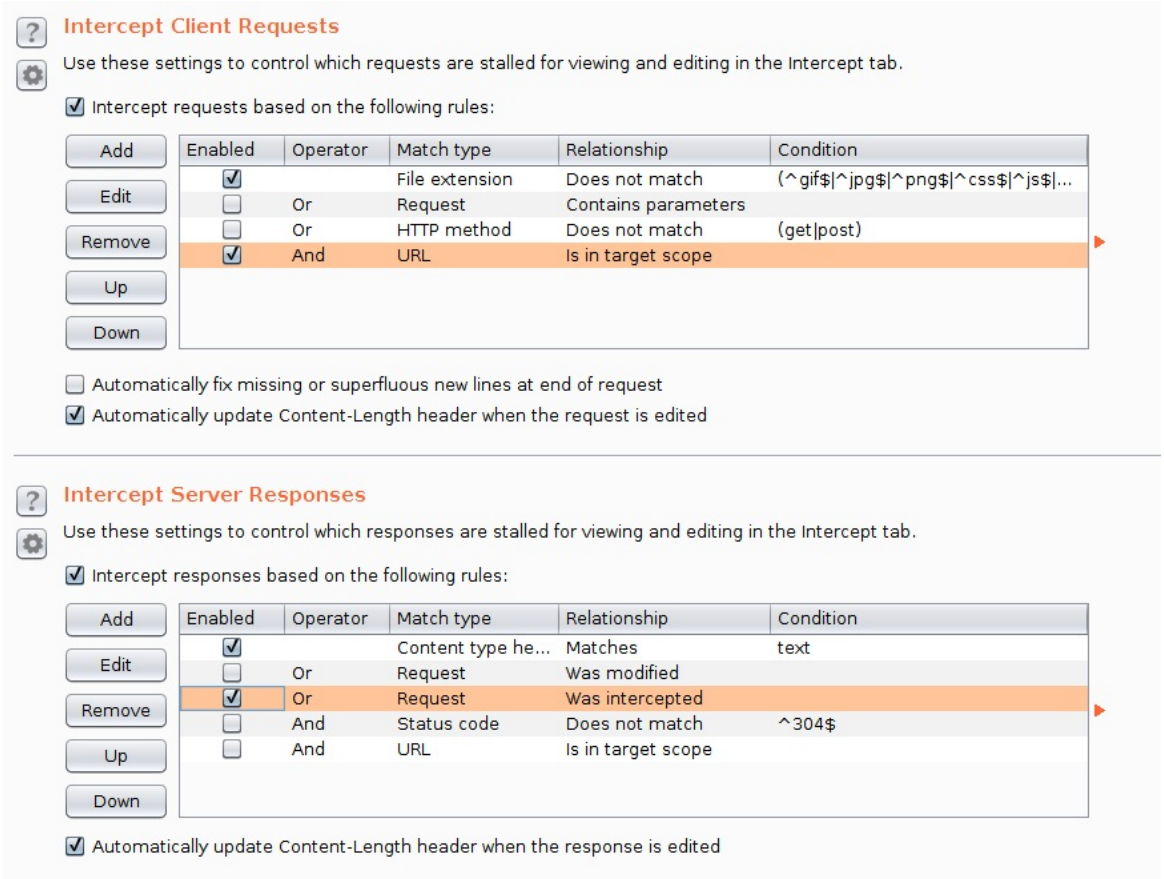


10. Click on "**Forward**" button, and analyze the next request.

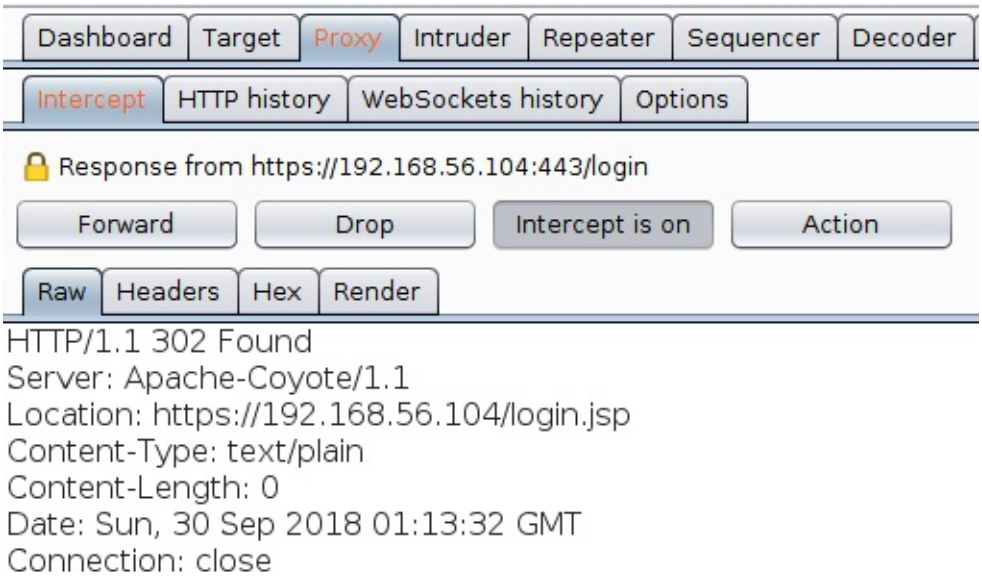
11. Go to "**Proxy**" tab > "**Options**" sub-tab > "**Intercept Server Responses**" section, and check the checkbox labelled as "**Intercept responses based on the following rules**".



12. For a smoother experience, add suitable interception rules for requests and responses. The following combination of request and response interception rules could be useful:



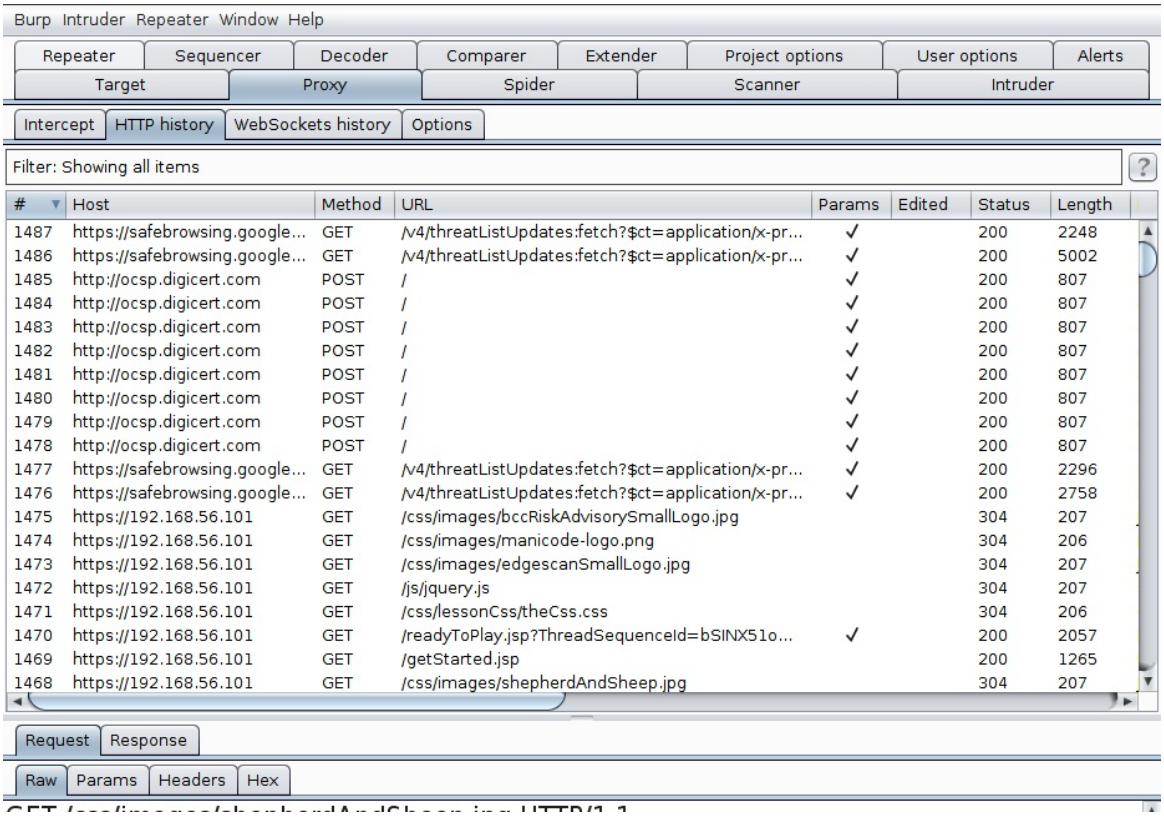
13. Switch to "Proxy" > "Intercept" tab and forward the intercepted request (from step-#10). This time, the server response should have been intercepted by the Burp interceptor.



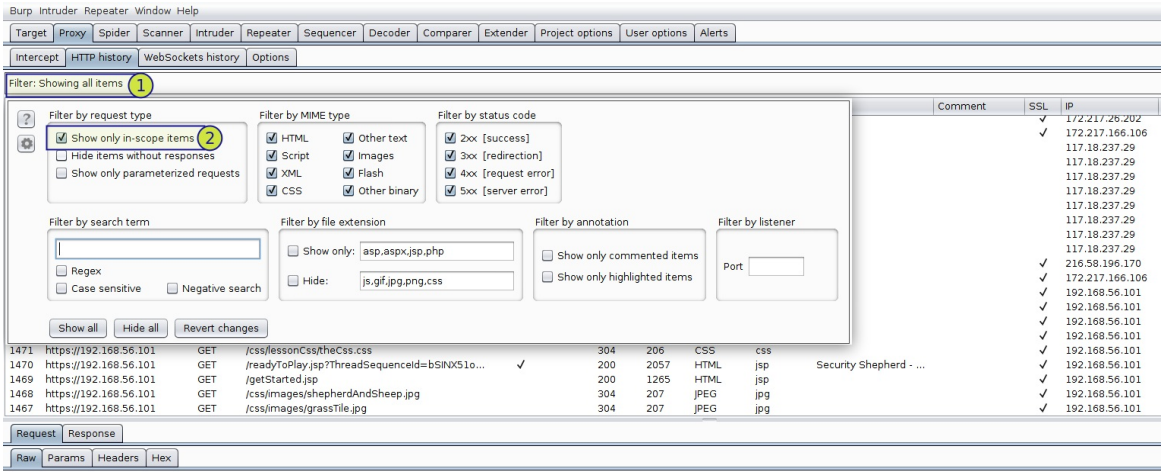
14. Click on "**Forward**" button, and analyze the next request/response. Repeat until there is no more request/response to forward. Alternatively, if you are done analyzing the request, turn interception mode off by clicking on the "Intercpet is on" button.

HTTP History

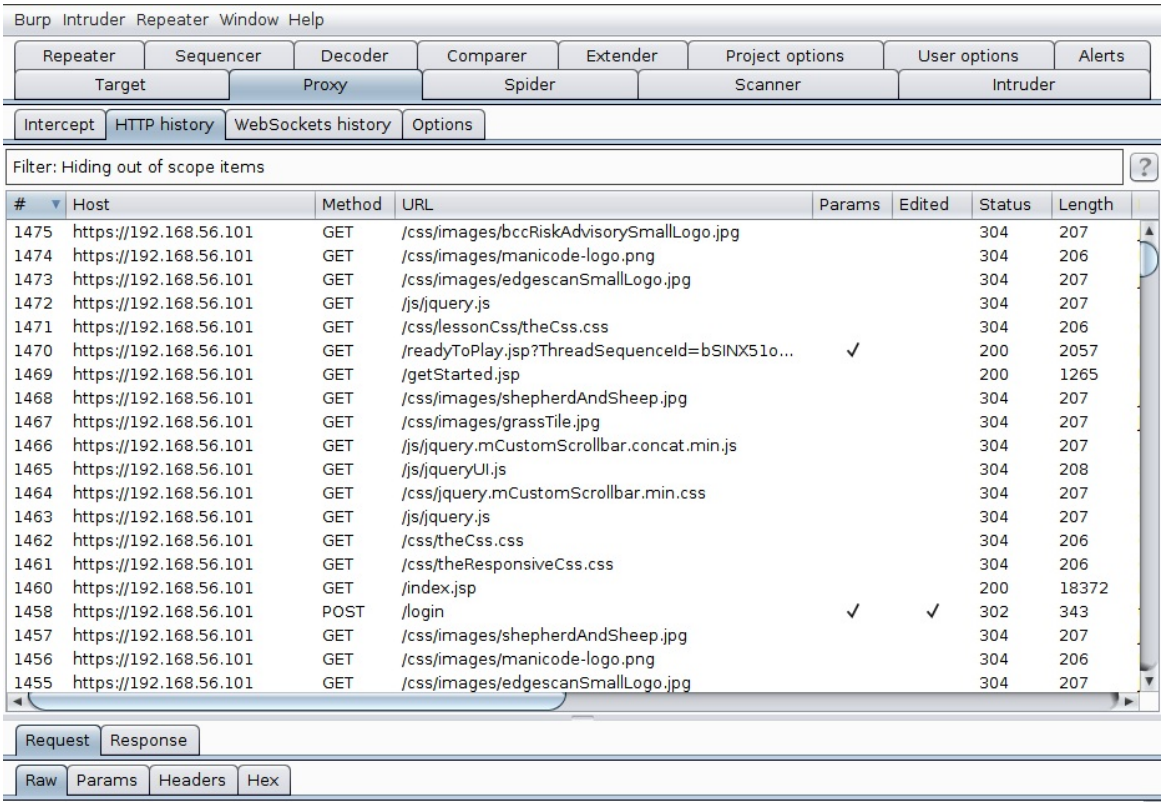
1. Navigate to "**Proxy**" tab > "**HTTP history**" sub-tab to see a full record of all messages that have been intercepted by the Burp Proxy.



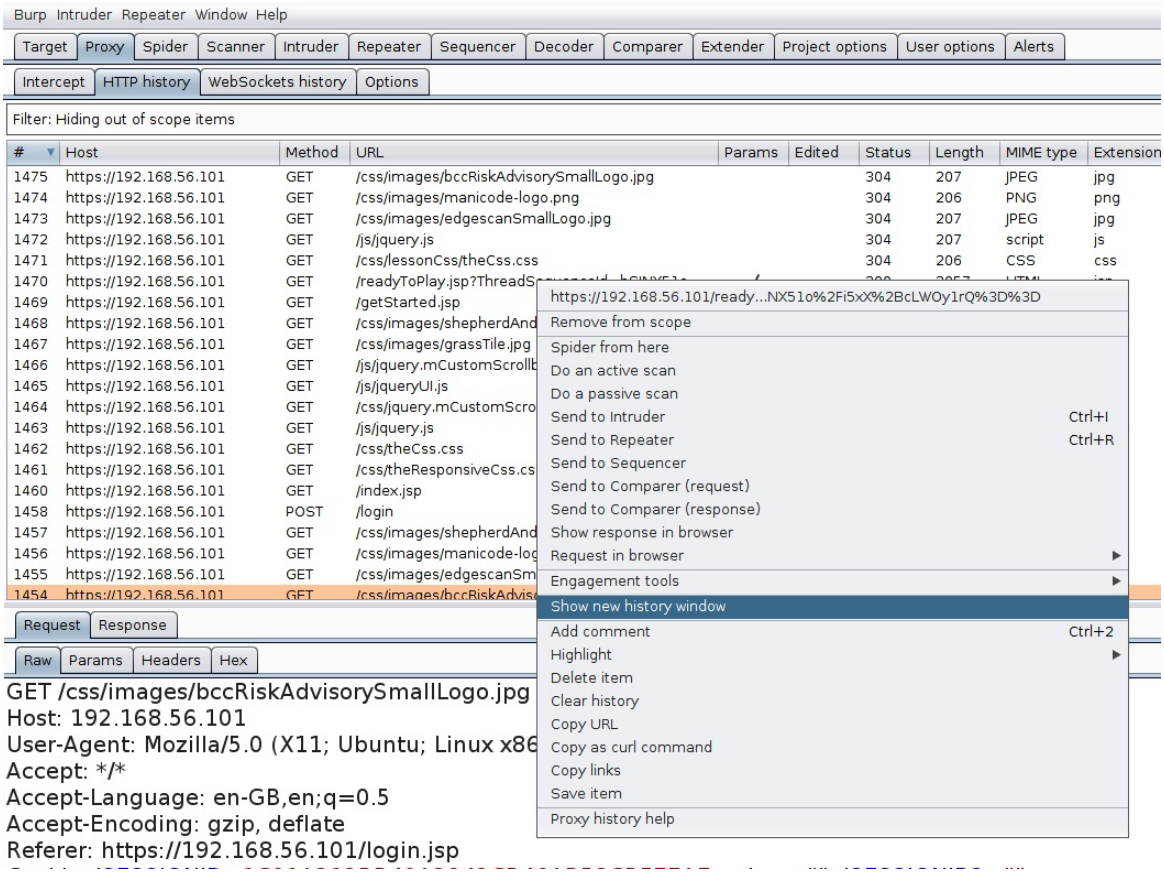
2. Click on the filter bar, above the history table, and select the checkbox labelled as "**Show only in-scope items**".



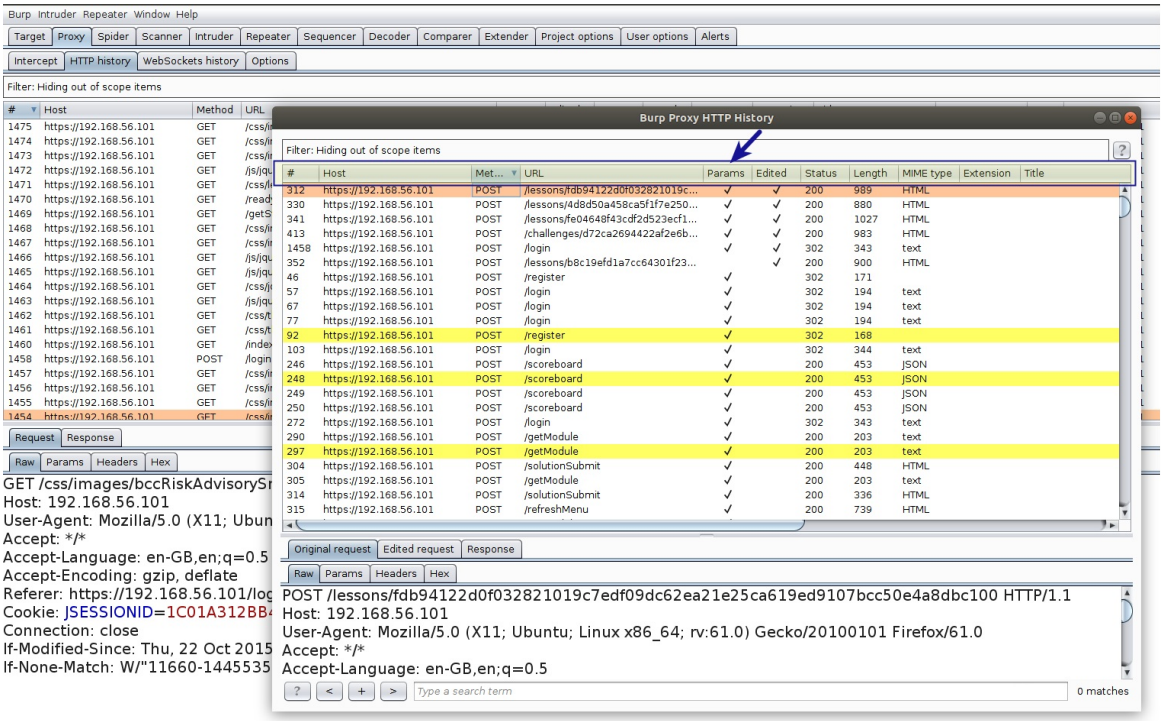
3. To apply the filter, click anywhere outside of the display filter form.



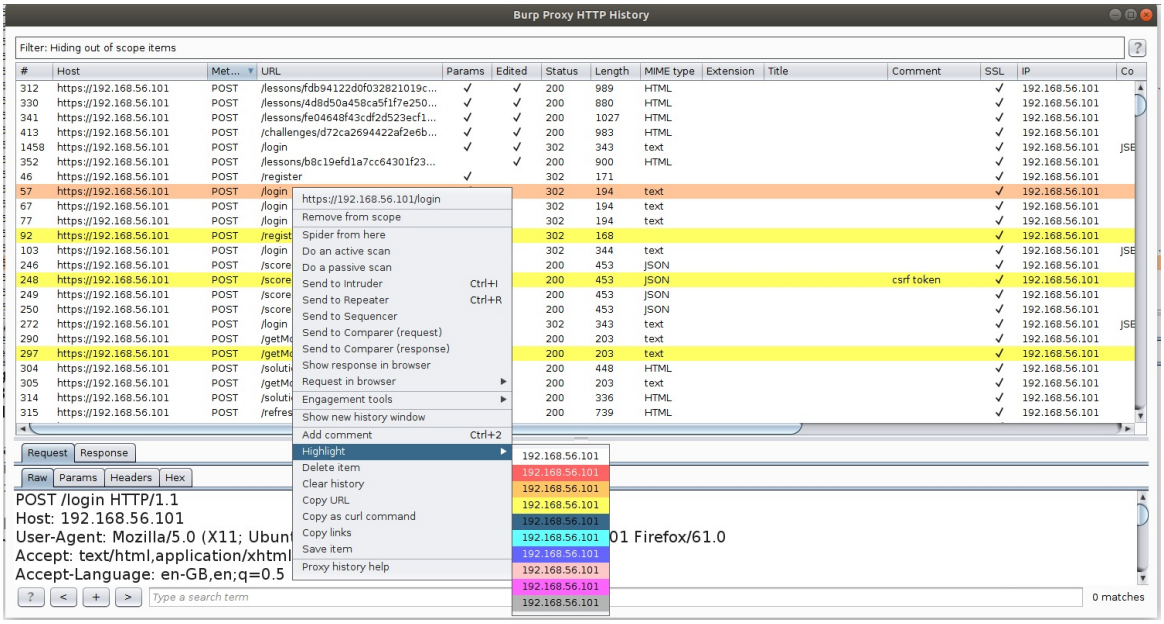
4. Right-click on the history table and select "**Show new history window**" option from the context menu, to open an additional view.



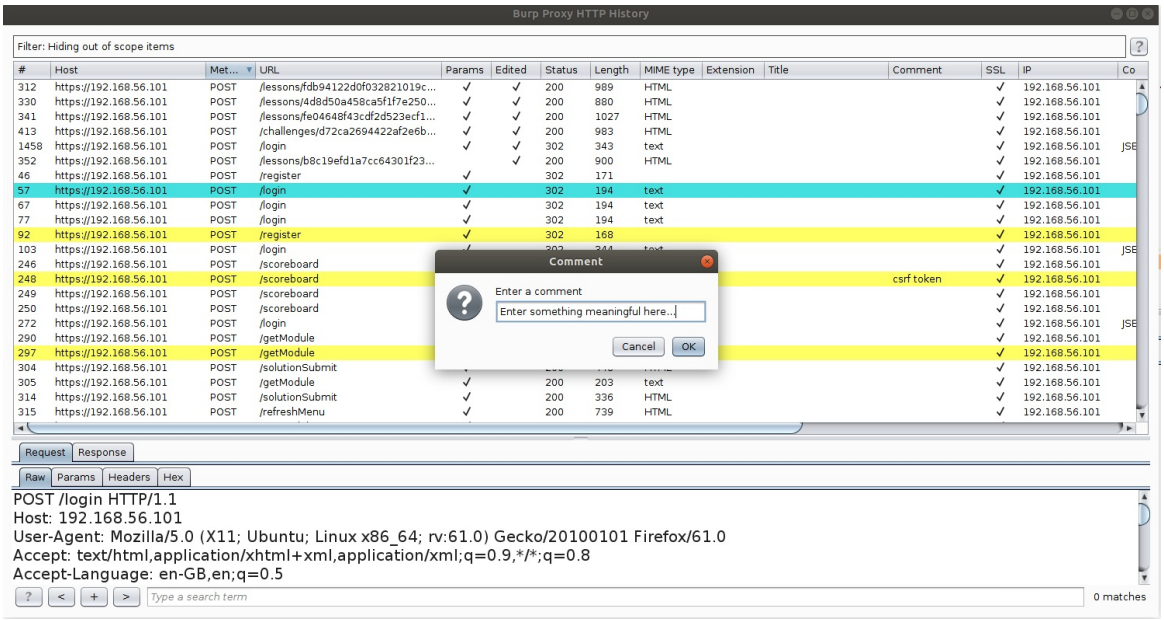
5. Click on a column header to sort contents of the history table.



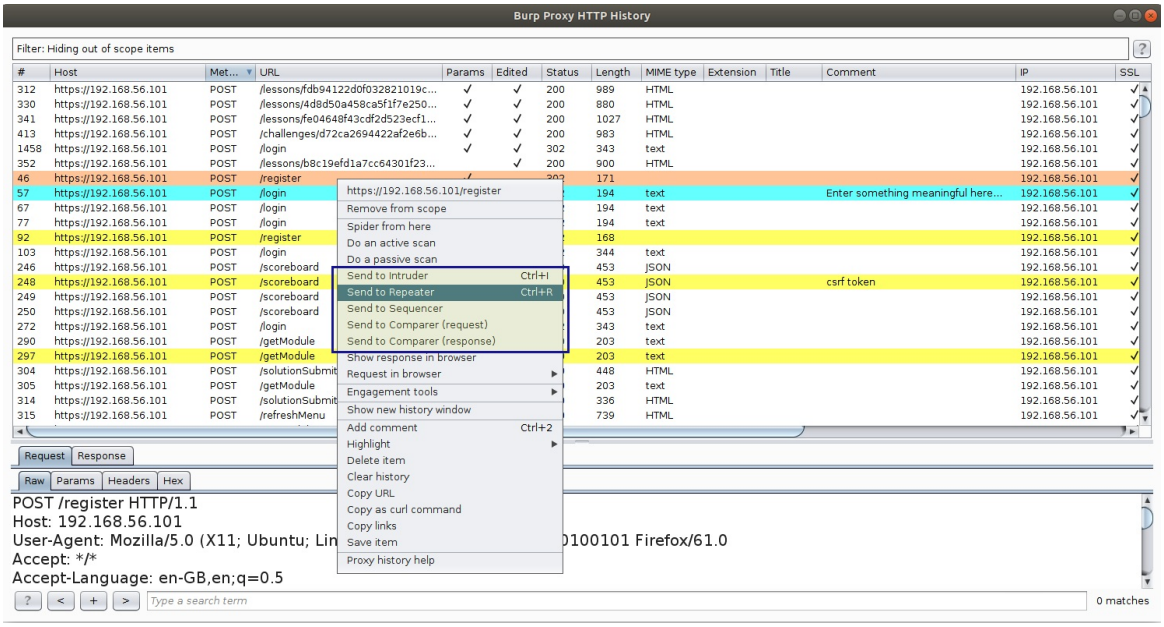
6. To highlight a request, right-click on the chosen request and select "**Highlight**" from the context menu.



7. To add a comment against a request, right-click on the chosen request and select "**Add comment**" from the context menu.



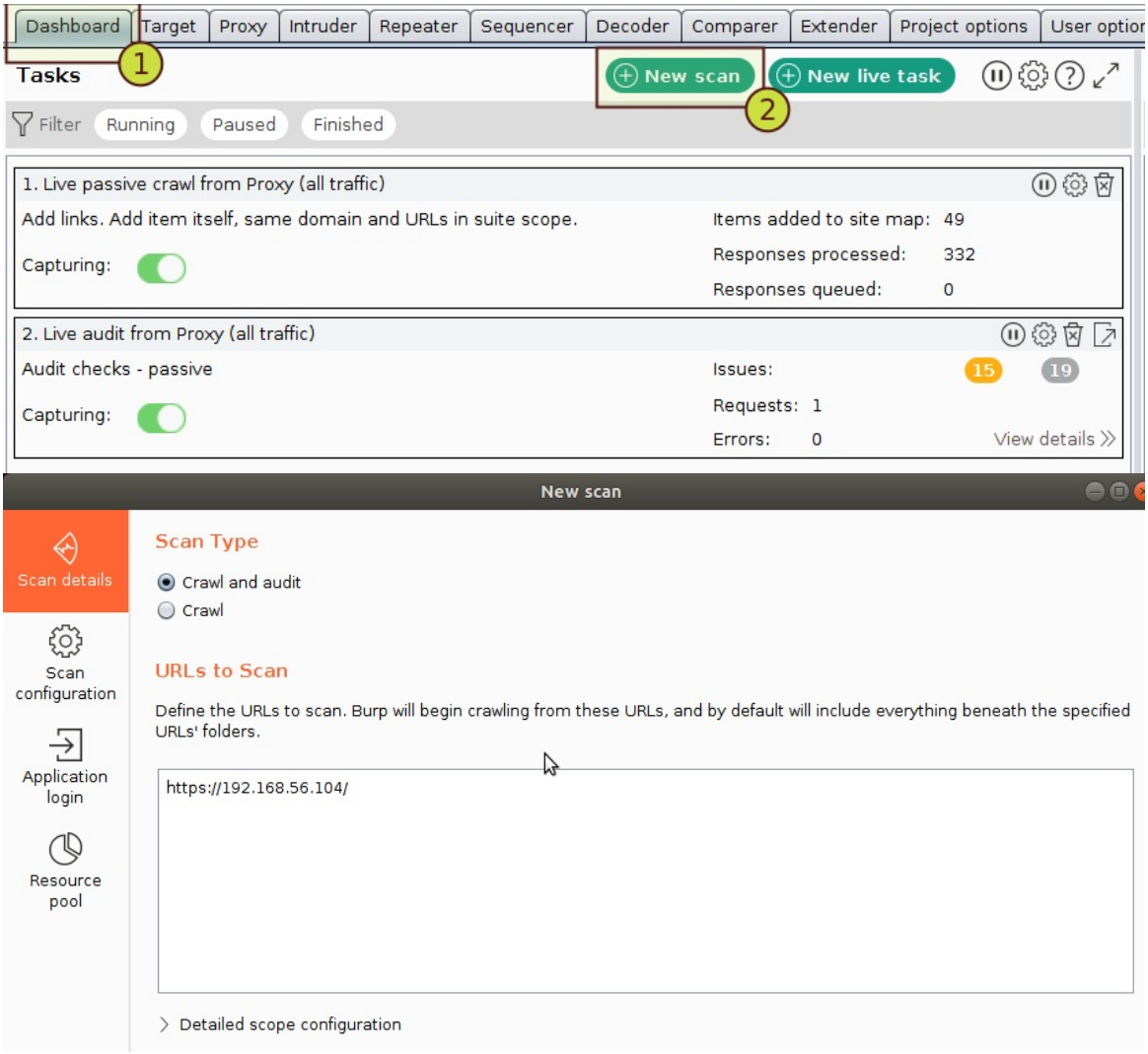
8. If you wish to forward an interesting request to Scanner, Repeater, Intruder, or Sequencer tools, right-click on the selected request and choose an appropriate option from the context menu.


Burp Proxy HTTP History
Filter: Hiding out of scope items
Request
Response
Raw
Params
Headers
Hex
POST /register HTTP/1.1
Host: 192.168.56.101
Accept: */*
Accept-Language: en-GB,en;q=0.5
Type a search term
0 matches

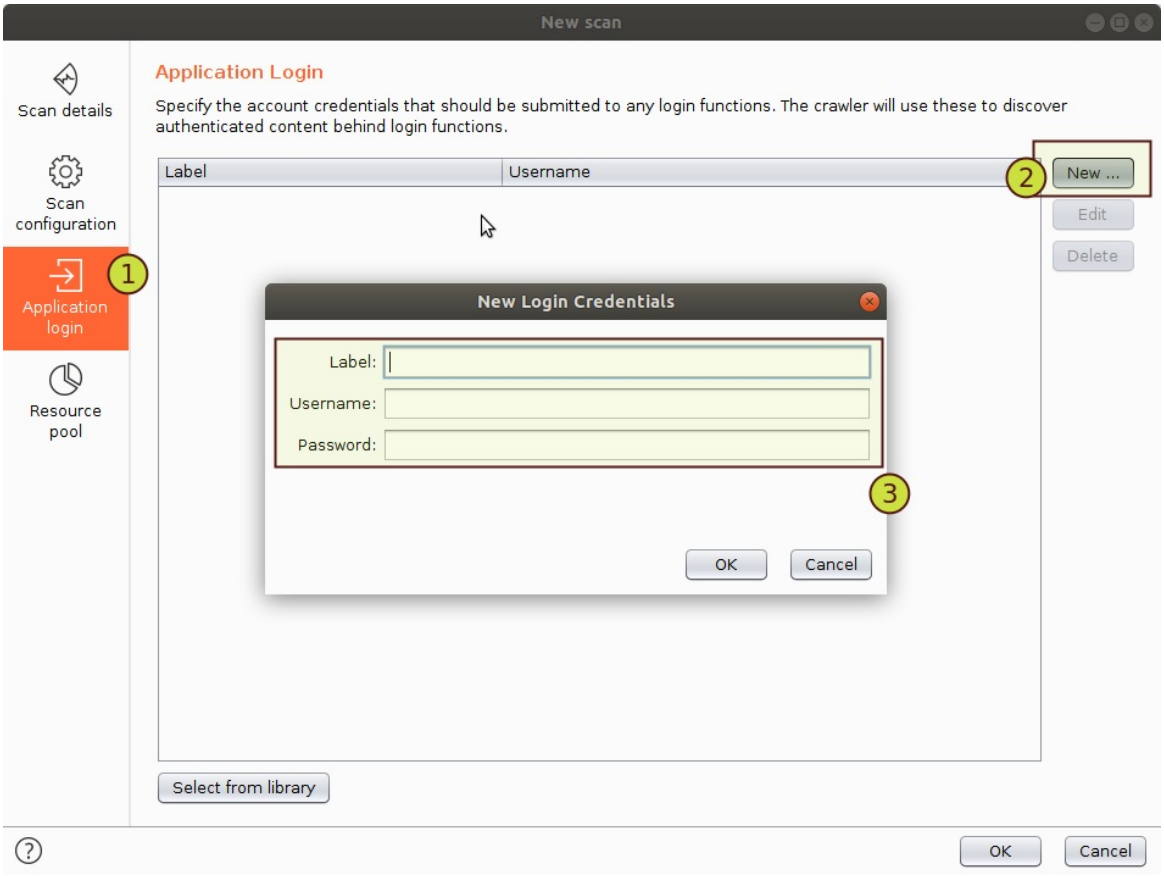
Scanner (10 Minutes)

This is an advanced web vulnerability scanner, which can automatically crawl content and audit for numerous types of vulnerabilities.

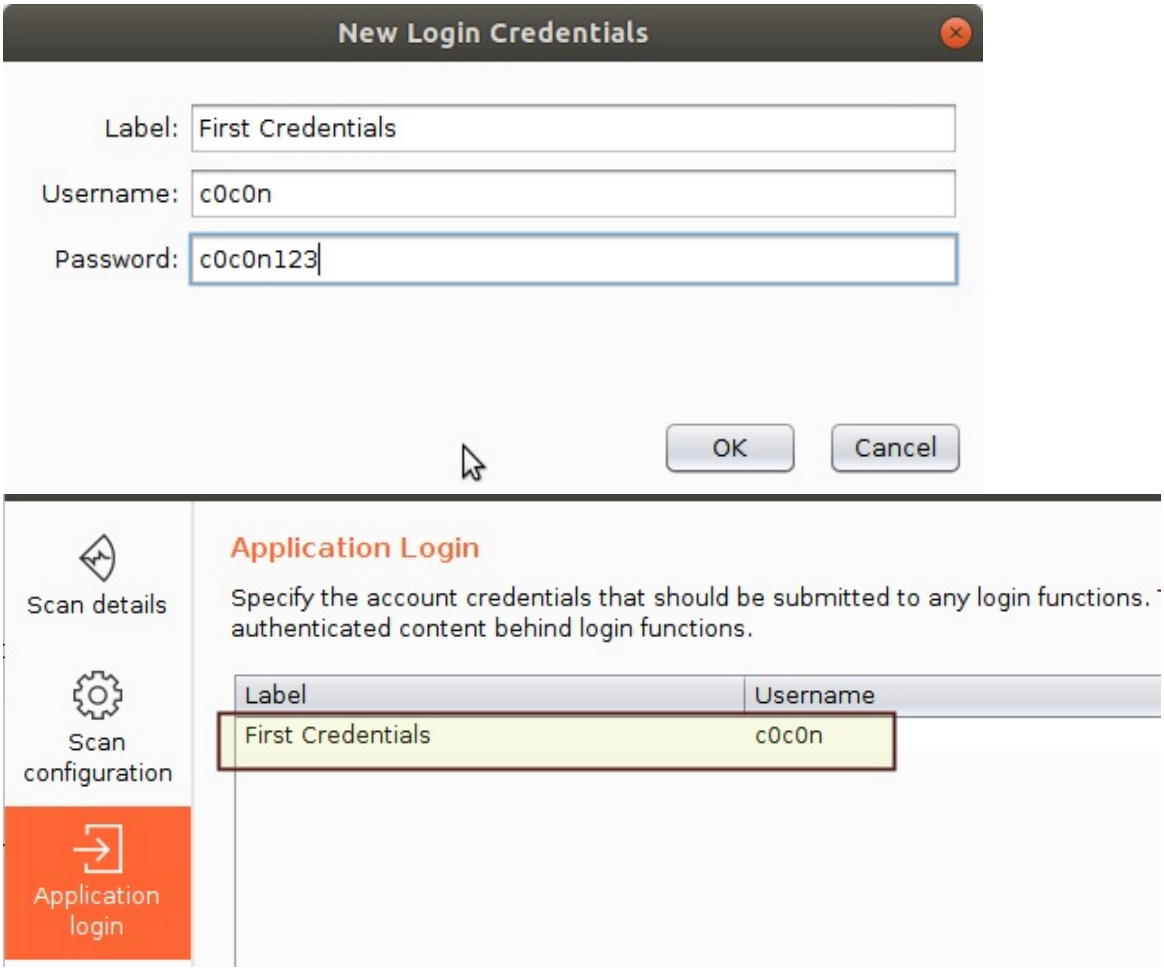
1. In Burp, go to "Dashboard" and click on "New scan" button.



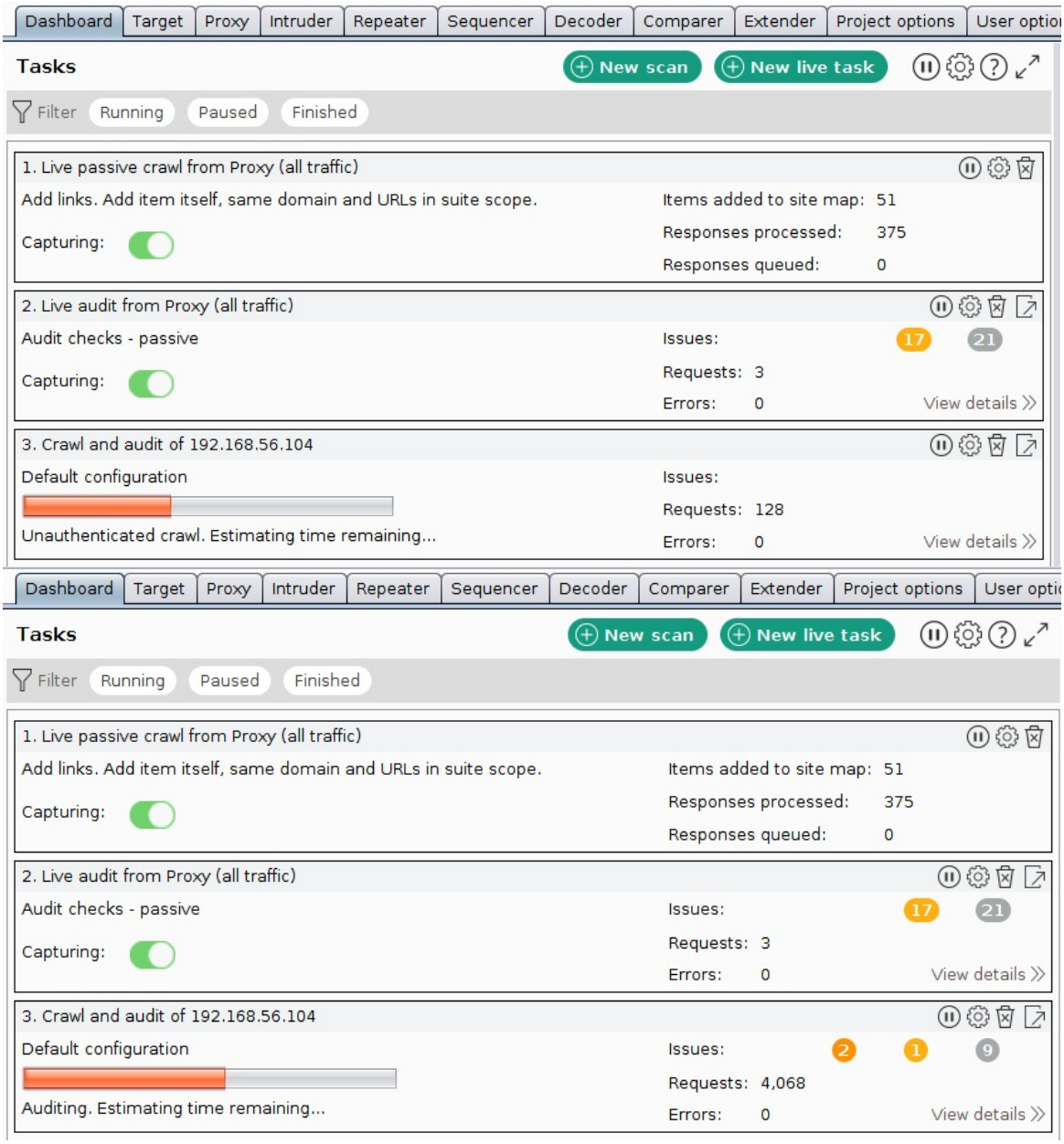
2. In the "New scan" window, click on "Application login" > "New" button.



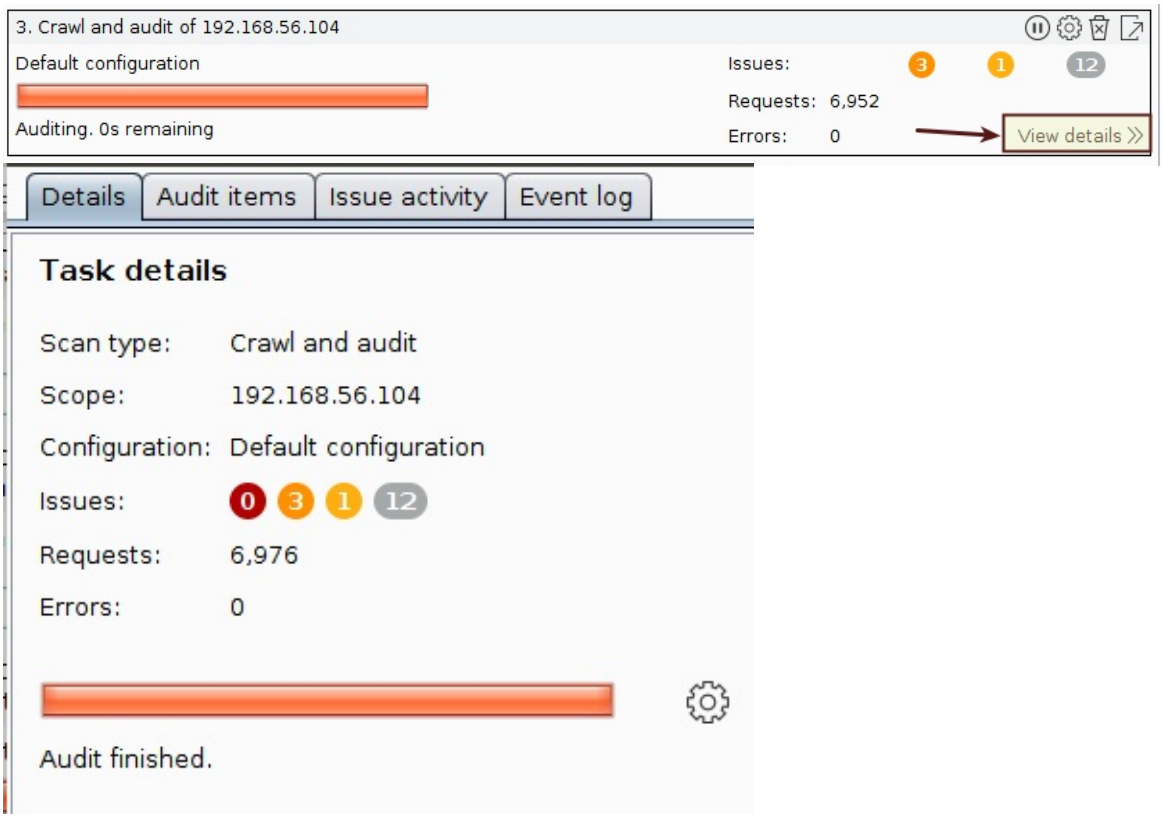
3. Enter valid login credentials for the target application, and click on "OK" button.



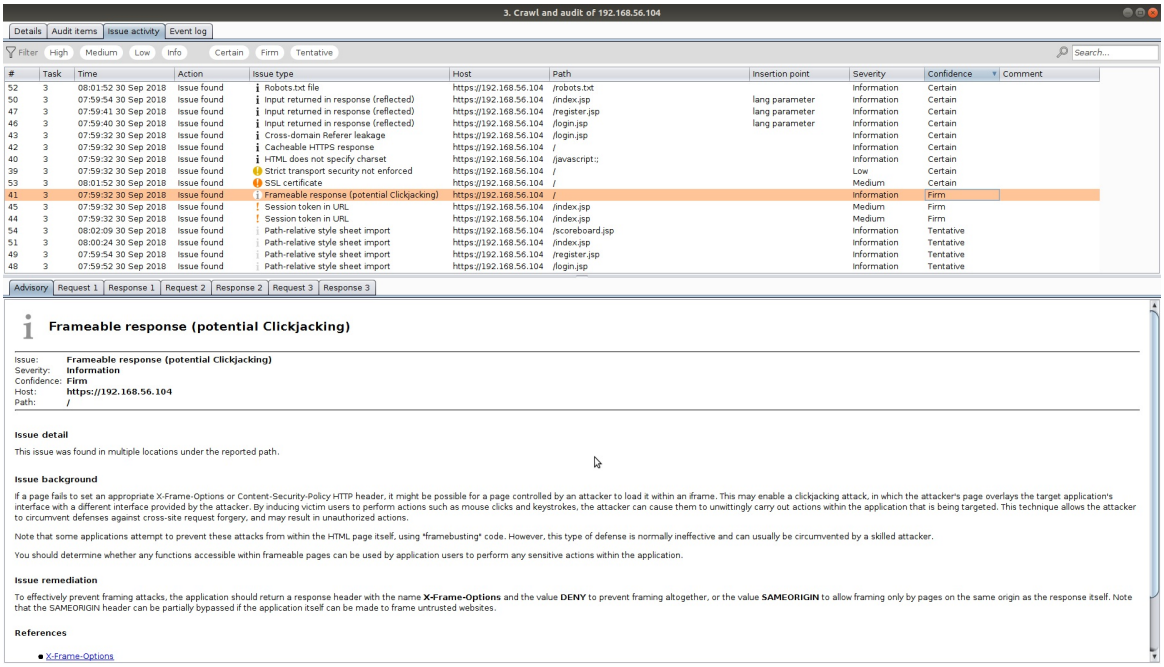
4. Close the "New scan" window by clicking on "OK" button.



5. In "Dashboard" > "Tasks" section, click on the "View Details" link.



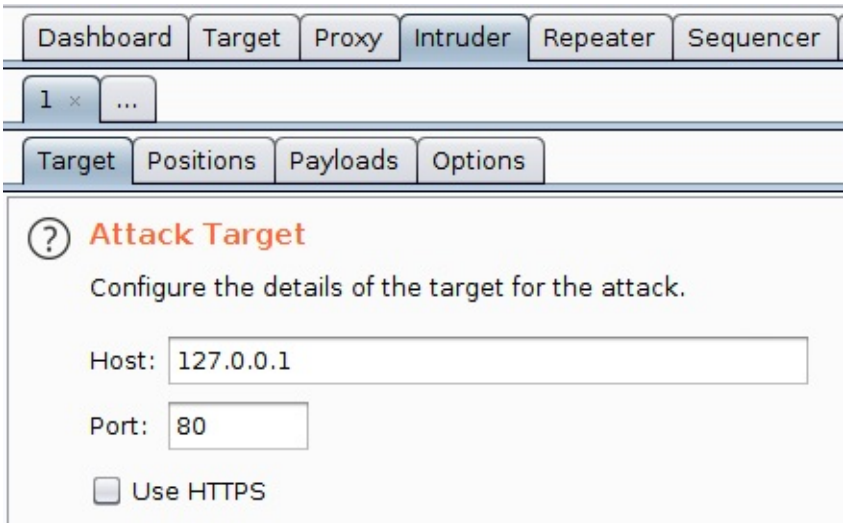
6. Go to "Issue activity" tab to see the list of issues identified by the scanner.



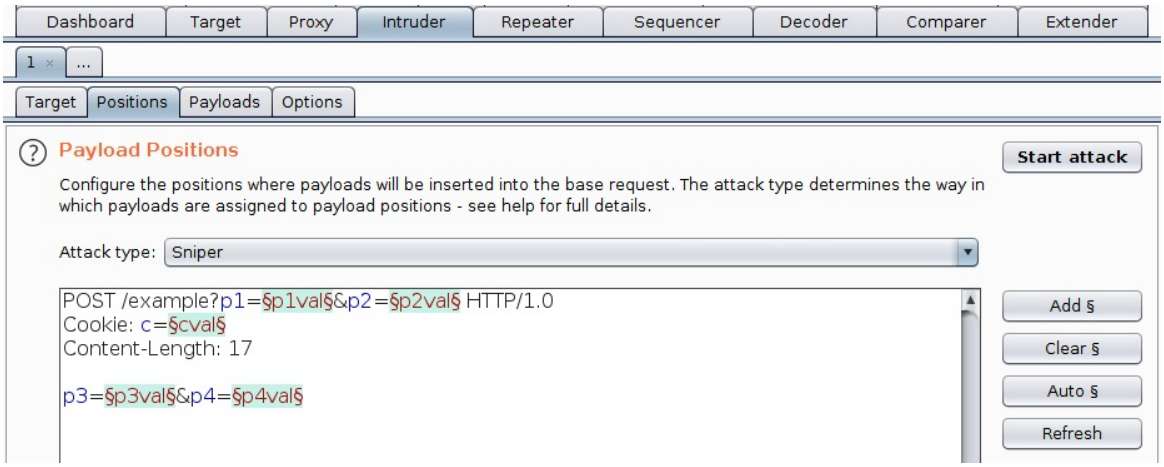
Intruder (30 Minutes)

This is a powerful tool for carrying out automated customized attacks against web applications. It is highly configurable and can be used to perform a wide range of tasks to make your testing faster and more effective.

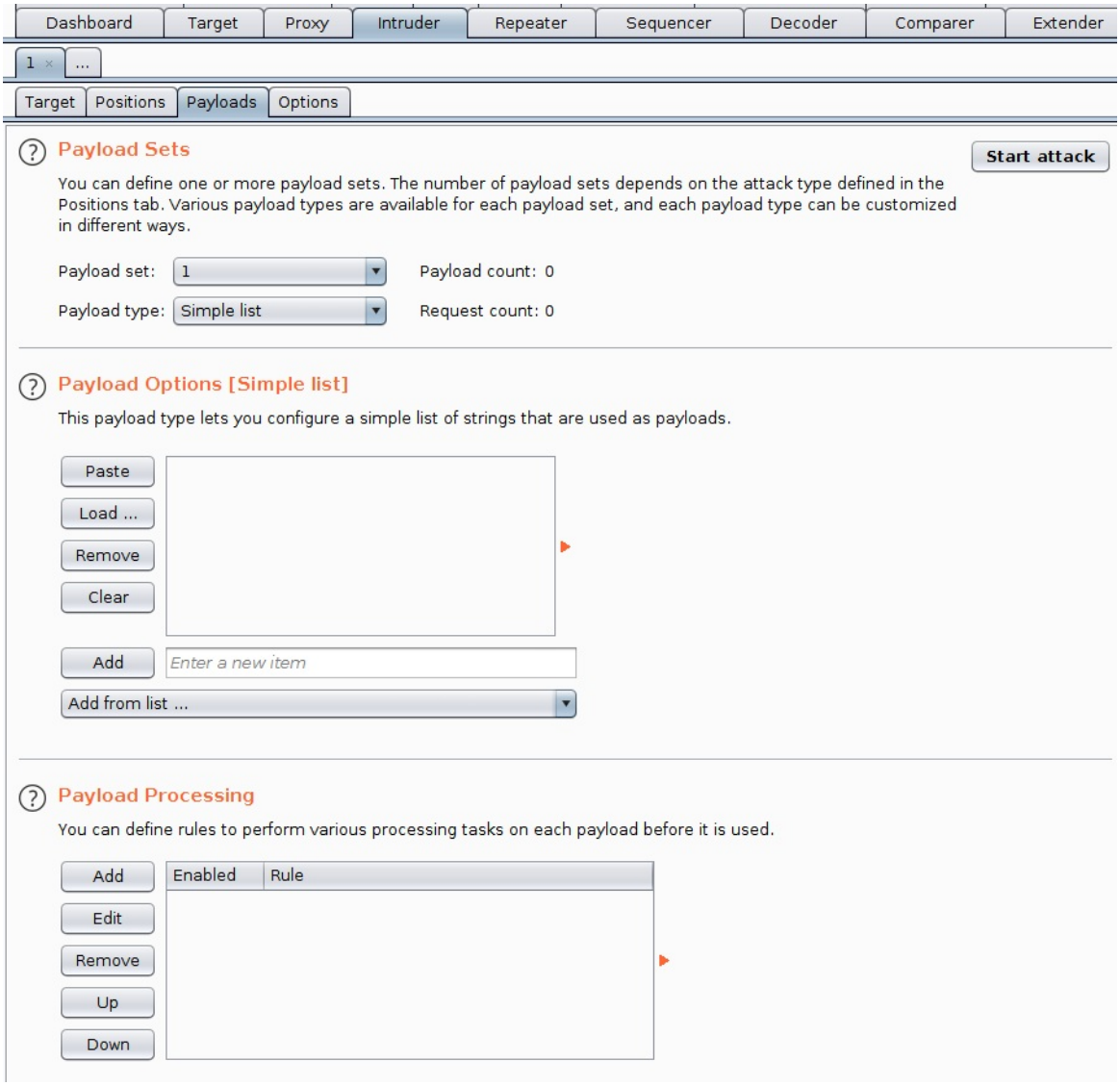
1. In Burp, go to "Intruder" > "Target" tab, and verify the "Attack Target" configuration.



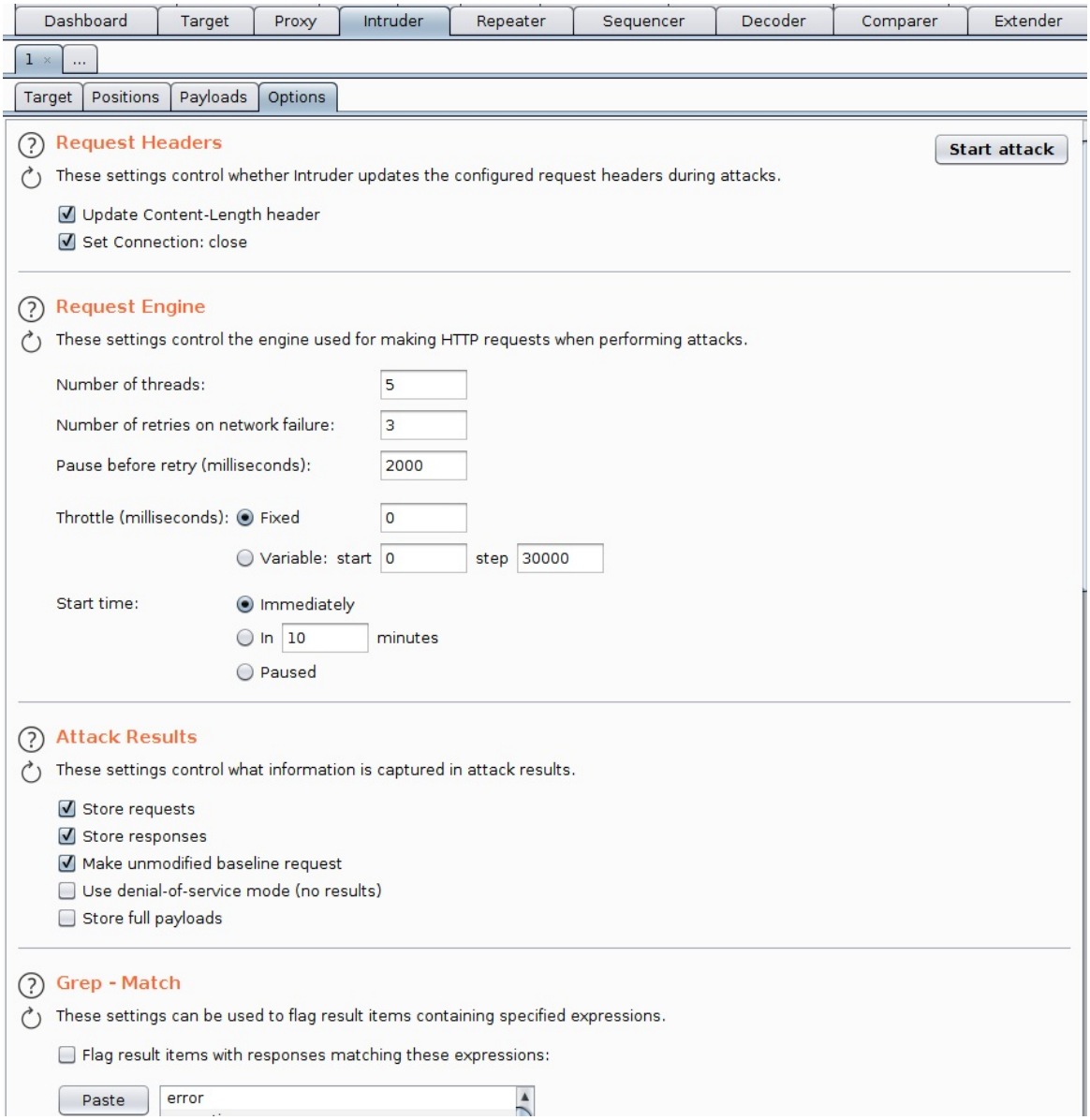
2. Switch to "Intruder" > "Position" tab, and get familiar with the user interface.



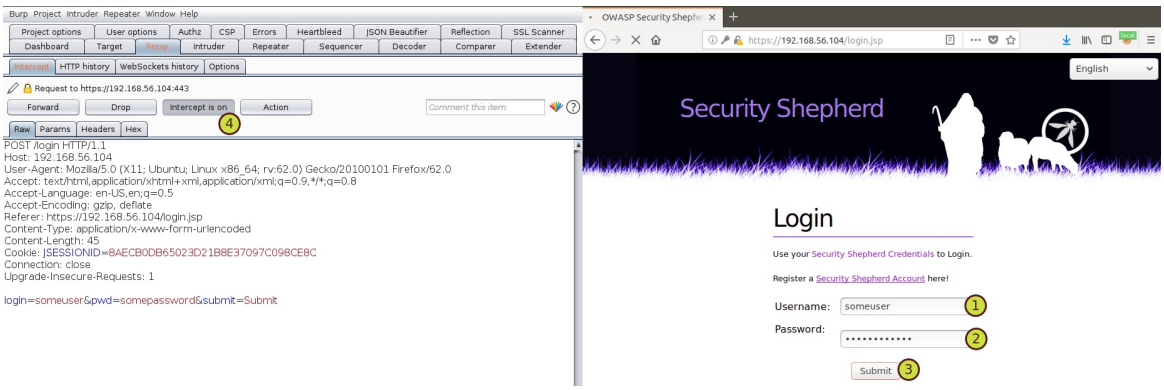
3. Switch to "Intruder" > "Payloads" tab, and get familiar with the user interface.



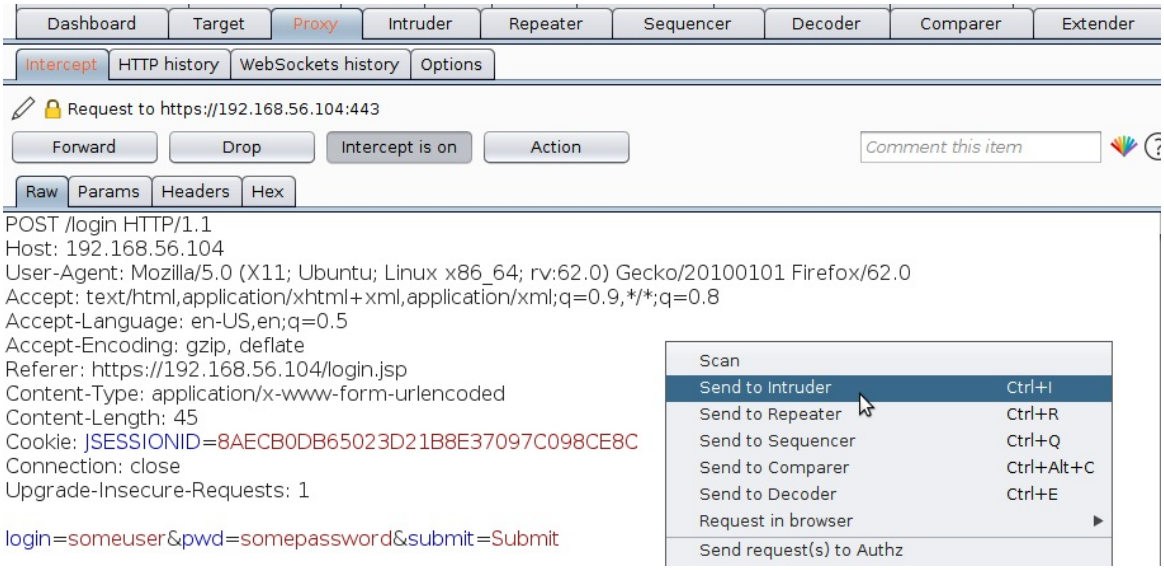
4. Switch to "Intruder" > "Options" tab, and get familiar with the user interface.



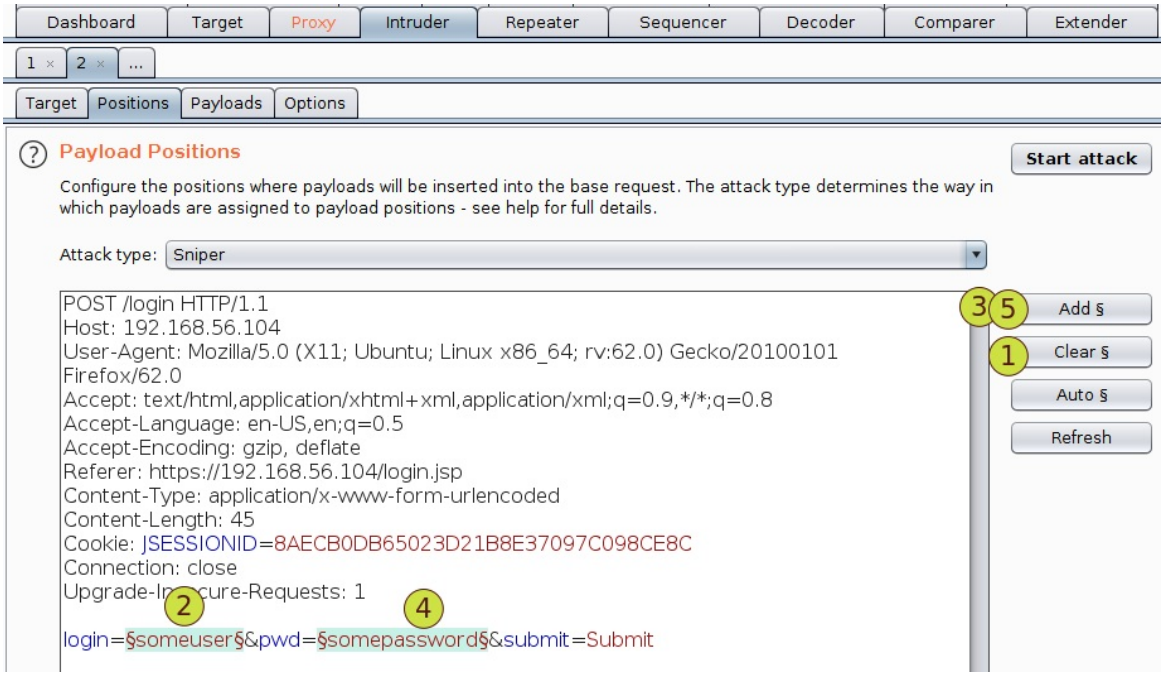
5. In Firefox, access the login page of Security Shepherd web application: `https://192.168.56.104/login.jsp`
6. Enter random values and submit the login form.
7. Intercept this request in Burp.



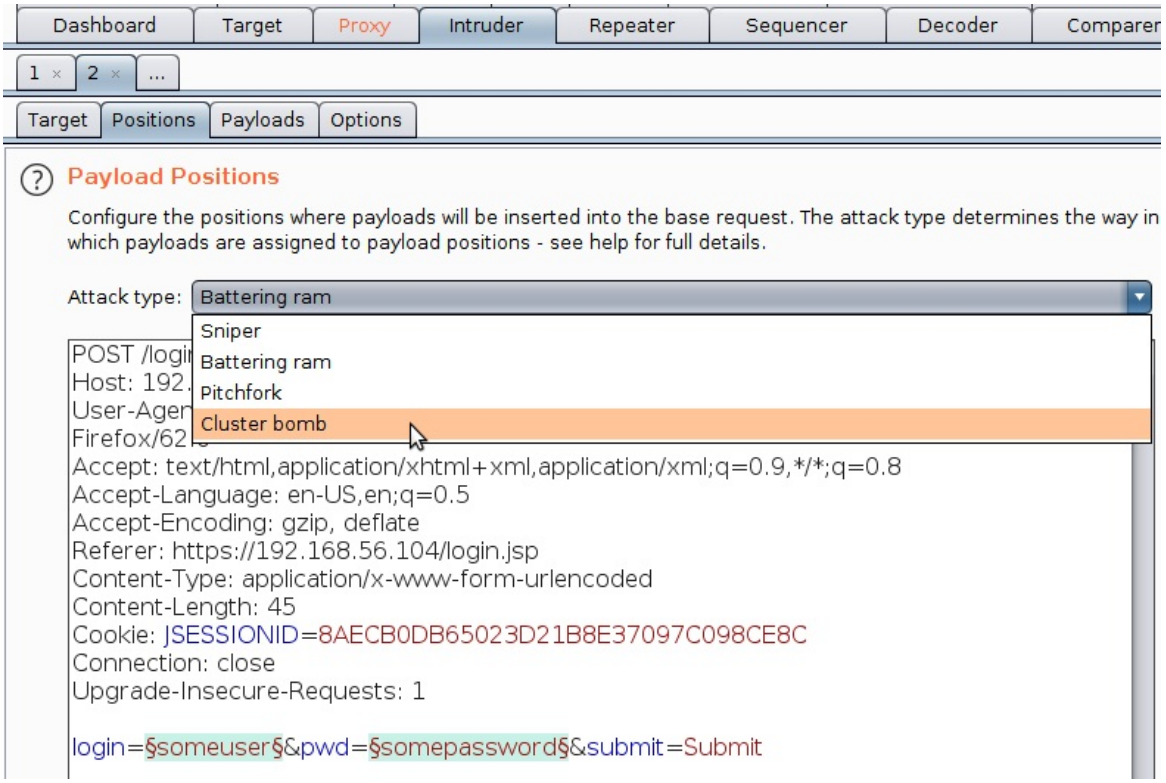
8. Send the intercepted request to `Intruder`.



9. Go to "Intruder" > "Positions" tab.
10. Click on "Clear" button to clear the pre-defined payload positions.
11. Identify parameters that accept user inputs.
12. Mark the payload positions by selecting the corresponding value for a parameter and then clicking on "Add" button. For Security Shepherd login request, mark payload positions for the parameters named as "login" and "pwd".

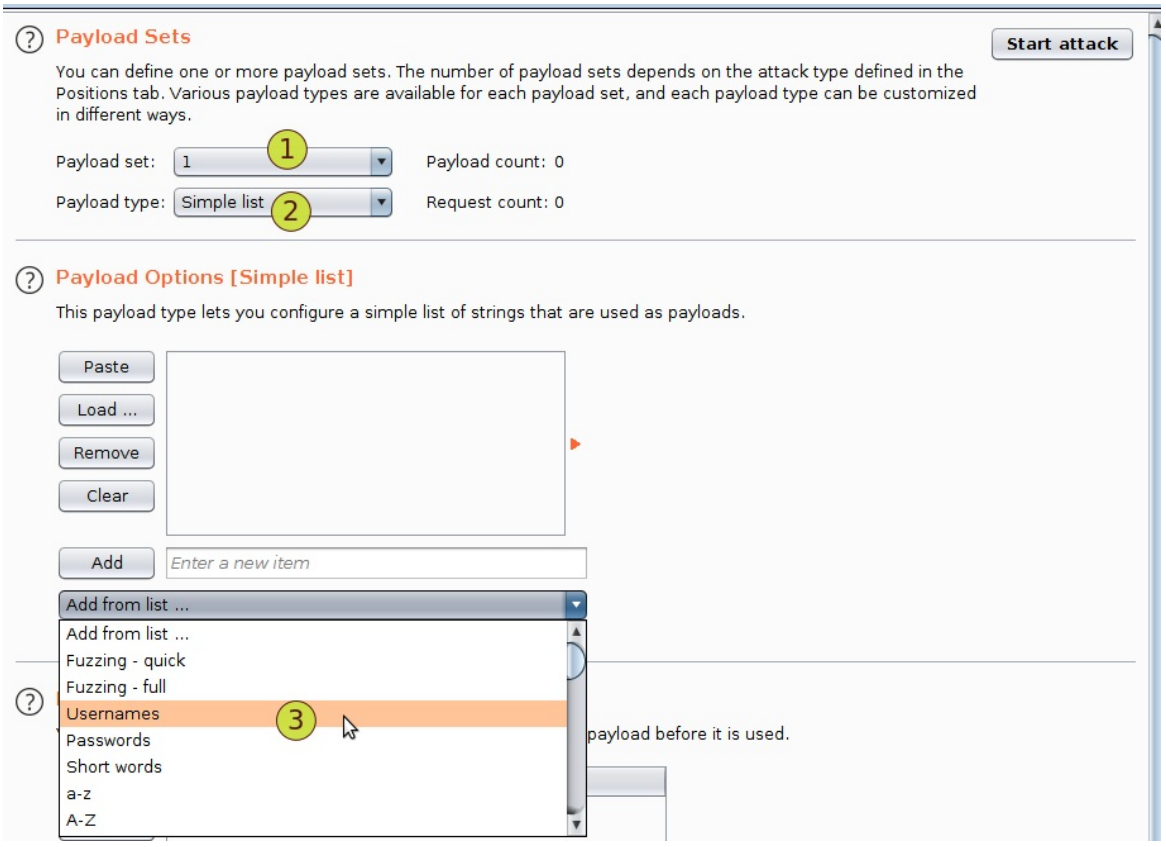


13. Choose "Cluster Bomb" as the *attack type*.

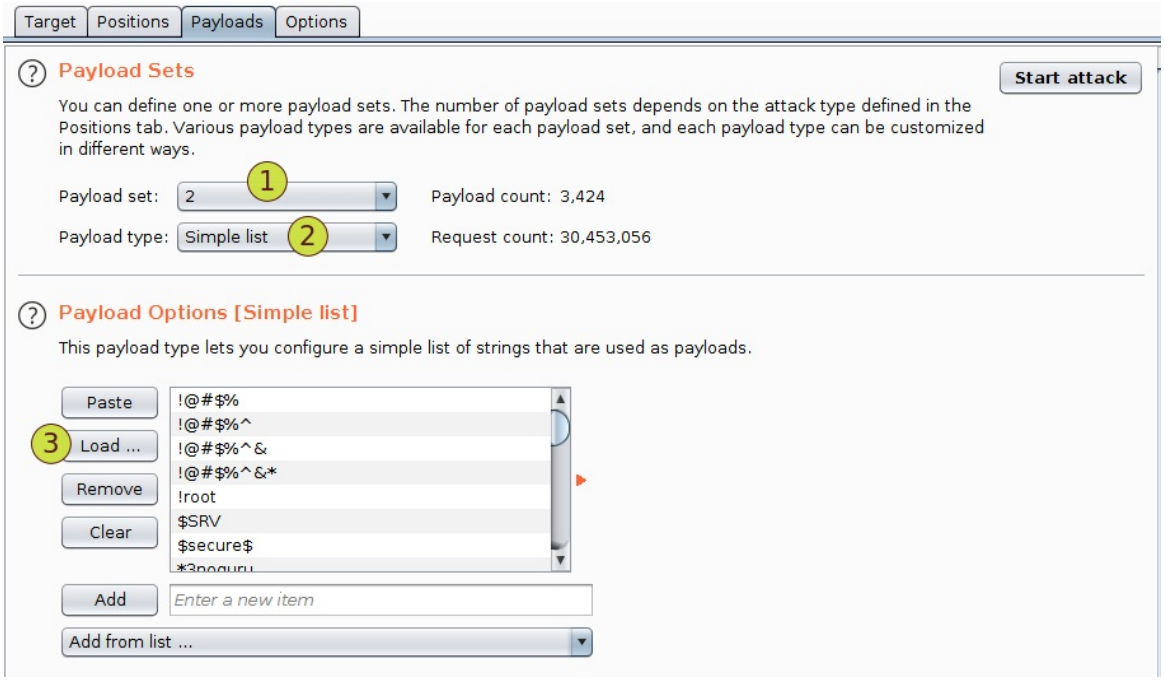


14. Go to "Intruder" > "Payloads" tab.

15. Choose "Simple list" payload type for payload set `1`, and add a list of possible usernames in the "Payload Options" section.

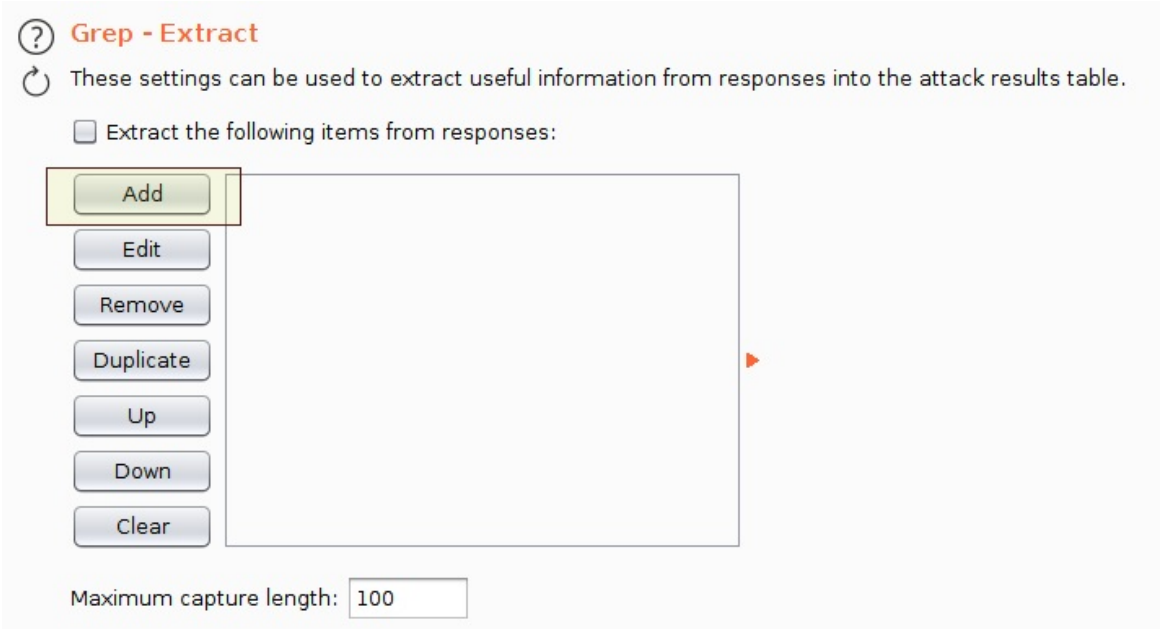


16. Choose "Simple list" payload type for payload set `2`, and add a list of possible passwords in the "Payload Options" section.

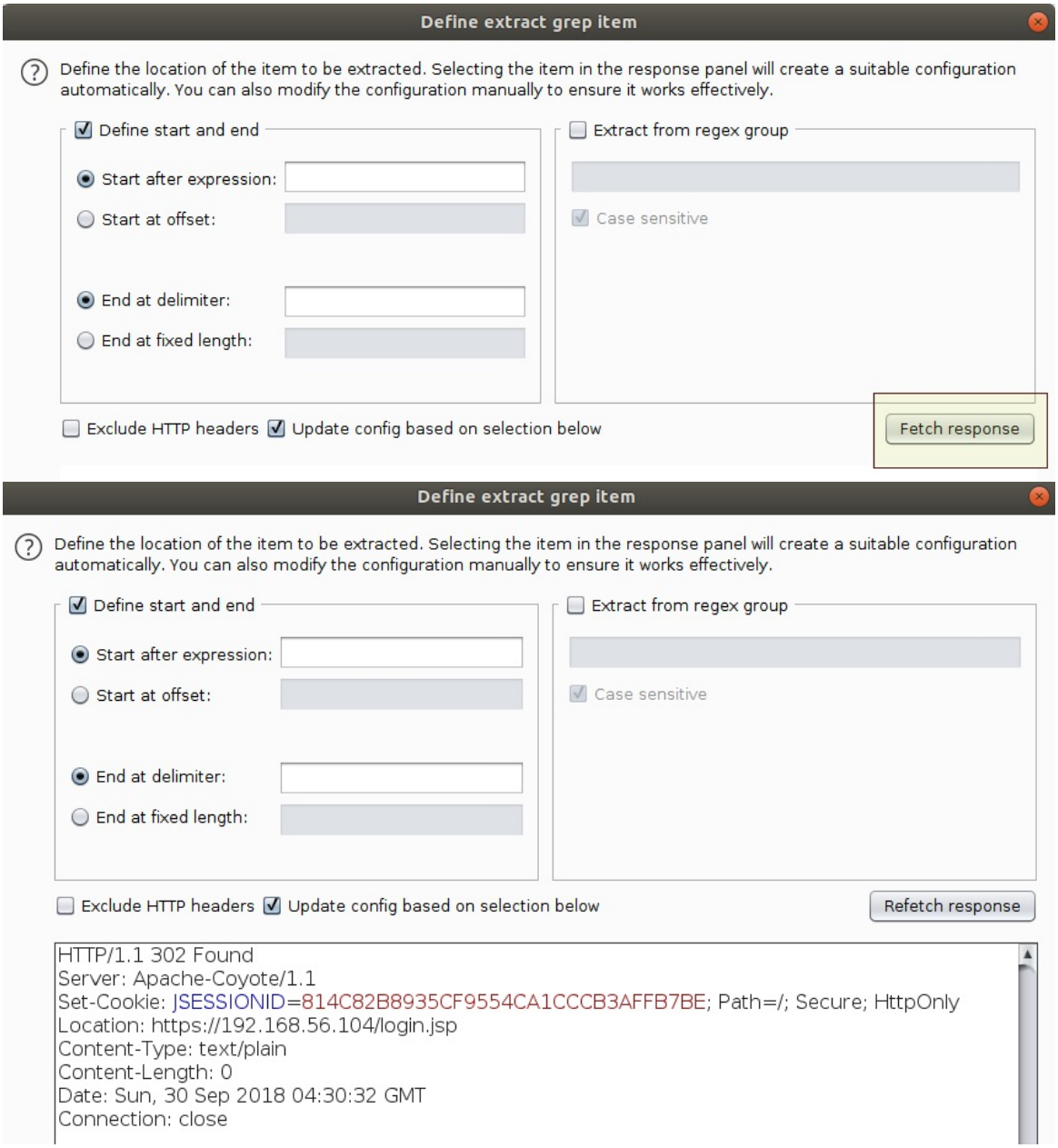


17. Go to "Intruder" > "Options" tab.

18. In the "Grep - Extract" section, click on "Add" button.

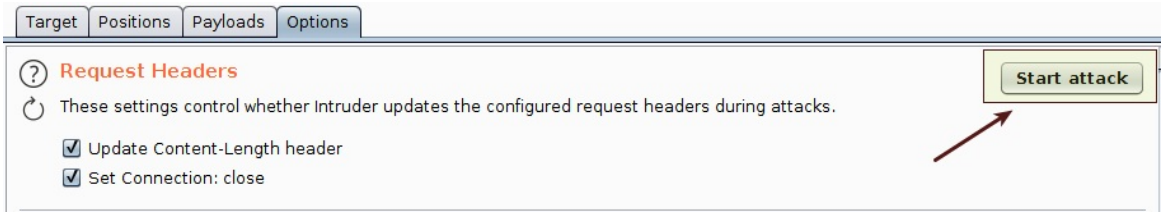


19. In the pop-up window, click on "Fetch response" button.

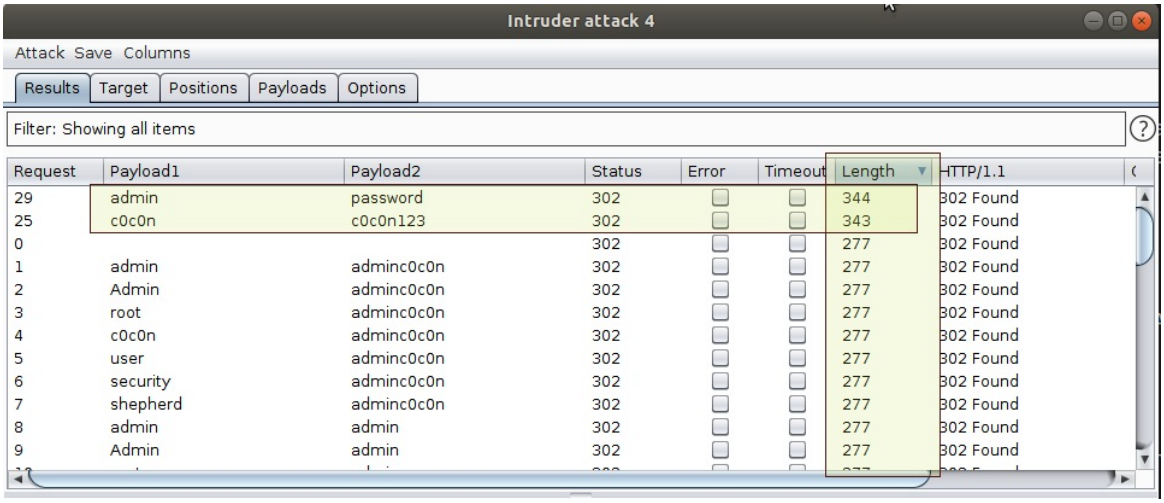


20. Highlight the text that you want to extract from the response, and click on "OK" button.

21. Start the attack by clicking on "Start attack" button.



22. Sort the response on **Length** column, in descending order.



23. Analyze the result set.

Request	Payload1	Payload2	Status	Error	Timeout	Length	HTTP/1.1
29	admin	password	302			344	302 Found
25	c0c0n	c0c0n123	302			343	302 Found
0			302			277	302 Found
1	admin	adminc0c0n	302			277	302 Found
2	Admin	adminc0c0n	302			277	302 Found
3	root	adminc0c0n	302			277	302 Found
4	c0c0n	adminc0c0n	302			277	302 Found
5	user	adminc0c0n	302			277	302 Found
6	security	adminc0c0n	302			277	302 Found
7	shepherd	adminc0c0n	302			277	302 Found
8	admin	admin	302			277	302 Found
9	Admin	admin	302			277	302 Found

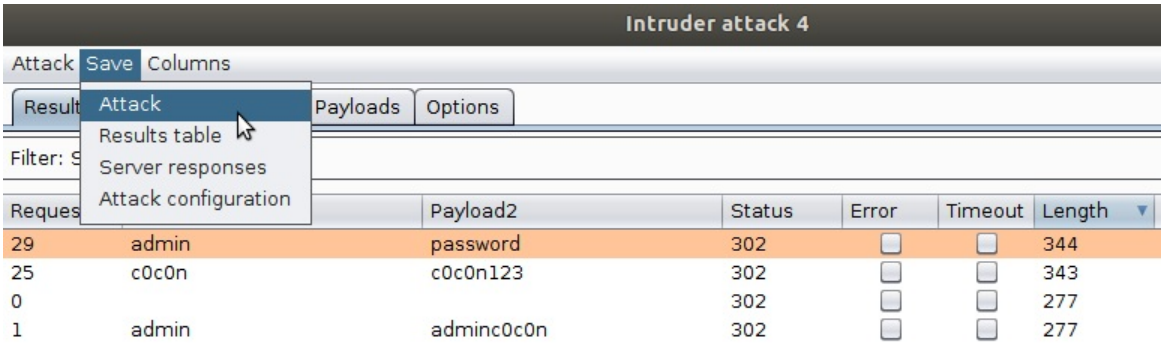
Request | Response

Raw | Headers | Hex | Render

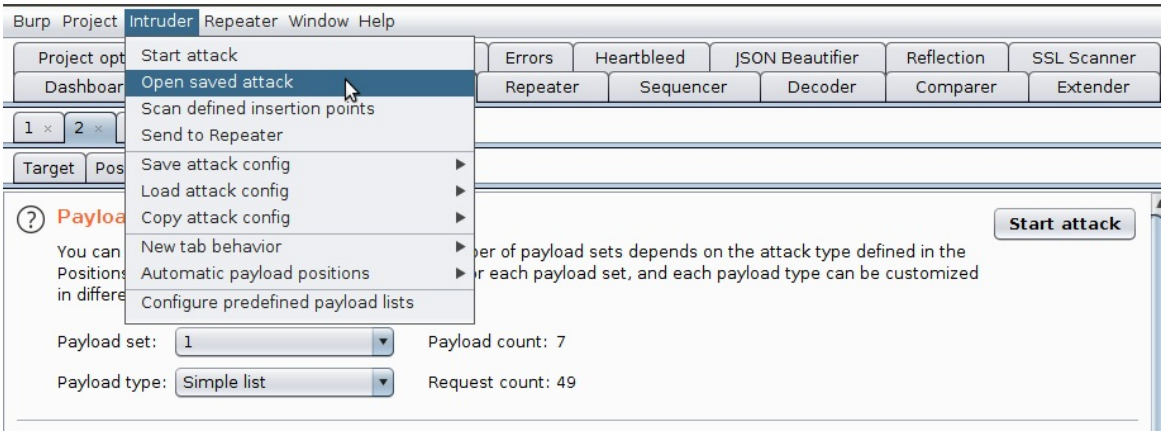
```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=0C062FBC2D6E38AF1B9707BA10FA2731; Path=/; Secure; HttpOnly
Set-Cookie: token=-7941955925642219268655563921873778330 6; Secure
Location: https://192.168.56.104/index.jsp
Content-Type: text/plain
Content-Length: 0
Date: Sun, 30 Sep 2018 04:43:44 GMT
Connection: close
```

24. Login to Security Shepherd web application using the admin credentials that was discovered through brute force attack.

25. To save the attack, click on "Save" in main menu of the attack window, and select "Attack" sub-menu option.



26. To load a saved attack, select "Intruder" > "Open saved attack" in Burp.


Burp Project Intruder Repeater Window Help
Start attack
Open saved attack
Scan defined insertion points
Send to Repeater
Save attack config
Load attack config
Copy attack config
New tab behavior
Automatic payload positions
Configure predefined payload lists
Errors
Heartbleed
JSON Beautifier
Reflection
SSL Scanner
Repeater
Sequencer
Decoder
Comparer
Extender
Target
Start attack
Payload set: 1
Payload count: 7
Payload type: Simple list
Request count: 49

Repeater (20 Minutes)

This is a tool for manually manipulating and reissuing individual HTTP requests, and analyzing the application's responses.

Assumption:

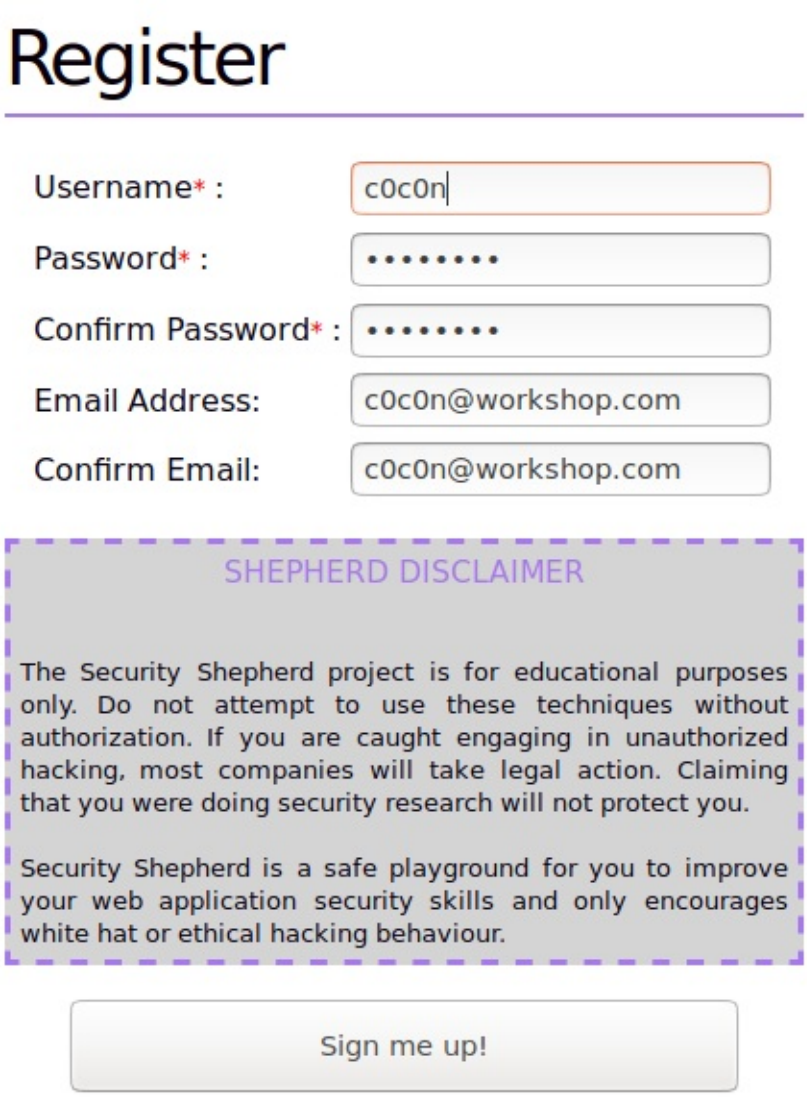
- Burp proxy has been configured correctly.
- You are currently logged in to Security Shepherd's admin account.

Steps:

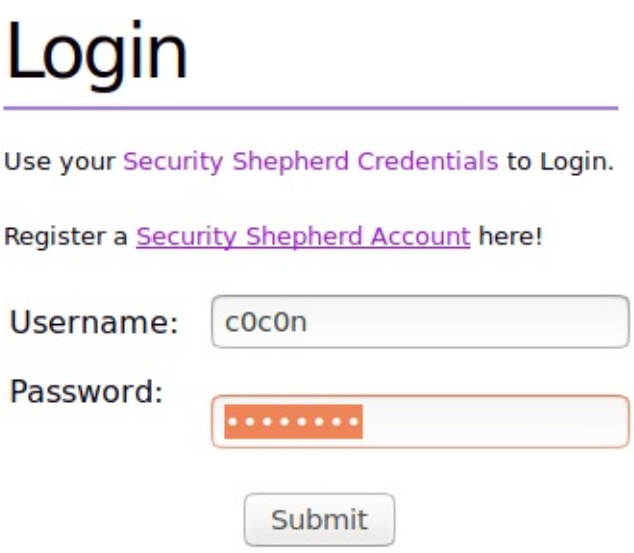
1. Log out of Security Shepherd's admin account by clicking on the "Logout" button.

2. On the login page of Security Shepherd application, click on the link labeled as "Security Shepherd Account".

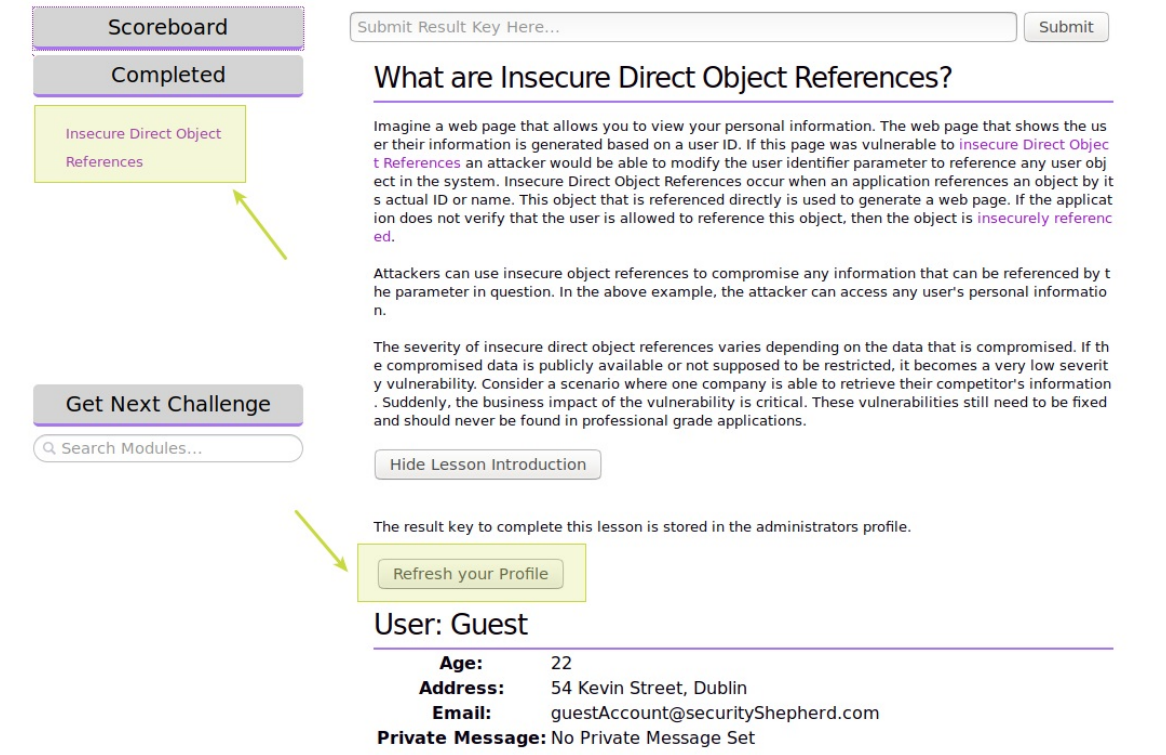
3. Fill-in the registration form and click on "Sign me up!" button.

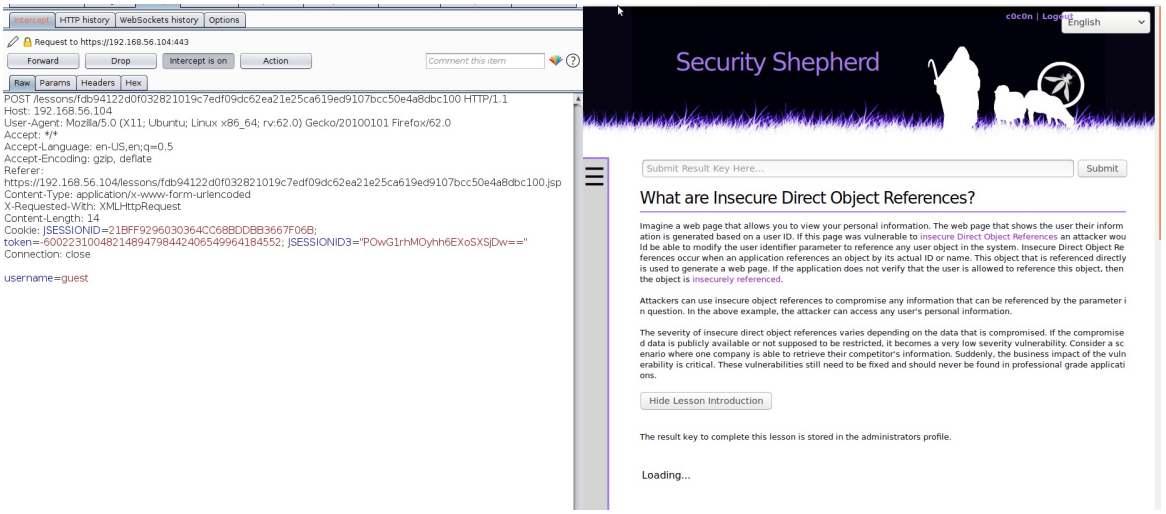


4. Login to the newly created (non-admin) account.

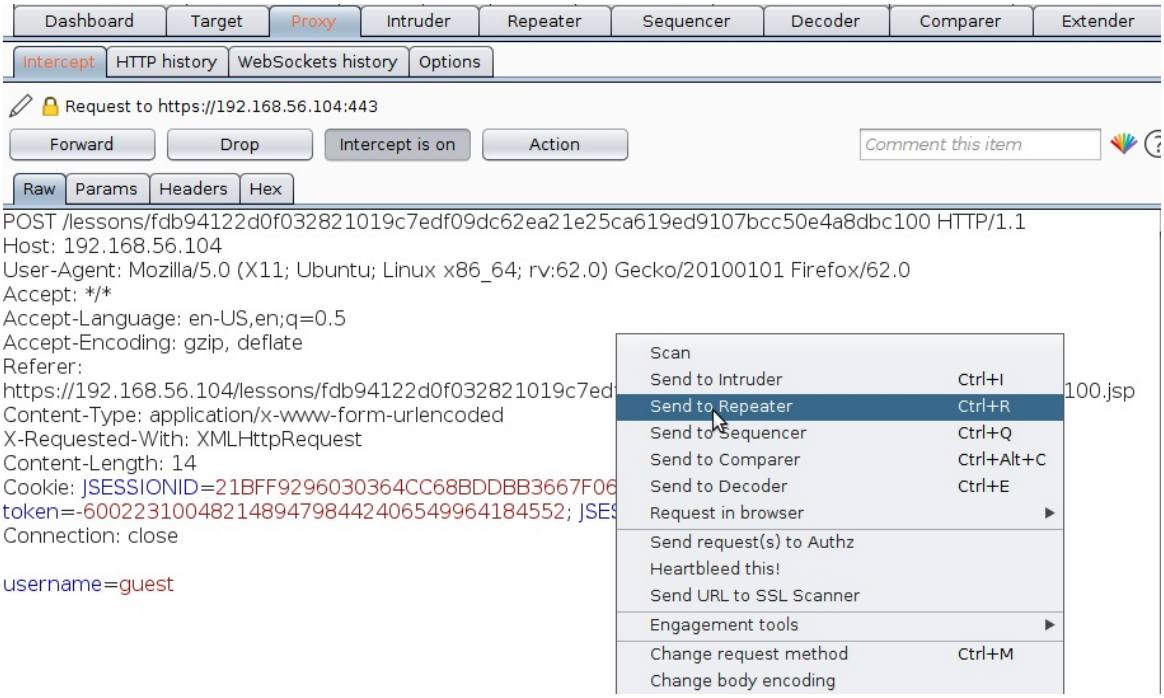


5. Click on "Insecure Direct Object References" link in the left navigation menu.
6. In Burp, turn the intercept mode on.
7. In Firefox, click on the "Refresh your Profile" button.

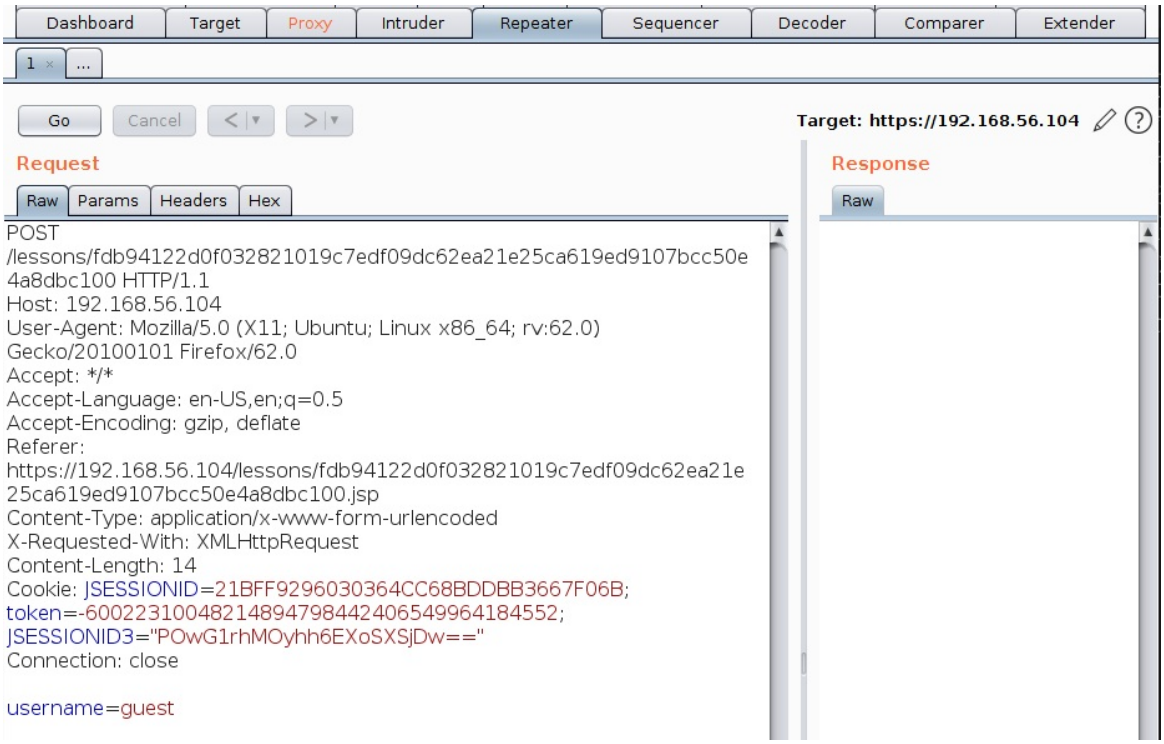




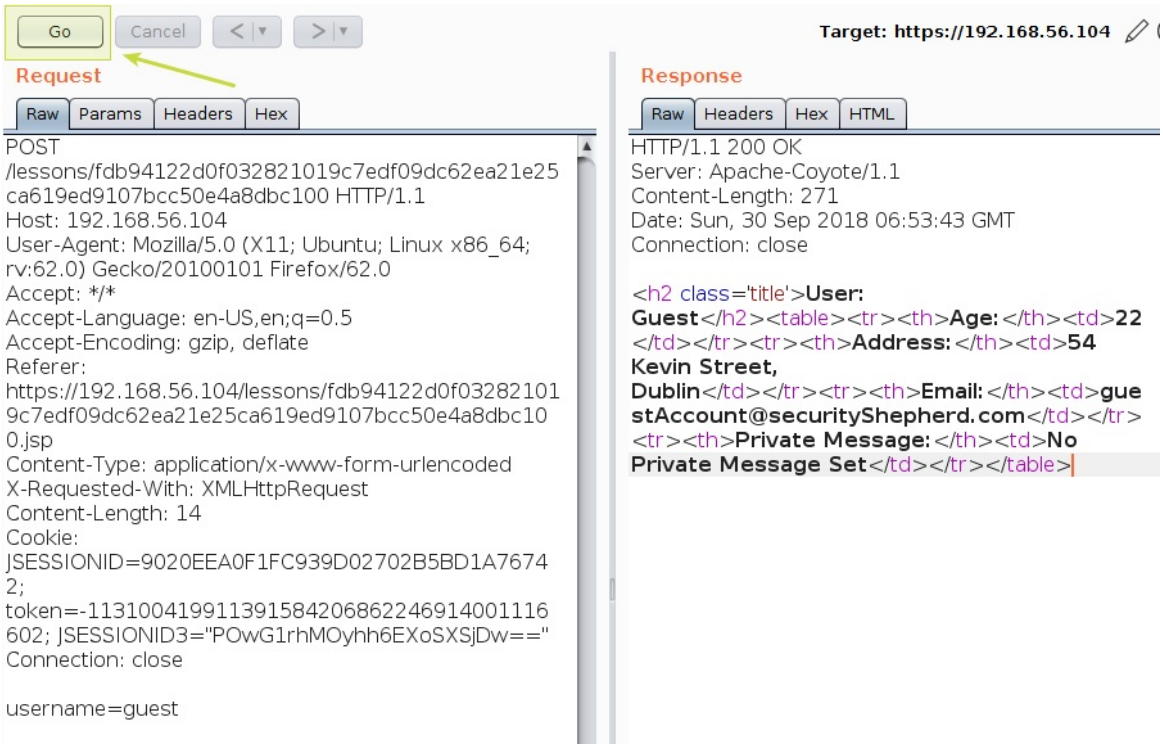
8. Go to Burp > "Proxy" > "Intercept" tab, and right-click on the intercepted request.
9. Select "Send to Repeater" from the context menu.



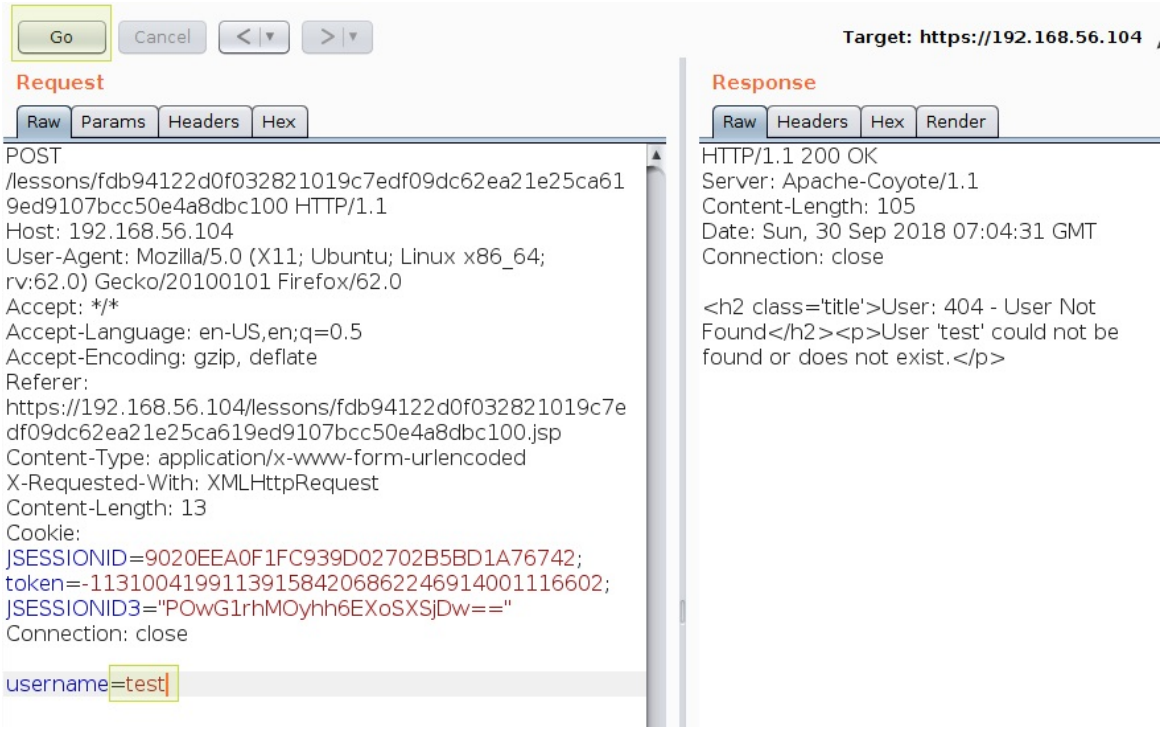
10. Switch to "Repeater" tab in Burp.



11. Click on the "Go" button.



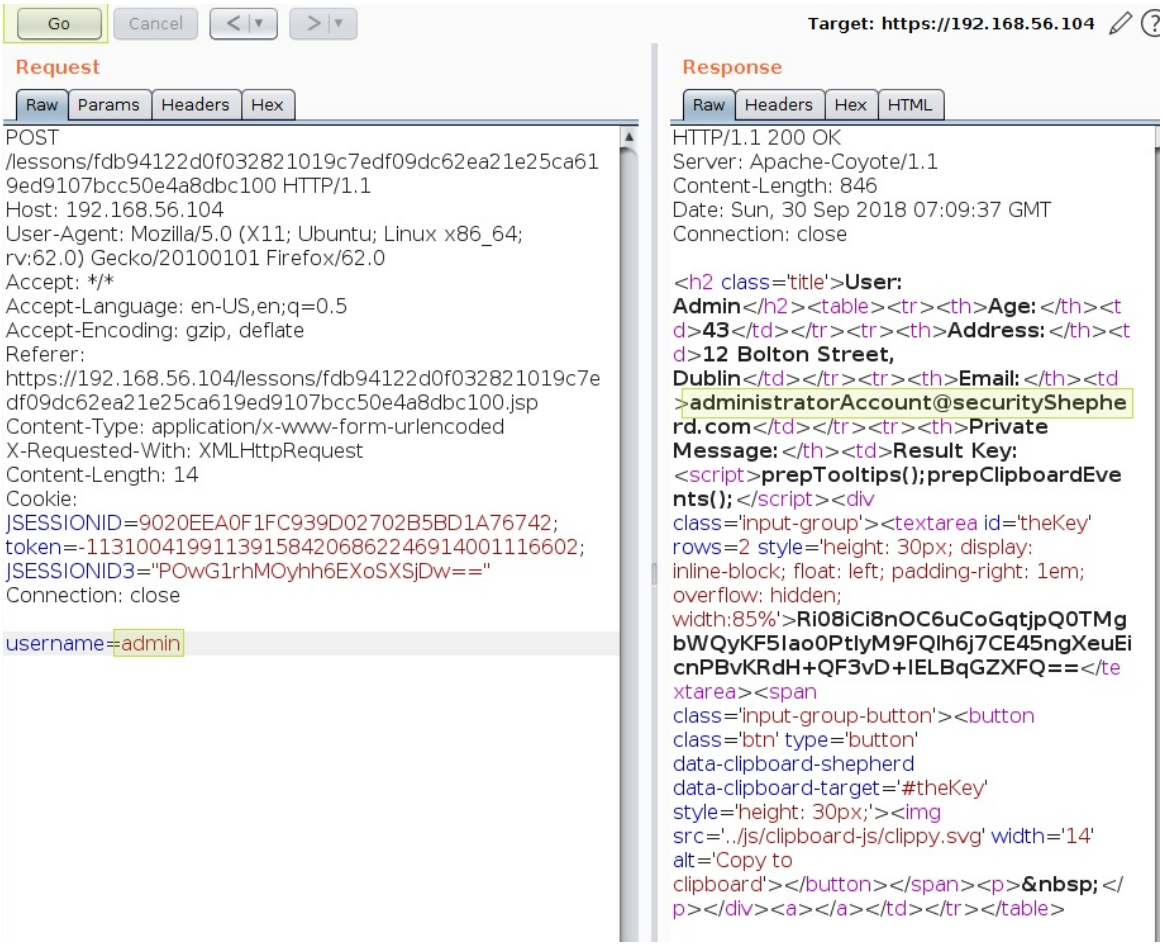
12. In the "Request" section, change the value of the "username" parameter to a random value, e.g. `test`, and click on the "Go" button.



13. Observe the changes in the response.

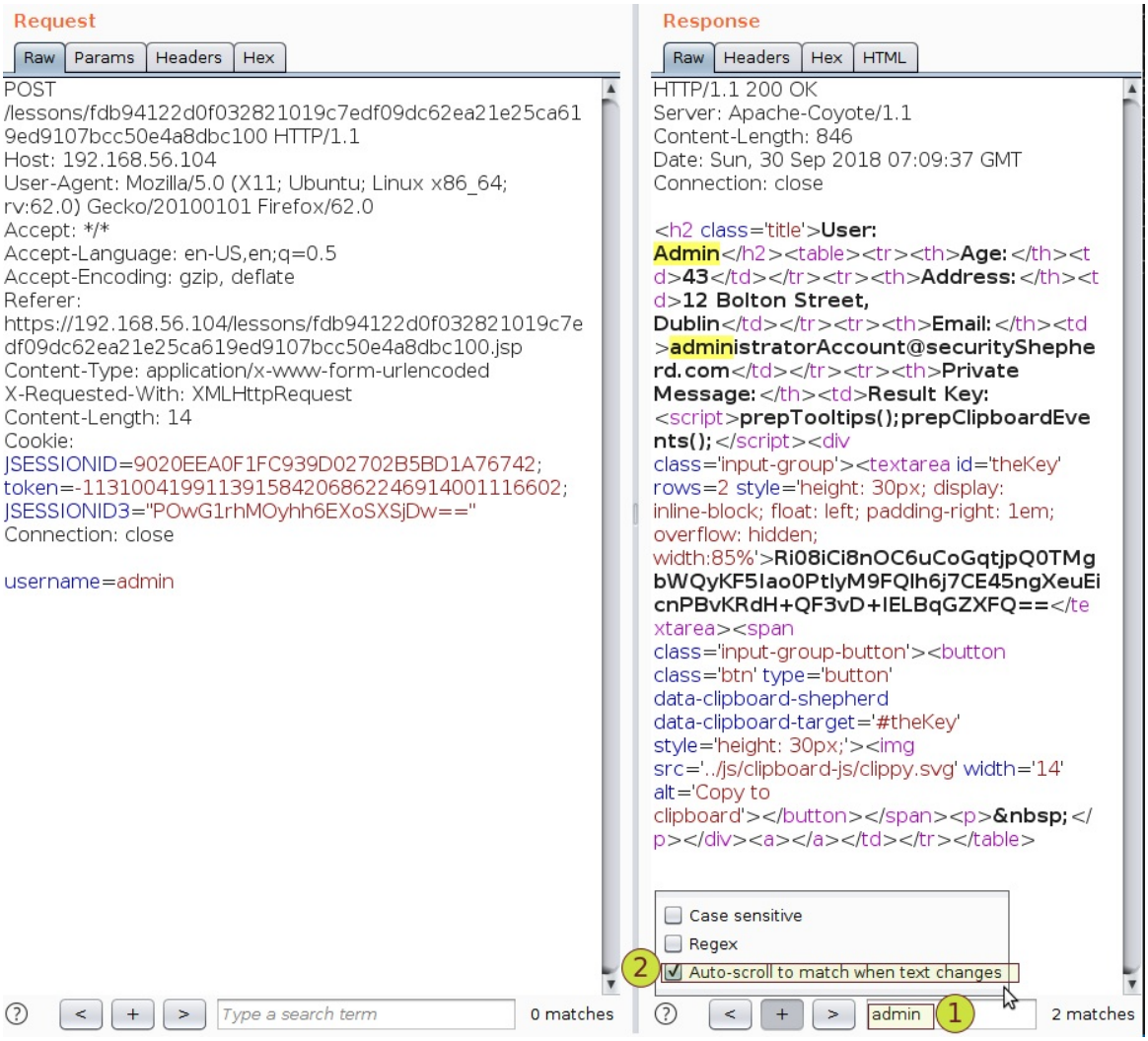
```
User: 404 - User Not Found</h2><p>User 'test' could not be found or does not exist.
```

14. Change the value of "username" parameter to `admin`, and click on the "Go" button.



15. Observe the changes in the response.

16. In "Response" section, enter the keyword "admin" in the search box.
17. Click on plus `+` symbol and select the checkbox labeled as "Auto-scroll to match when text changes".



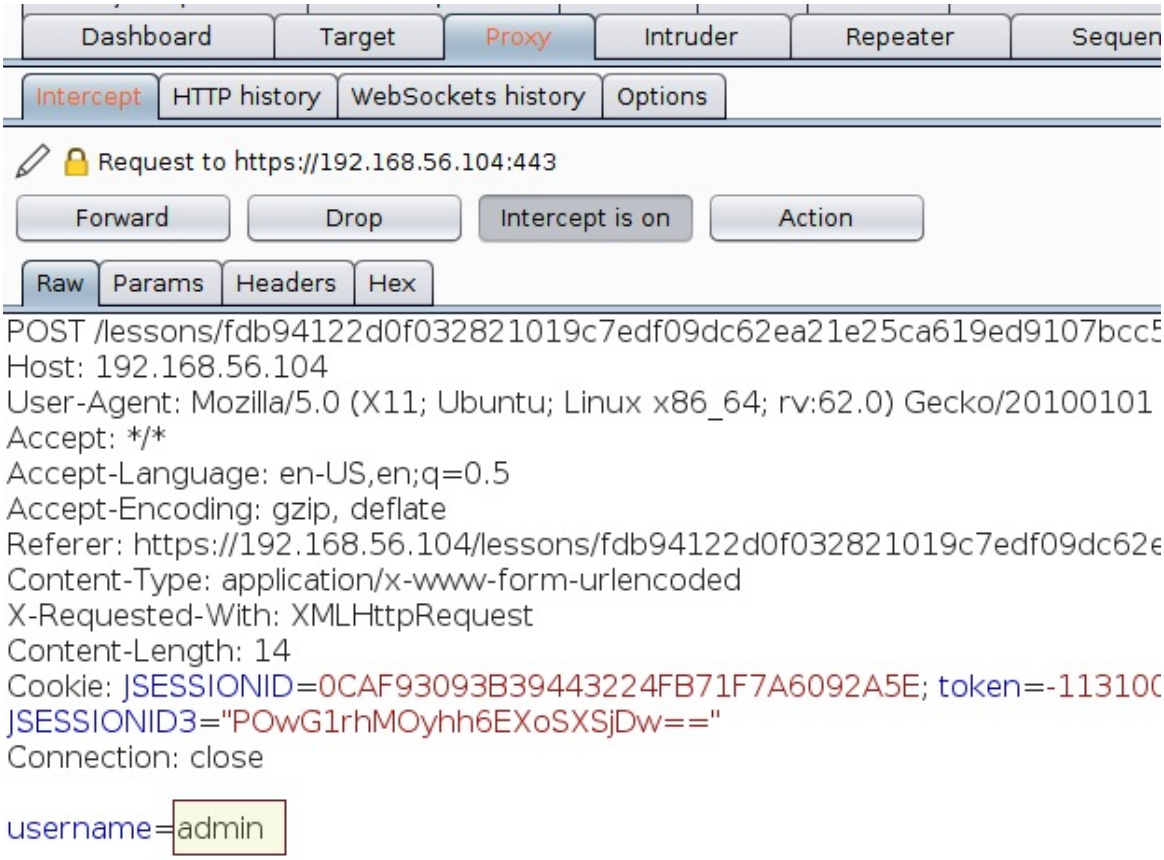
18. To see the previously triggered requests, click on the back arrow symbol.

19. Use the forward arrow symbol to move to the request that was triggered next, after the currently visible request.

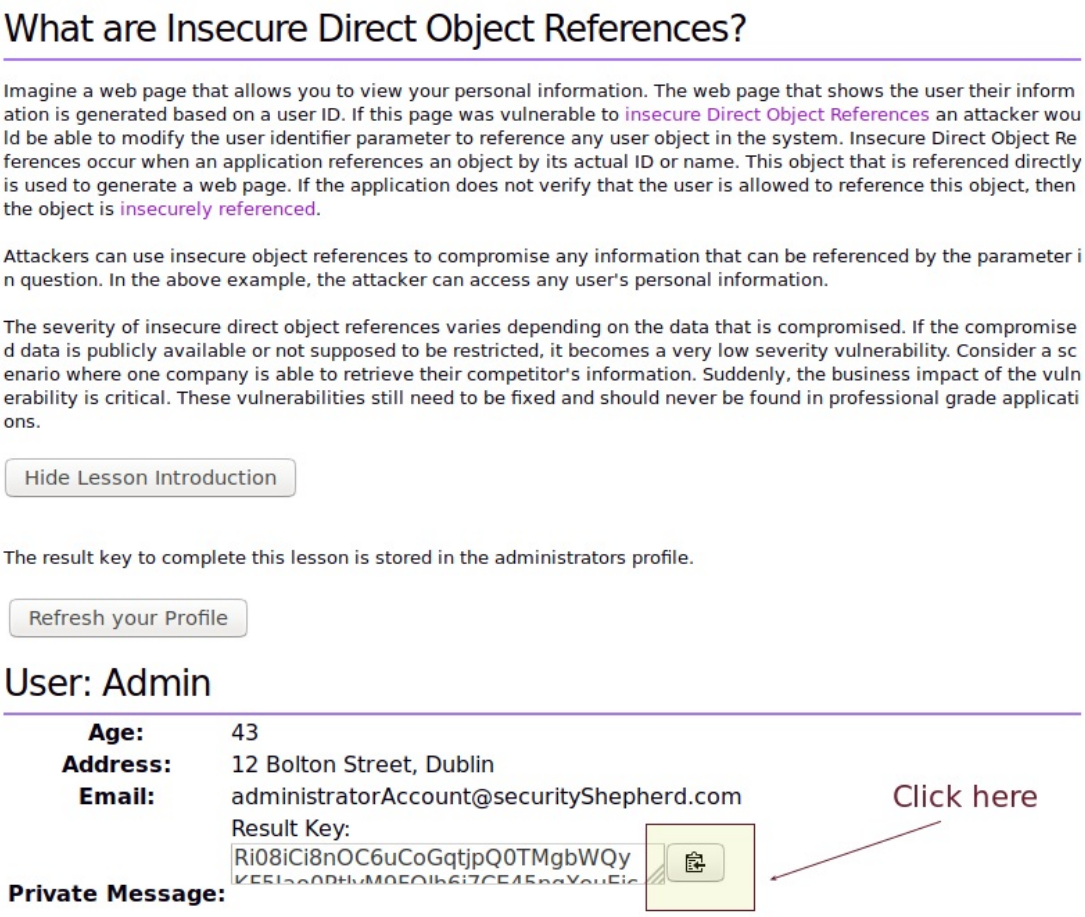
20. Double-click on the tab header to rename a sub-tab in Repeater.

21. Return to Burp > "Proxy" > "Intercept" tab.

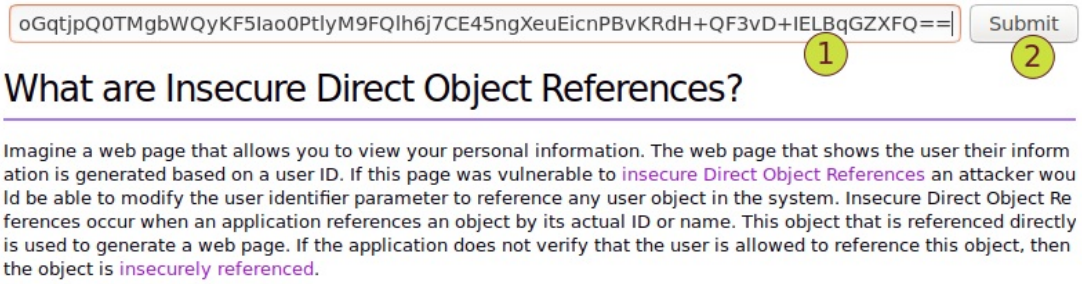
22. Change the value of the "username" parameter to `admin`.



23. Click on "Forward" button.
24. Turn the intercept mode off by clicking on the "Intercept is on" button.
25. In Firefox, you should see the details of the Admin user.
26. Copy the result key by clicking on the "Copy to clipboard" icon.



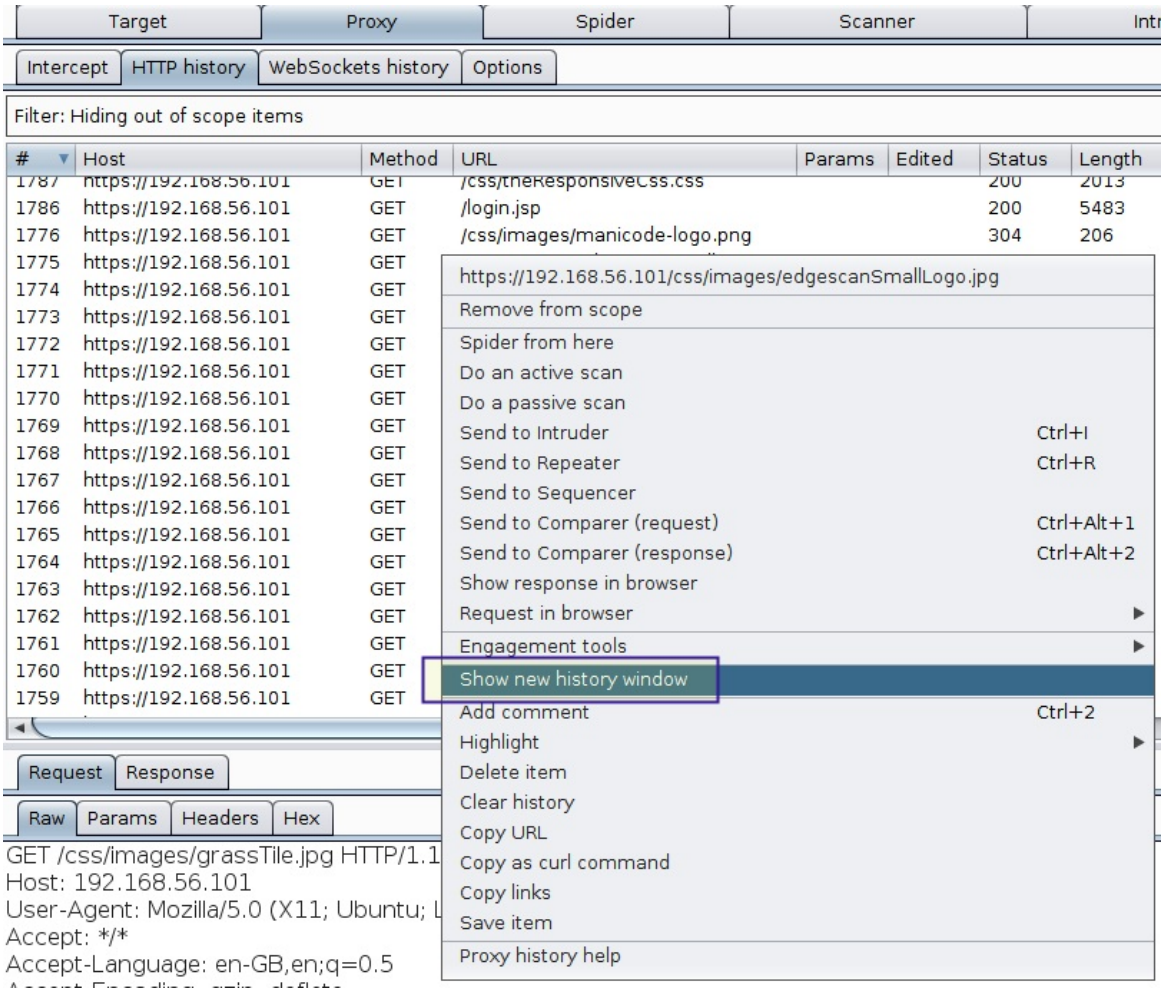
27. Paste the copied text in the result key input box, and submit the result key by clicking on the "Submit" button.



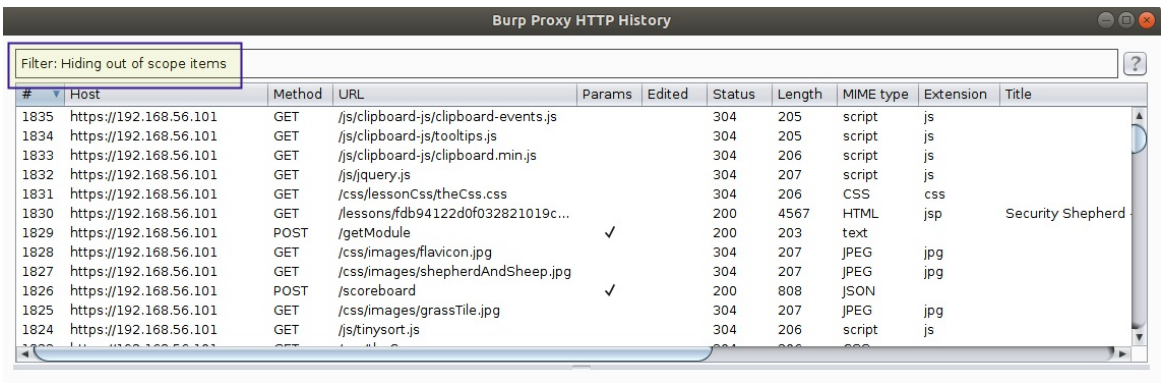
Sequencer (10 Minutes)

This is a sophisticated tool for analyzing the quality of randomness in an application's session tokens or other important data items that are intended to be unpredictable.

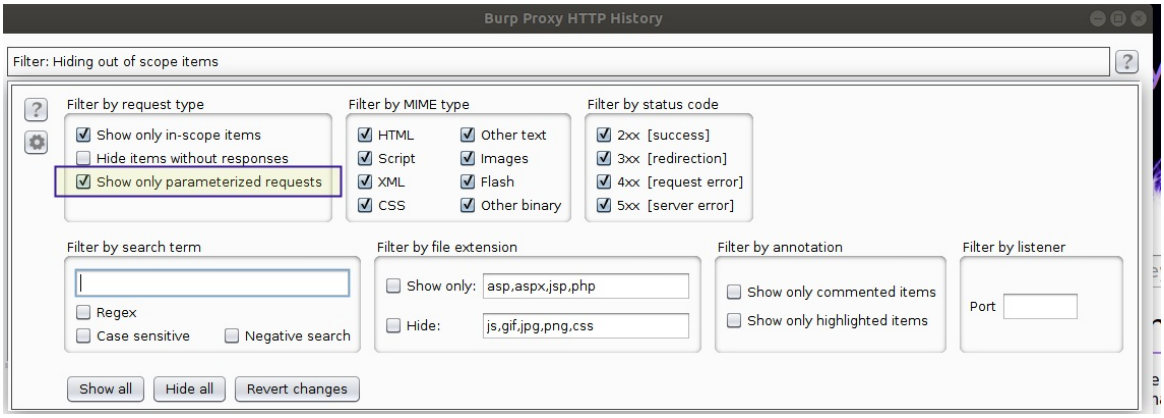
1. Go to Burp > "Proxy" tab > "HTTP history" sub-tab and right-click within the results table to open the context menu.
2. Select "Show new history window" option from the context menu.



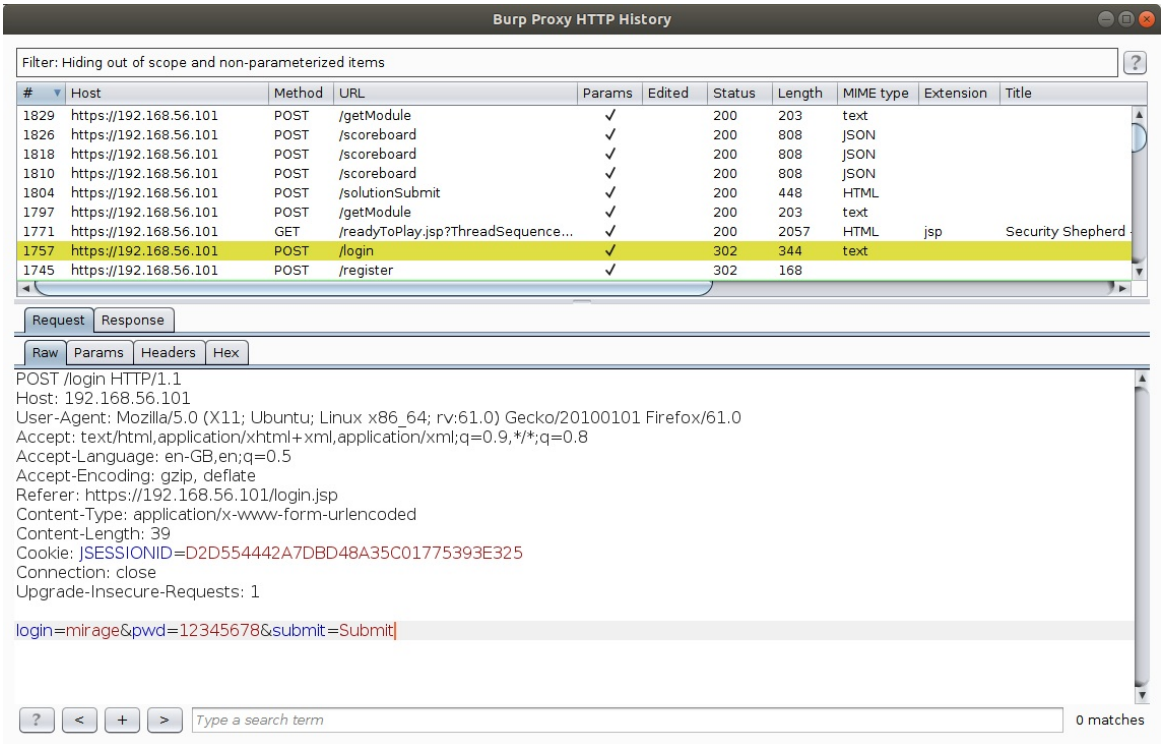
3. In the new "Burp Proxy HTTP History" window, click on "Filter" tab to view the various display filter options.



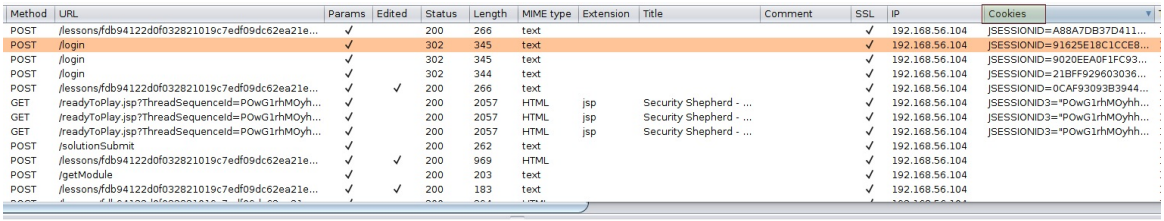
4. In the display filter window, select the checkbox labeled as "Show only parameterized requests".



5. Identify a parameterized request which you may wish to tamper with.

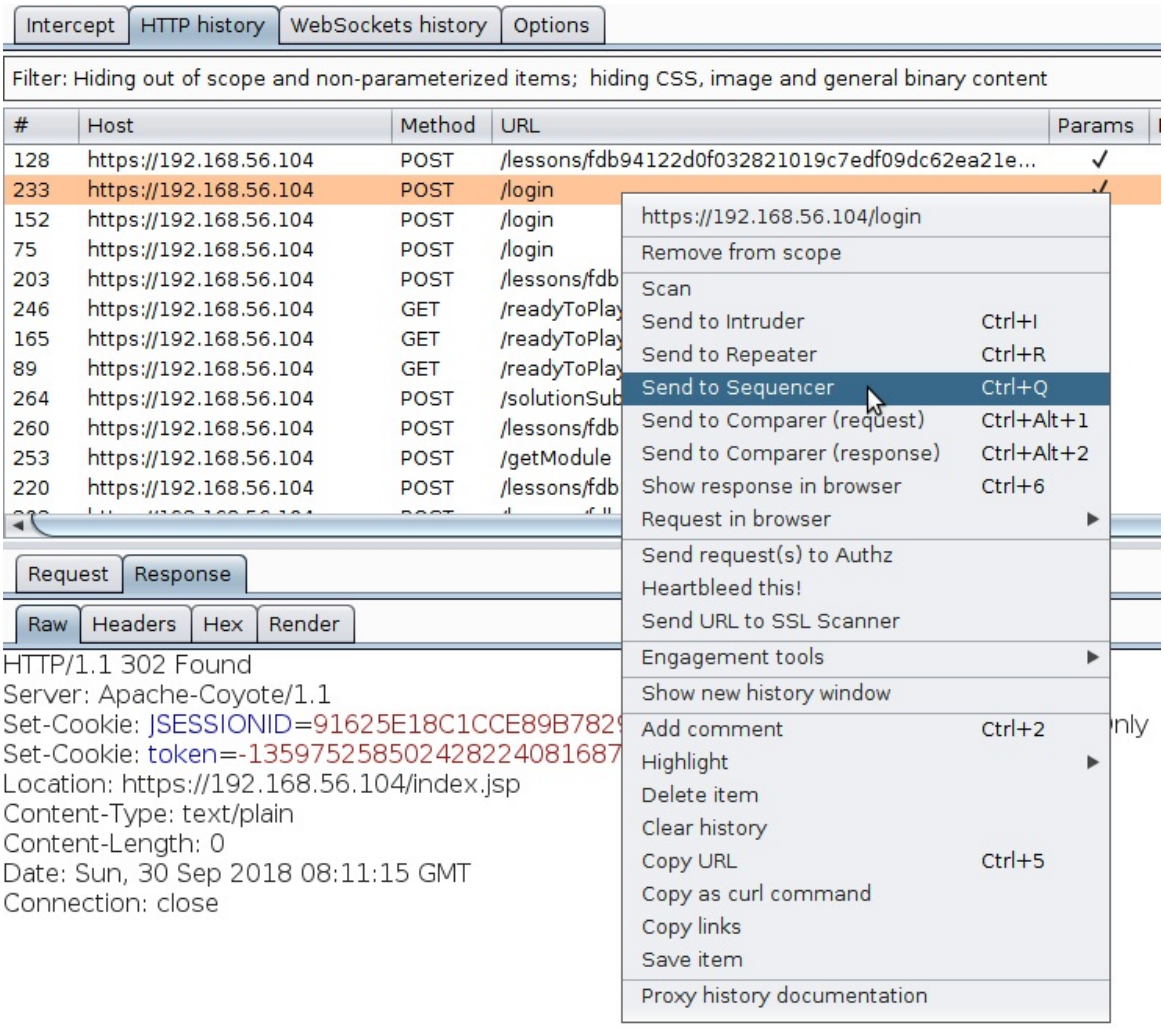


6. Click on the "Cookies" column twice, to identify requests that issue a session token.

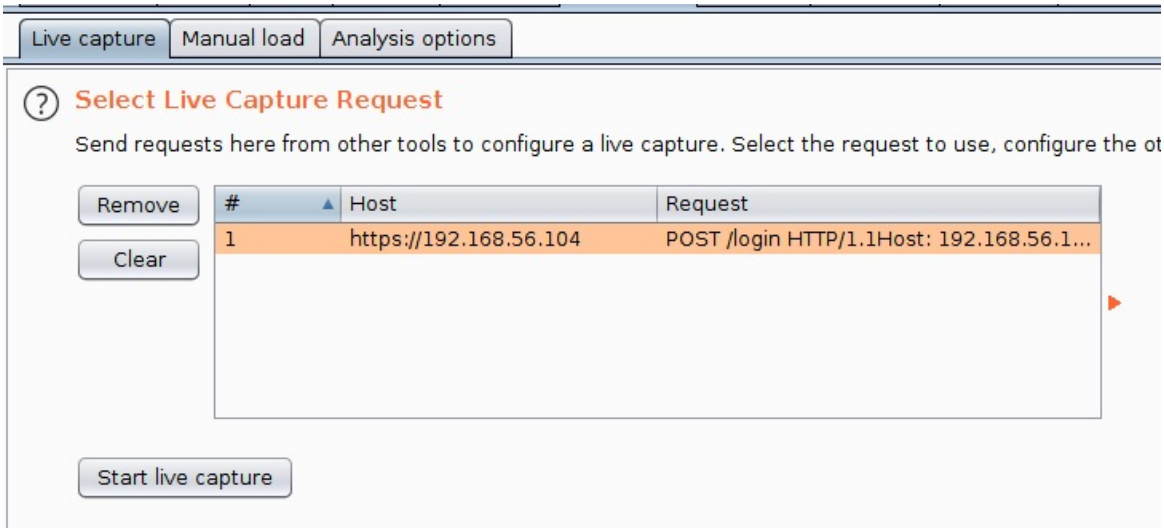


7. Select the `/login` POST request.

8. Right-click on the selected request, and select "Send to Sequencer" option from the context menu.

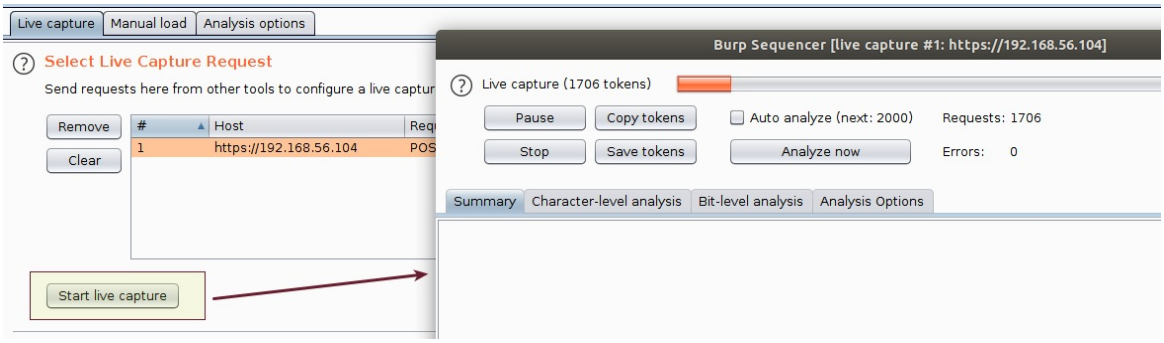


9. Go to "Sequencer" > "Live capture" tab, and in the "Select Live Capture Request" section, select the item that you have just sent.

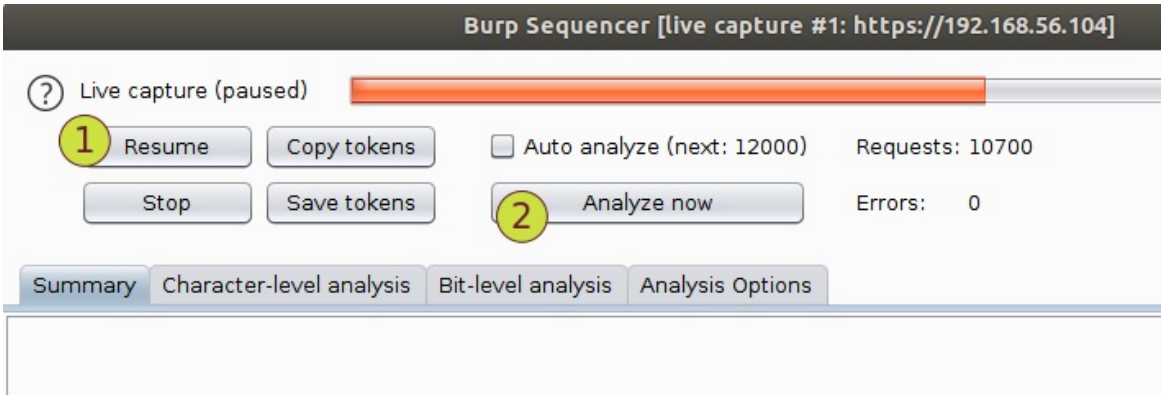


10. In the "Token Location Within Response" section, select the "Cookie" radio button.
11. Select a token from the dropdown menu. For this example, let's select the token named as "token".

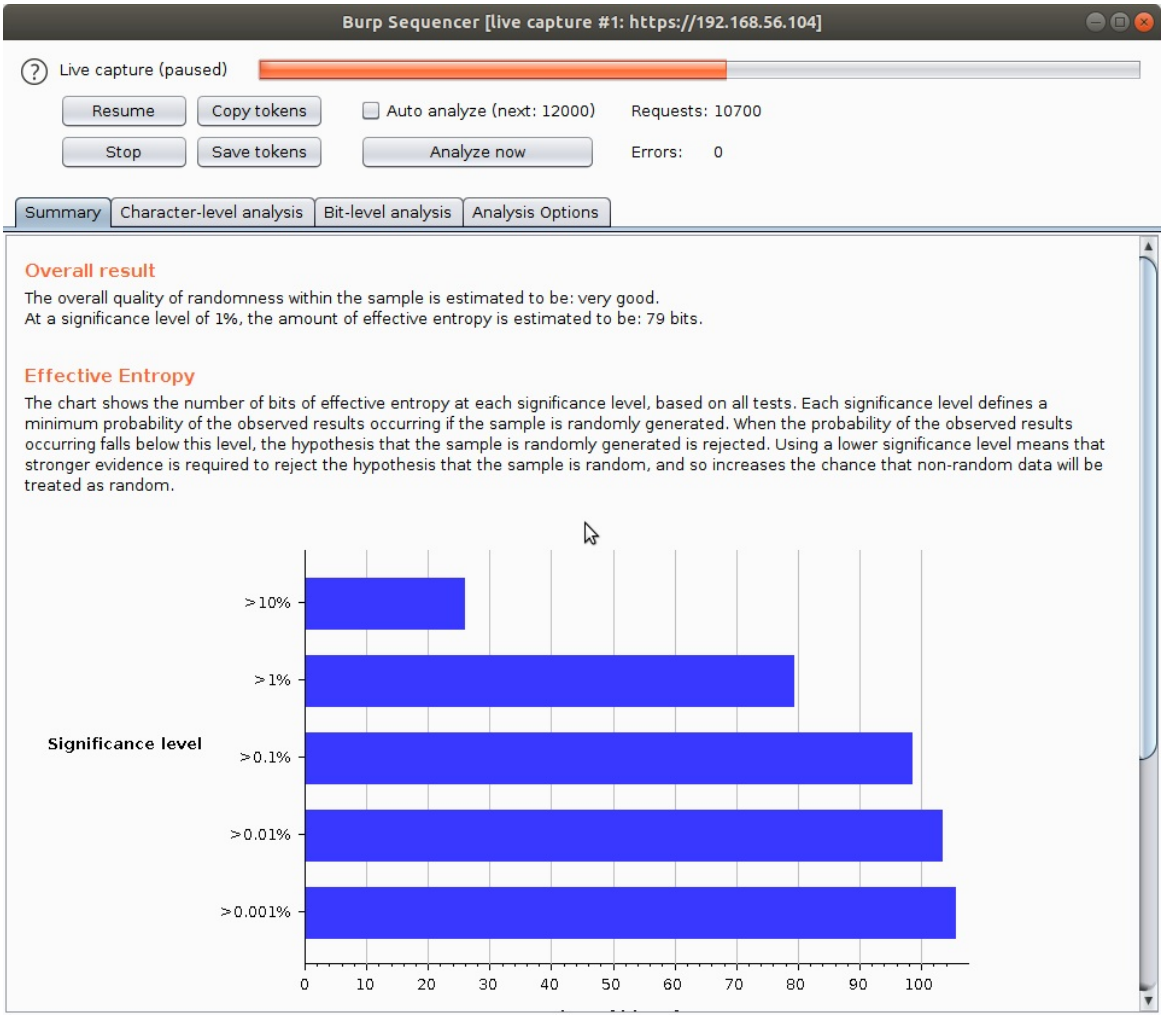
12. Click on the "Start live capture" button.



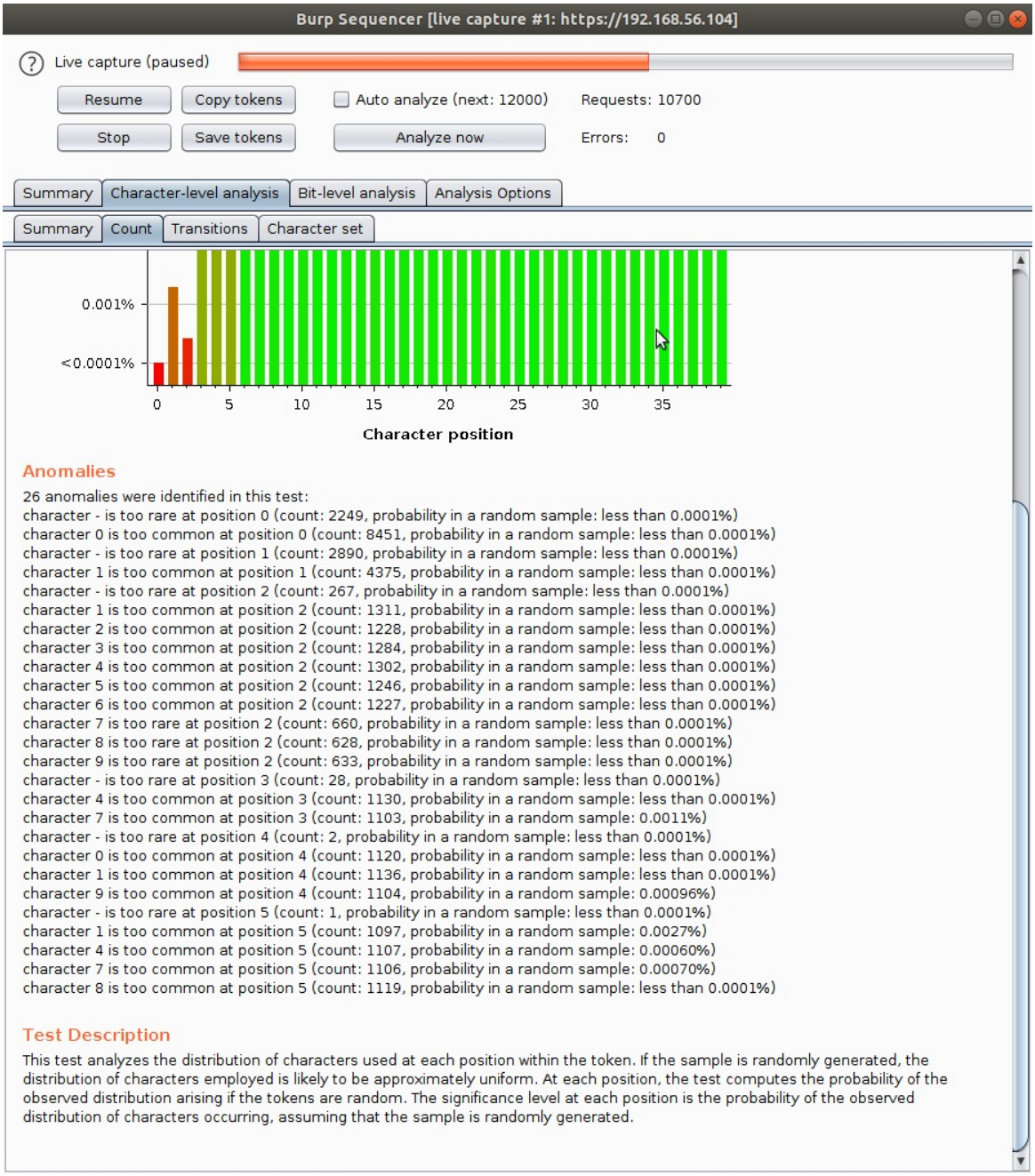
13. When a few hundred tokens have been obtained, pause the live capture session and click the "Analyze now" button.



14. You should see the results of the randomness tests.



15. Go to "Character-level analysis" > "Count" tab and read the details listed under "Anomalies" section.

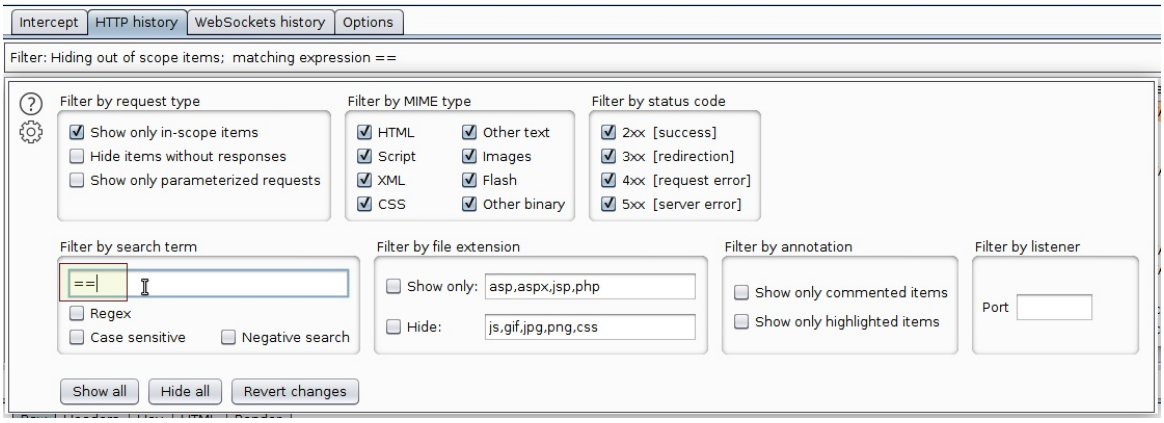


16. Explore the data shown in different tabs and sub-tabs.

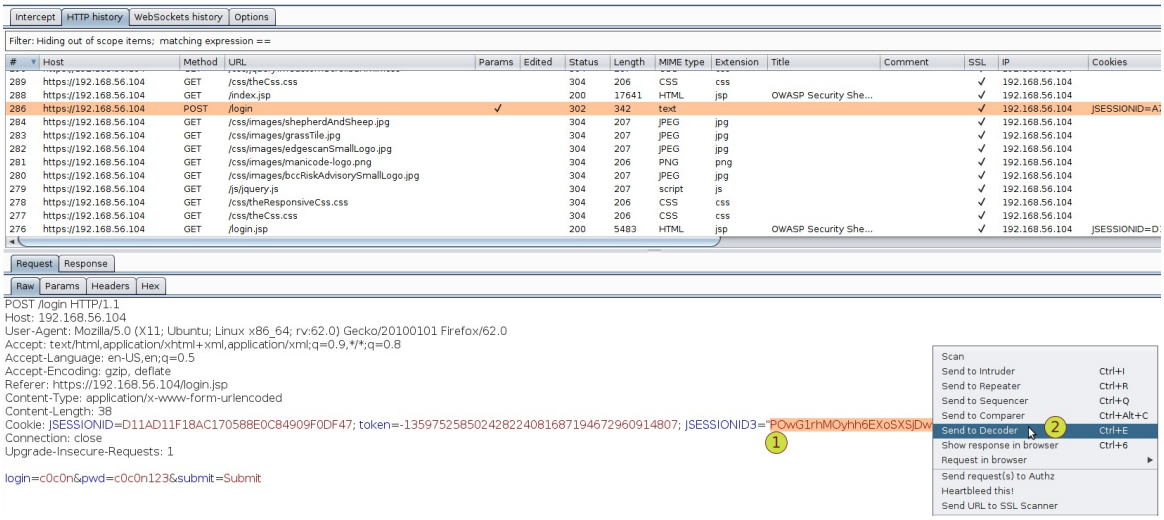
Decoder (10 Minutes)

This is a useful tool for performing manual or intelligent decoding and encoding of application data.

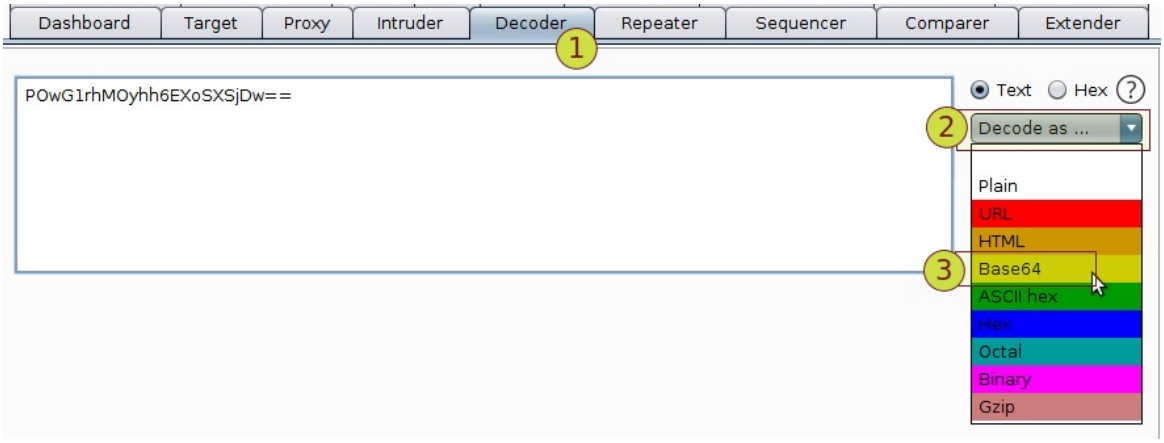
1. In Burp, go to "Proxy" > "HTTP history" tab.
2. Open the display filter by clicking on the filter tab.
3. Enter the search text `==` in the search box under the "Filter by search term" section.



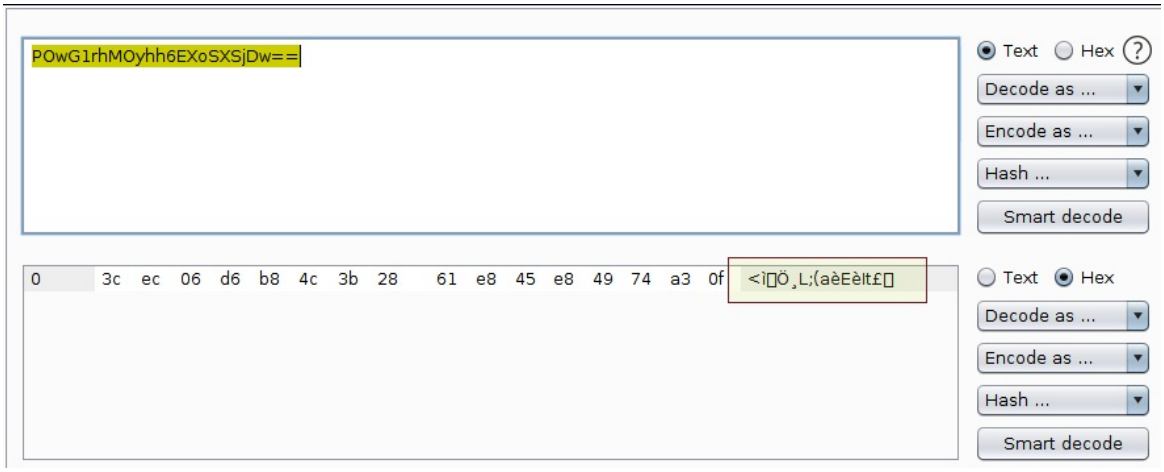
4. Select the POST request to `/login` page.
5. In the request body, select the base64 encoded text value for the parameter "JSESSIONID3".
6. Right-click and select "Send to Decoder" option.



7. Switch to the "Decoder" tab.
8. In Burp > "Decoder" tab, click on the "Decode as ..." dropdown menu, and select "Base64" option from the dropdown list.



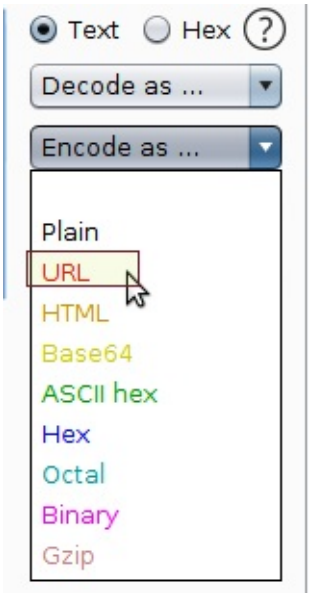
9. You should see the decoded text in a new box.



10. In "Decoder" tab, overwrite the value in the first input box with following value:

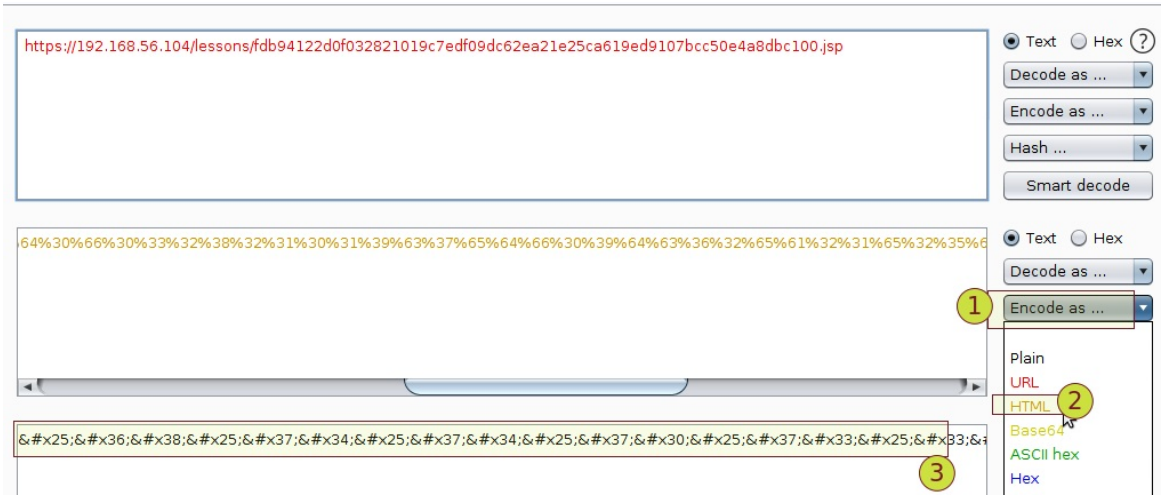
```
https://192.168.56.104/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
```

11. Click on "Encode as ..." > "URL".

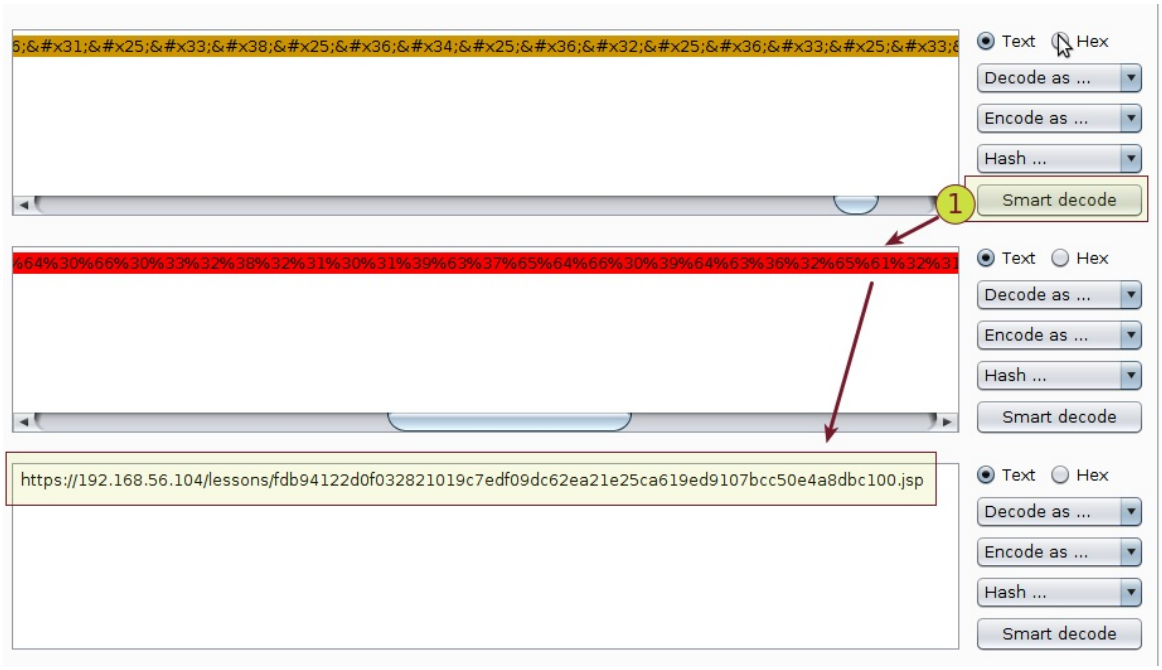


12. The URL encoded value should appear in a new table.

13. Click on "Encode as ..." > "HTML".
14. The HTML encoded value should appear in a new table.



15. Click on "Smart decode" button, against the box that holds (URL + HTML) encoded value, to see the original URL being retrieved automatically by Burp Decoder.



Comparer (10 Minutes)

This is a handy utility for performing a visual "diff" between any two items of data, such as pairs of similar HTTP messages.

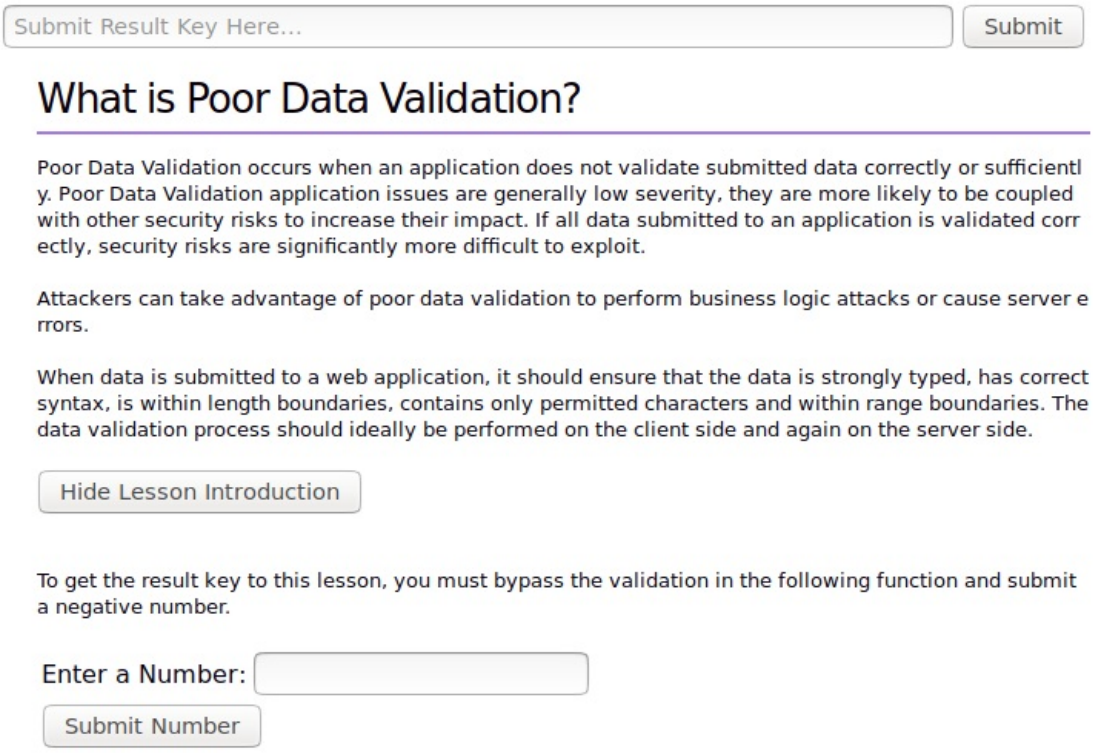
Assumption:

You have already solved the "Insecure Direct Object References" challenge of Security Shepherd.

Steps:

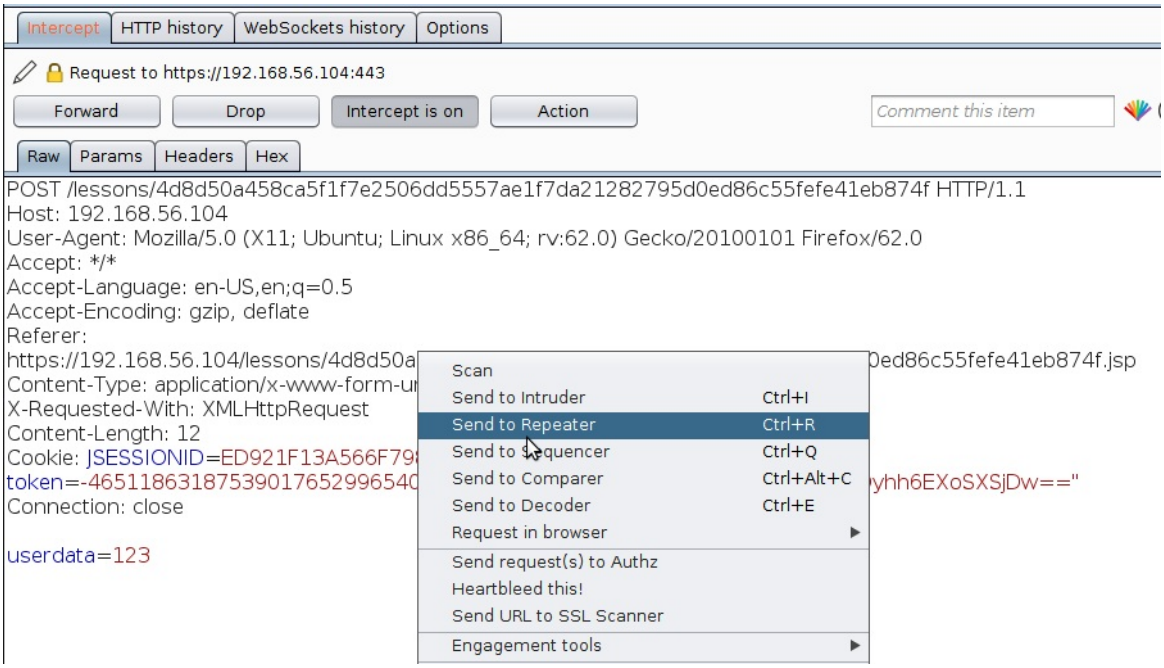
1. Assuming that you have completed the first challenge only, i.e., "Insecure Direct Object References", click on the "Get Next Challenge" button.

2. You should see "Poor Data Validation" challenge.

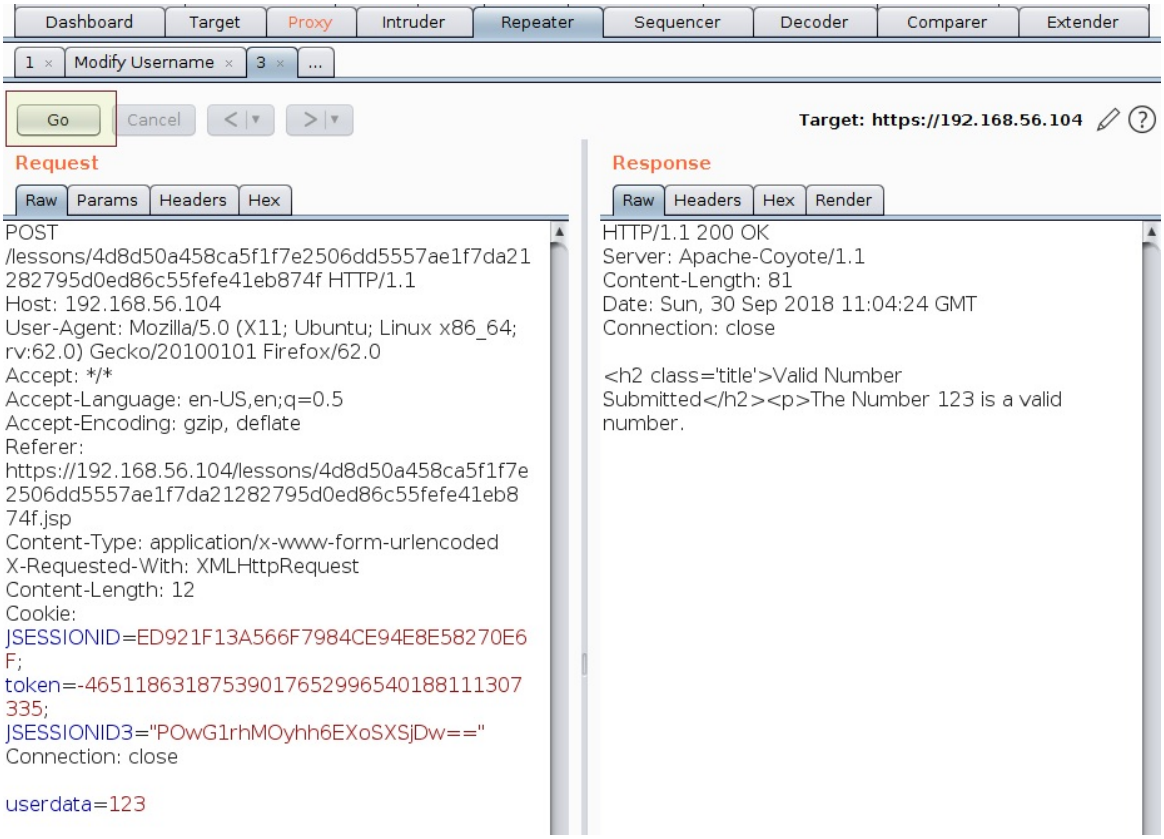


3. Enter `123` in the input field labled as "Enter a Number".
4. Ensure that intercept mode is enabled in Burp.

5. Click on "Submit Number" button.
6. Send the intercepted request to Repeater.

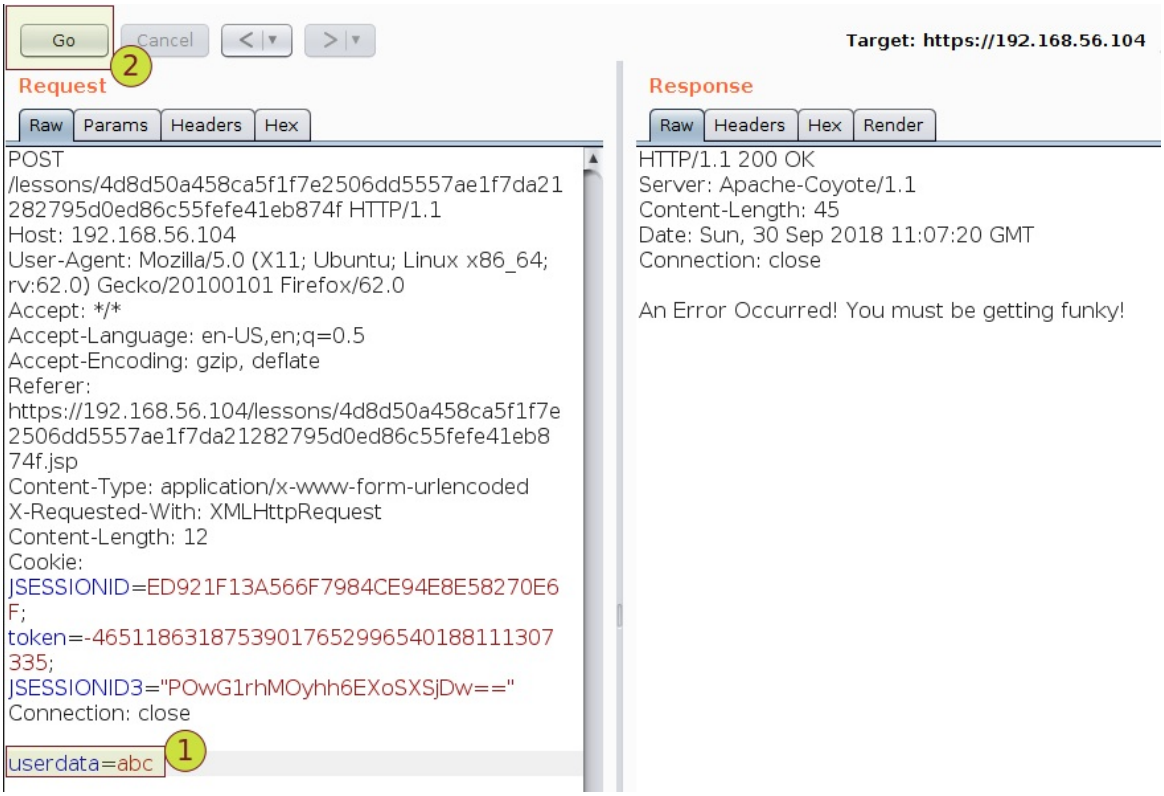


7. Click on "Go" button.

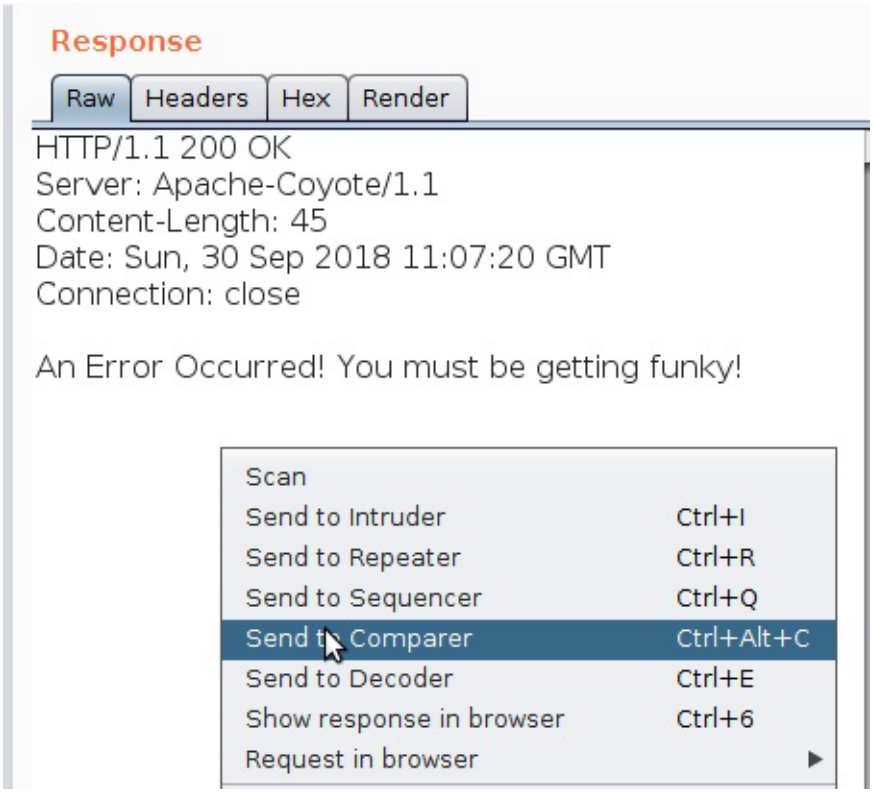


8. Modify the request by changing the value of "userdata" parameter to `abc` .

9. Click on "Go" button.

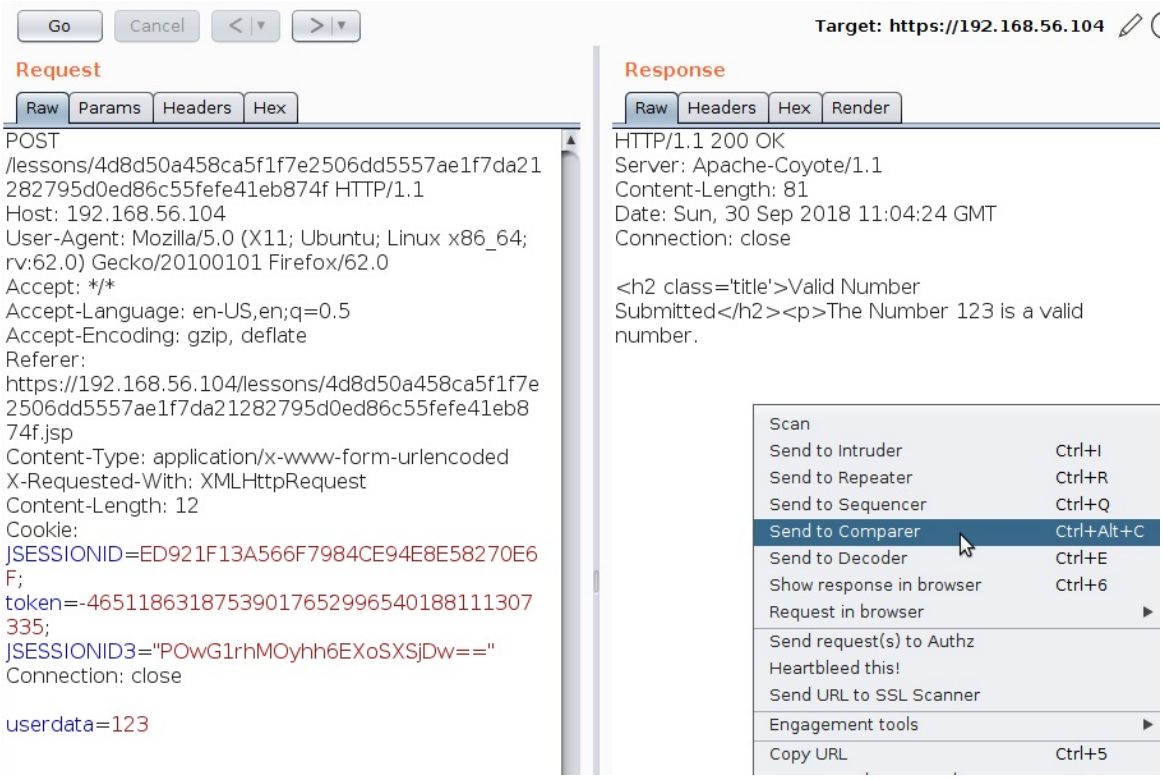


10. Right-click on the response and select "Send to Comparer".



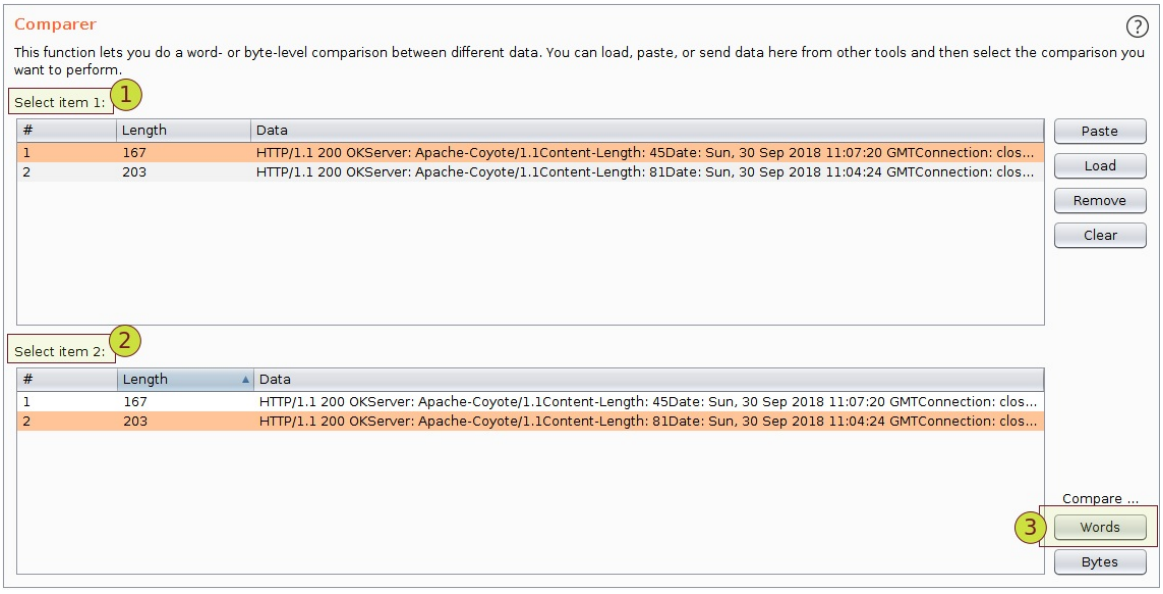
11. Click on the back arrow to see the previously triggered request.

12. Right-click on the response and select "Send to Comparer".

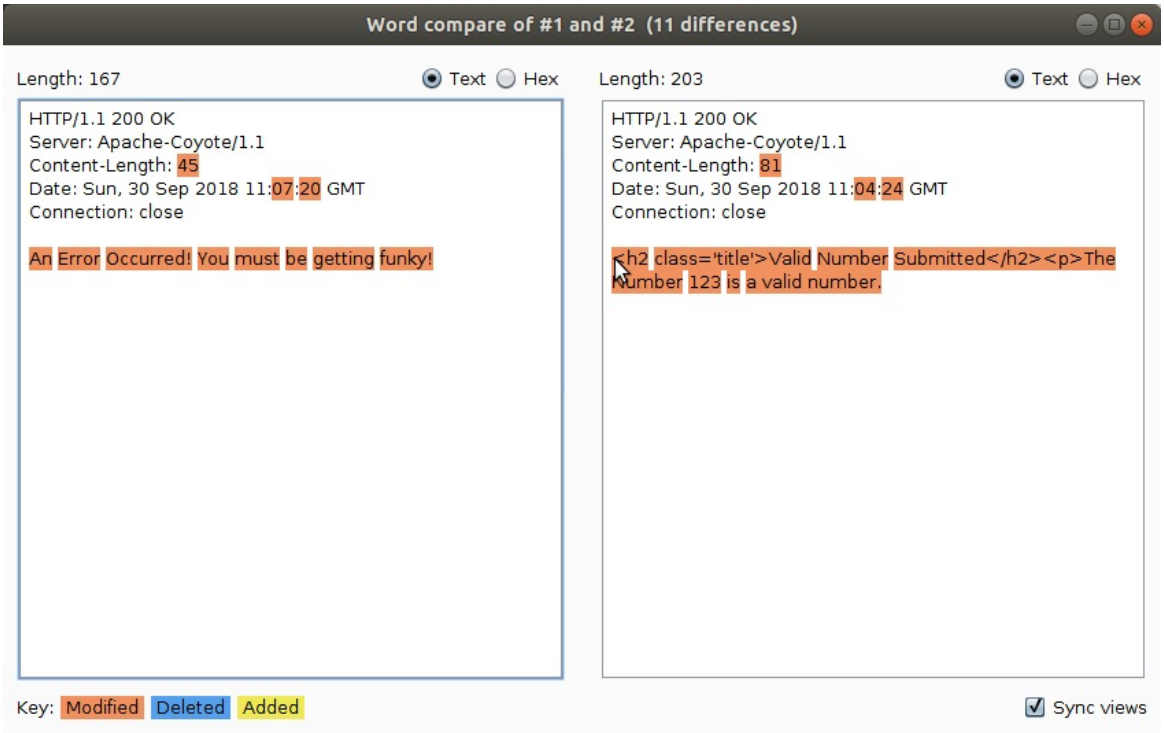


13. Switch to the "Comparer" tab.

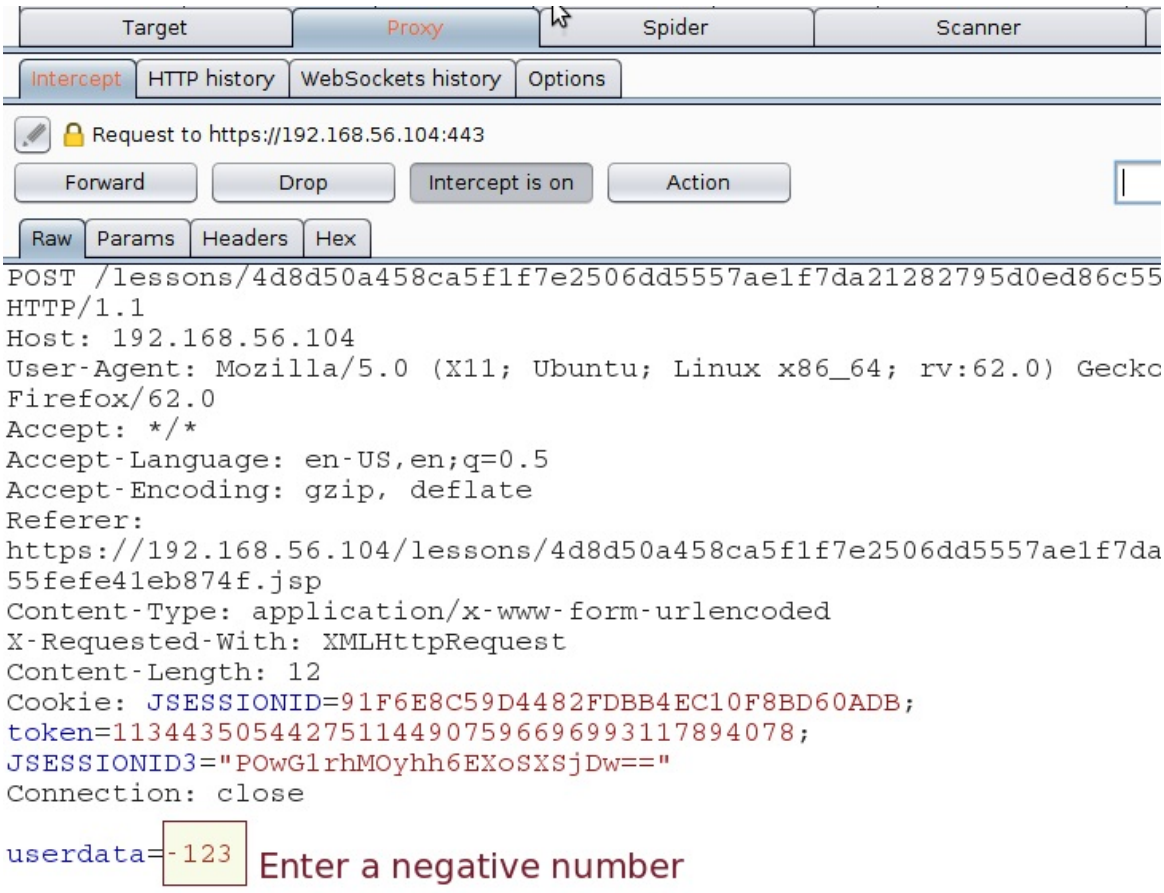
14. Select the first item to compare.
15. Select the second item to compare.



16. Click on the button labeled as "Words", to compare the two selected items word-by-word.

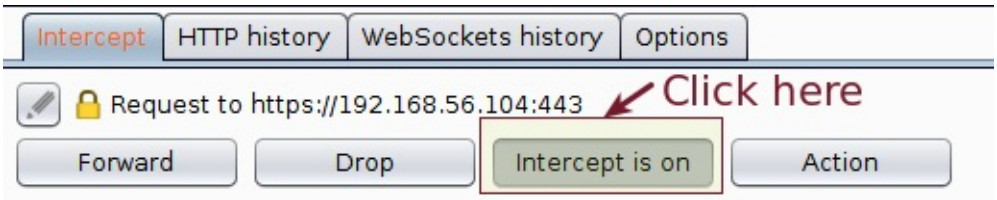


17. Go to "Proxy" > "Intercept" tab.
18. Modify the value of "userdata" input parameter to a negative value, e.g., `-123`



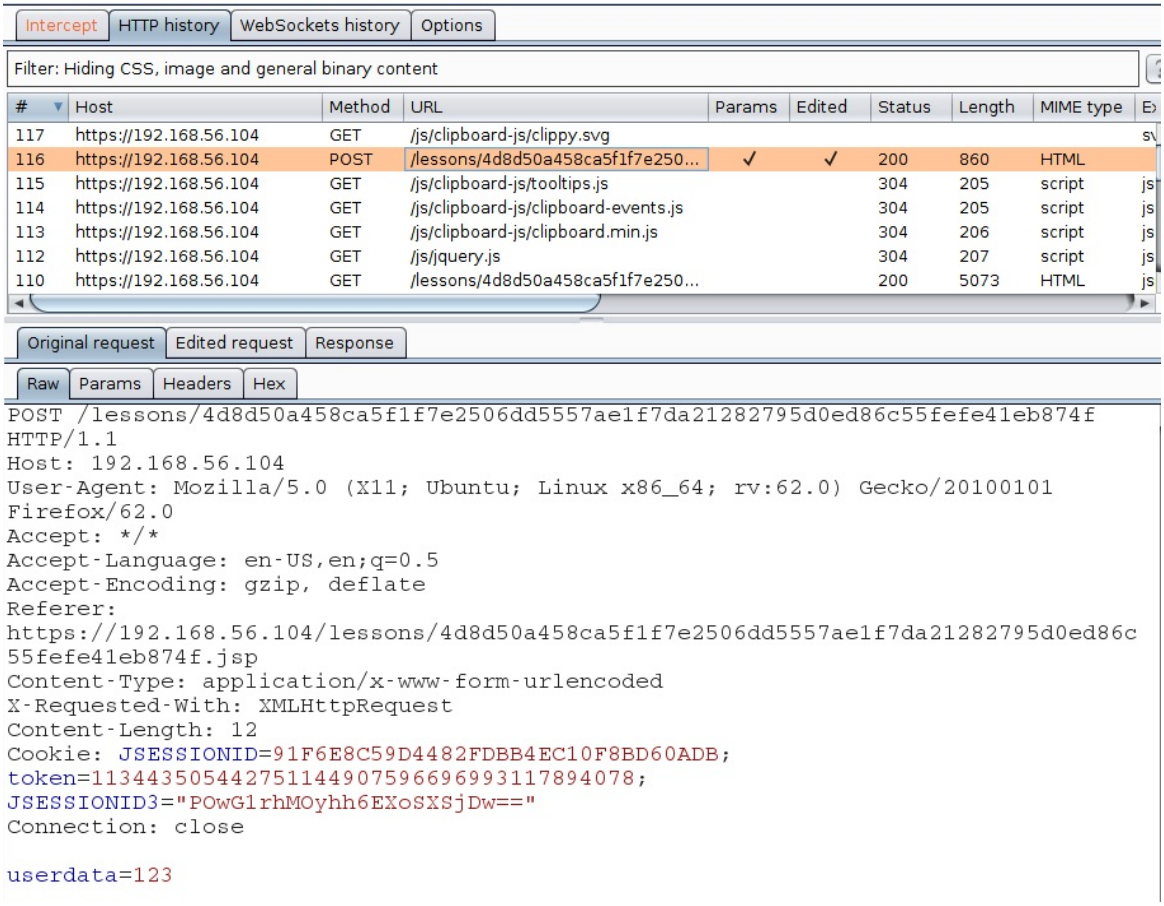
19. Click on "Forward" button.

20. Turn off interception mode by clicking on the "Intercept is on" button.

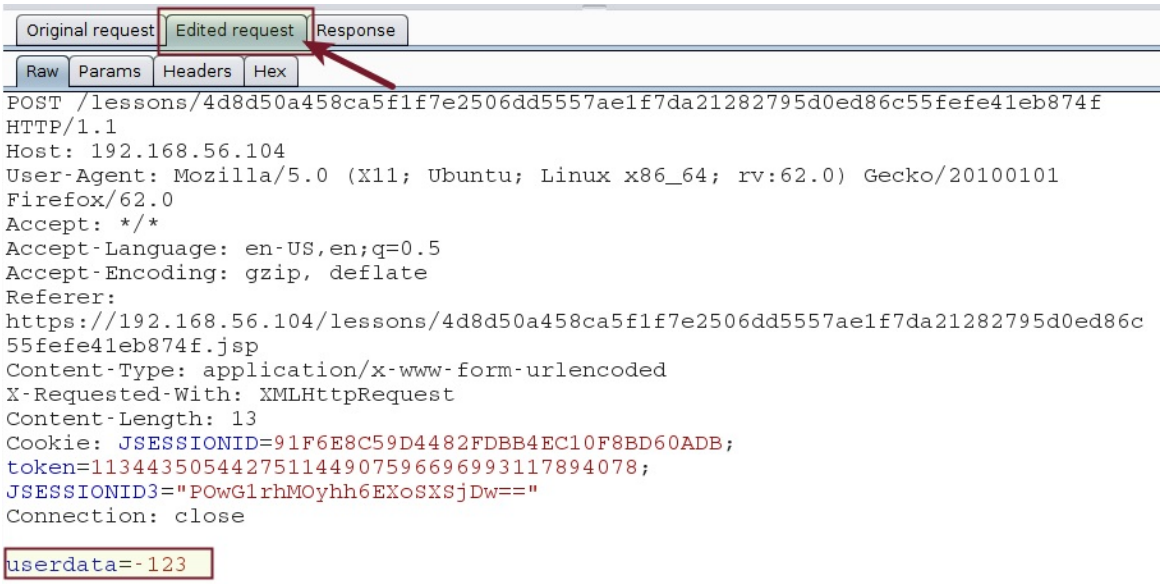


21. Go to "Proxy" > "HTTP history" tab.

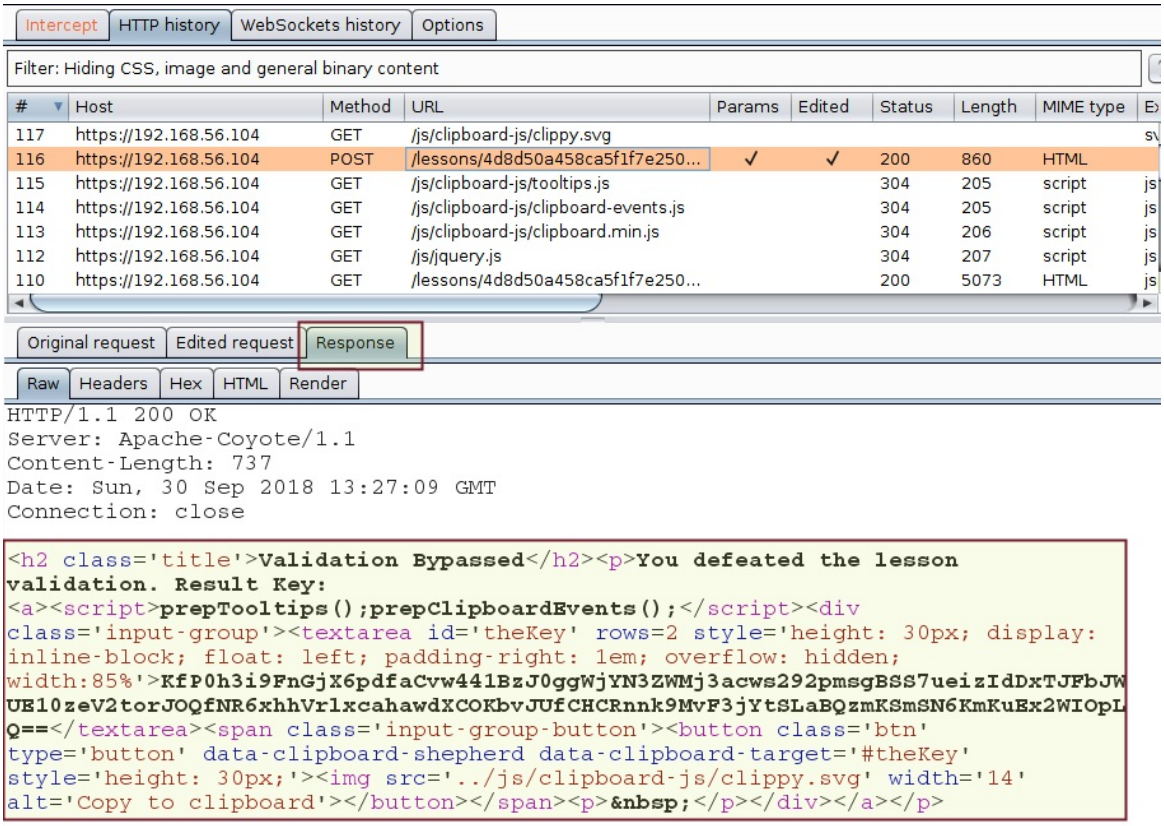
22. Identify the request that you just modified, and select it in the history window.



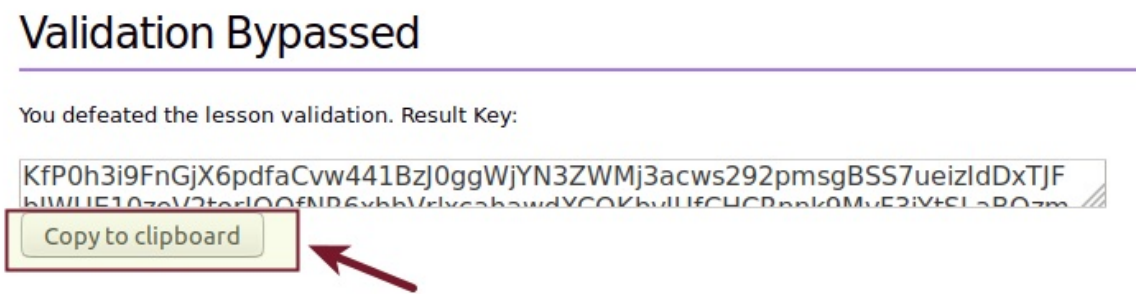
23. Click on "Edited request" sub-tab to see the modified request.



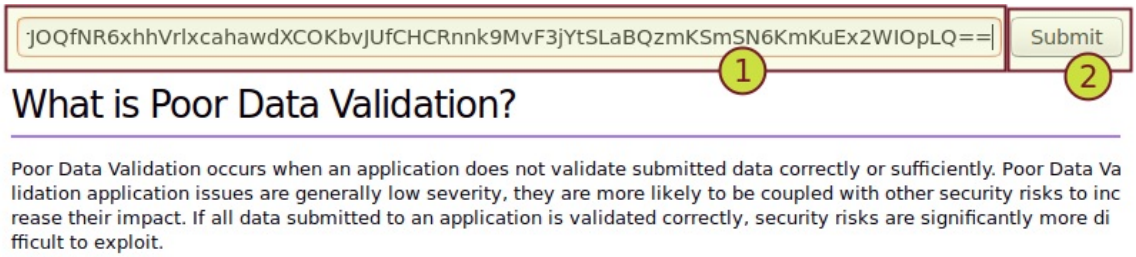
24. Click on "Response" sub-tab to see the response to the modified request.



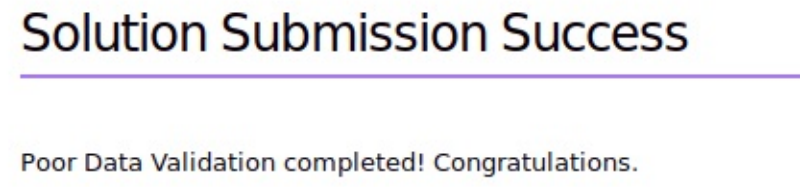
25. In Firefox, click on "Copy to clipboard" button.



26. Paste the copied value into the result key input box, and click on "Submit" button.



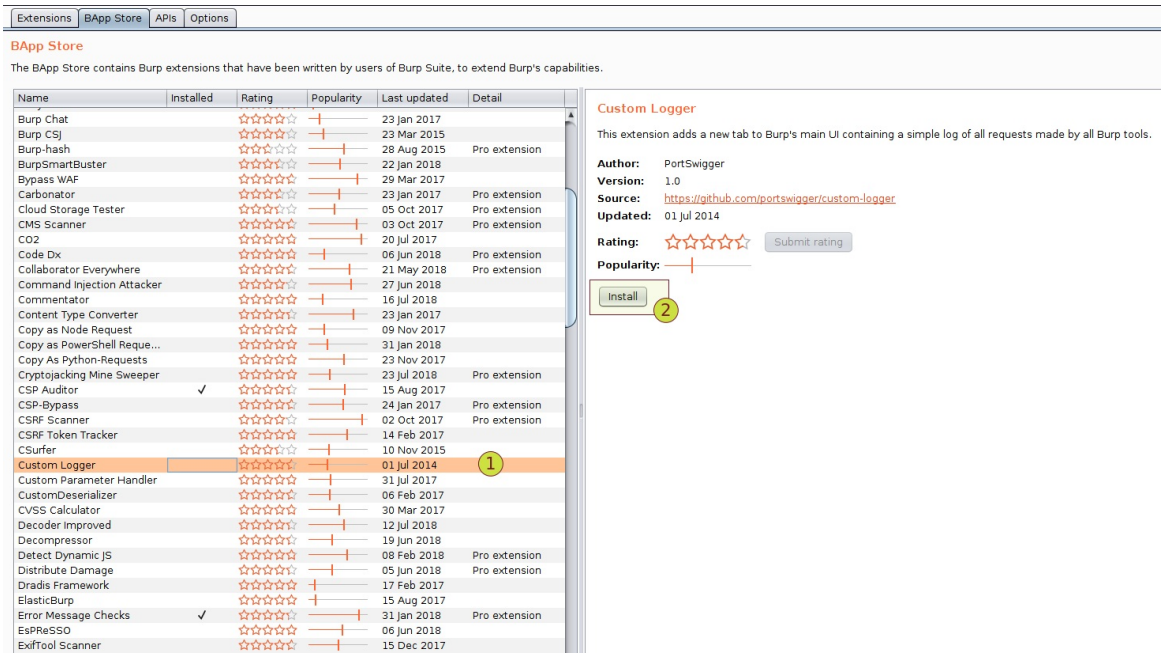
27. You should see a success message on the screen.



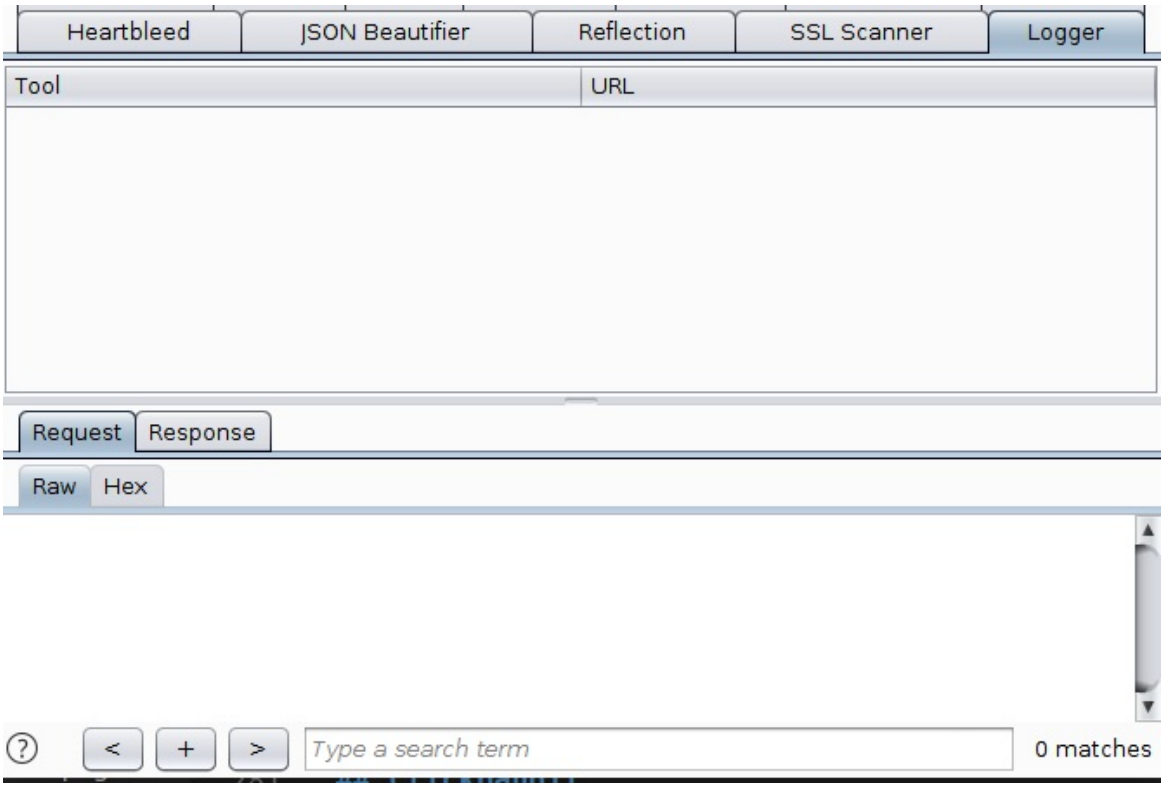
Extender (10 Minutes)

This lets you load Burp extensions, to extend Burp's functionality using your own or third-party code.

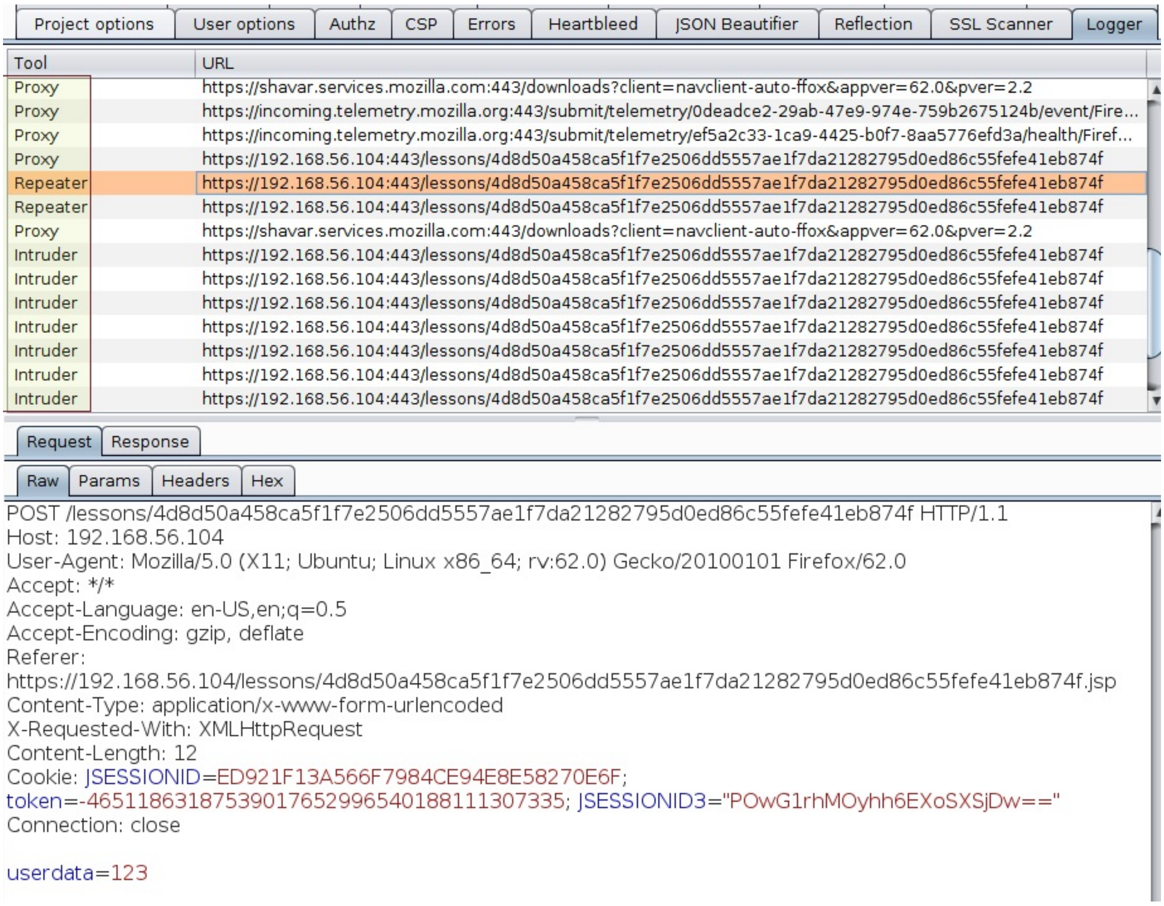
1. In Burp, go to "Extender" > "BApp Store" tab.
2. Select an extension to see its description.
3. Click on "Install" button to install the desired extension.
4. Let's install the "Custom Logger" Burp extension.



5. After successful installation, you should see a new tab named as "Logger" appear in Burp.



6. Browse through the Security Shepherd application.
7. Use "Repeater" to send modified requests to server.
8. Use "Intruder" to launch a brute force attack.
9. Go to the "Logger" tab and observe the logs.



About Appsecco

Appsecco is a specialist application security company, founded in 2015, with physical presence in London, Bangalore, Doha and Boston, providing industry leading security advice that is firmly grounded in commercial reality.

Our services cover the entire software development lifecycle from advising on how to build and foster a culture of security within development teams and organisations, to reviewing and advising on the security of applications and associated infrastructure under development, and also providing rapid response and advice in the event of a security breach or incident.

As a team, we are highly qualified and have many years of extensive experience working with clients across multiple counties and in a wide range of industries and sectors; from financial services to software development, manufacturing to governmental organisations and consumer brands to ecommerce.

The solutions, advice and insight that we deliver to our clients always follow the three core principles:

1. It must be pragmatic; taking into account the specific commercial, organisational and operational realities of each client individually
2. It must genuinely add value; the advice or solutions we provide must address the specific problem a client seeks to solve and must include actionable insights to enable them to achieve this
3. Never be purely automated; whenever we are testing for security issues, our reports and output always include significant, expert, human inputs to give the greatest possible value for our clients

In addition to client-facing work, our technical teams are actively involved in researching and developing new and better ways to stay secure and can regularly be found presenting their findings at industry conferences and events ranging from nullcon in India, DevSecCon in London and Singapore, to DEF CON, the world's largest security conference held annually in the USA.

Appsecco: https://appsecco.com