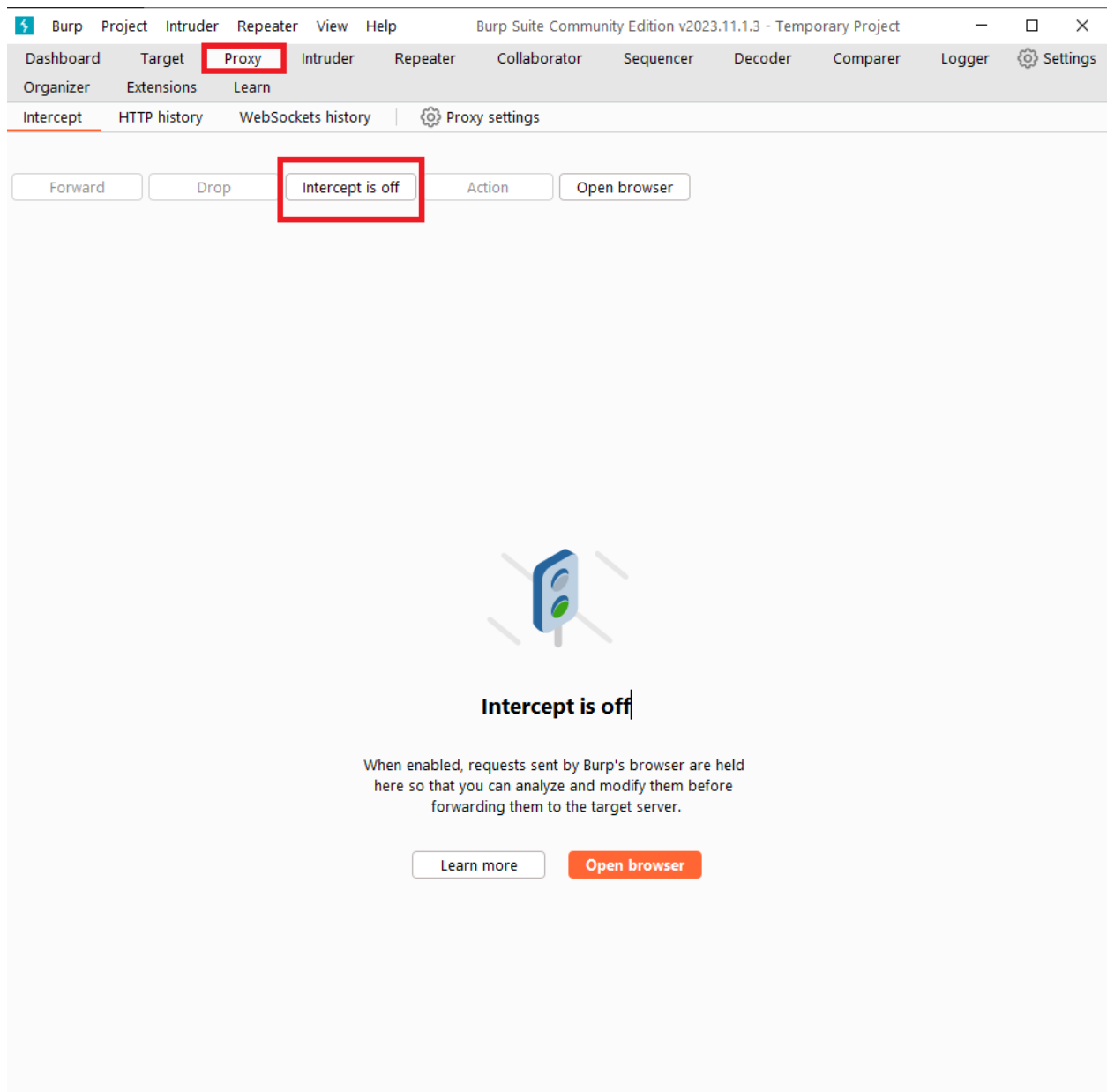


Burp Suite Login Bypass (Brute-Force)

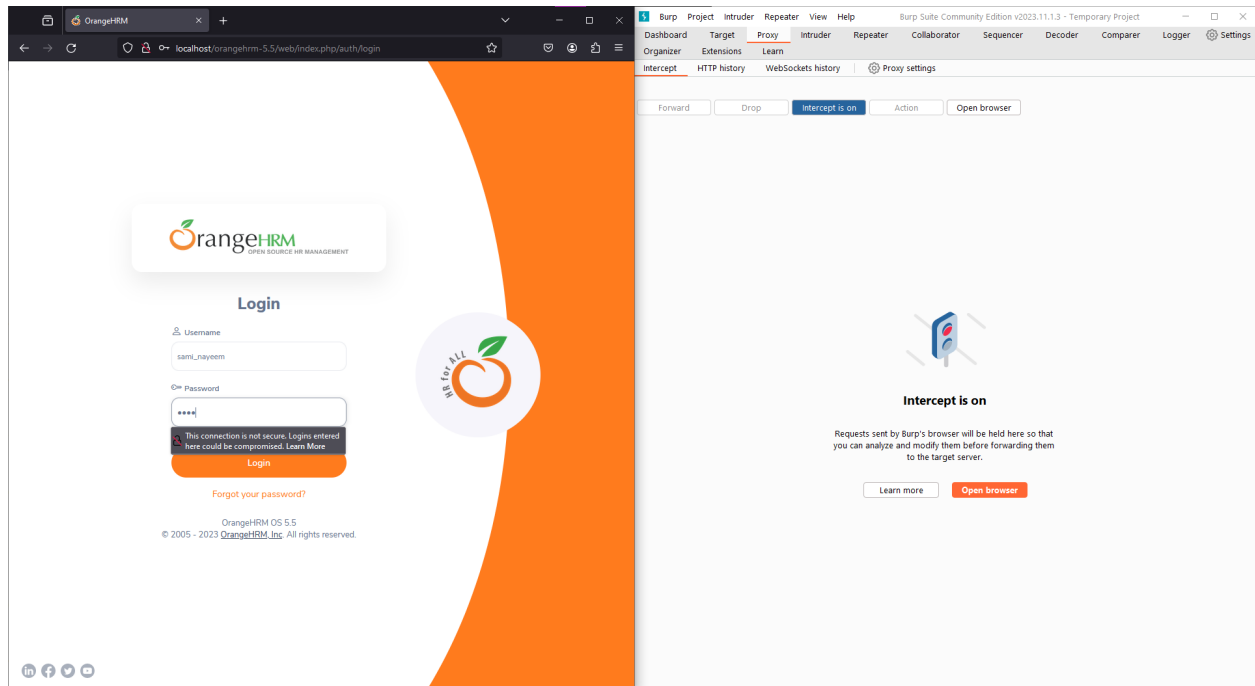
Step 01. Launch Burp Suite and create a new project

Step 02. Open the project in a browser where the Burp Suite certificate is imported

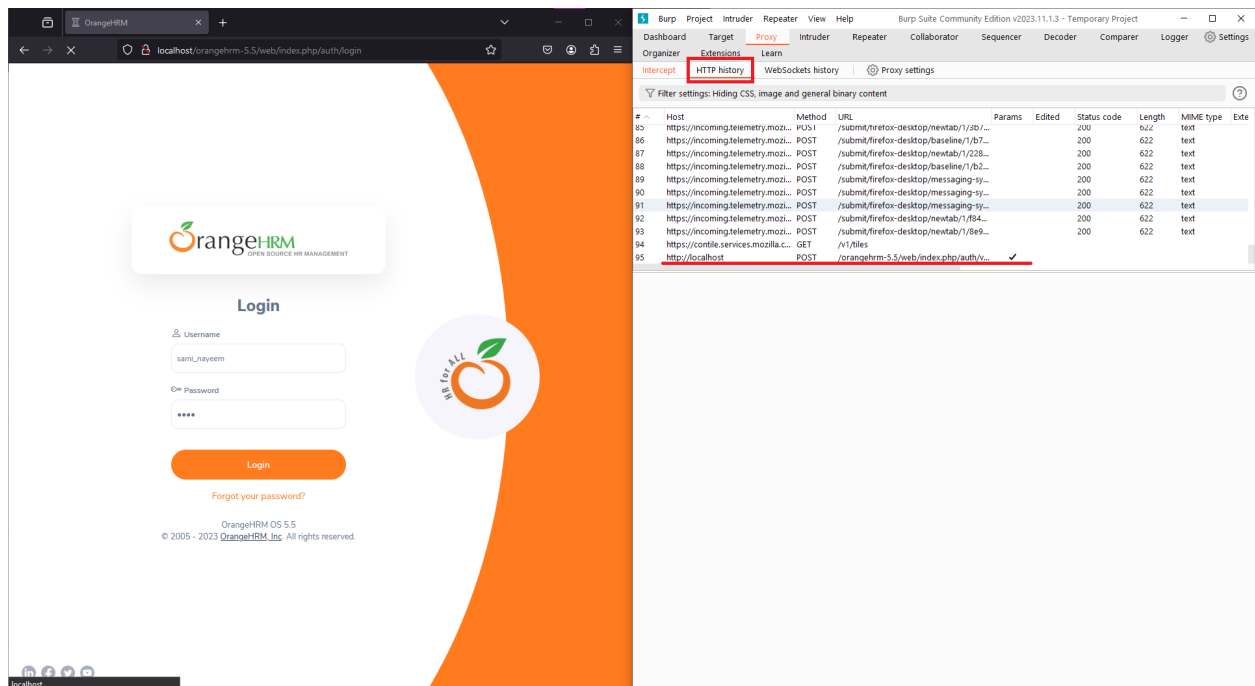
Step 03. Turn on the intercept in proxy tab in Burp Suite



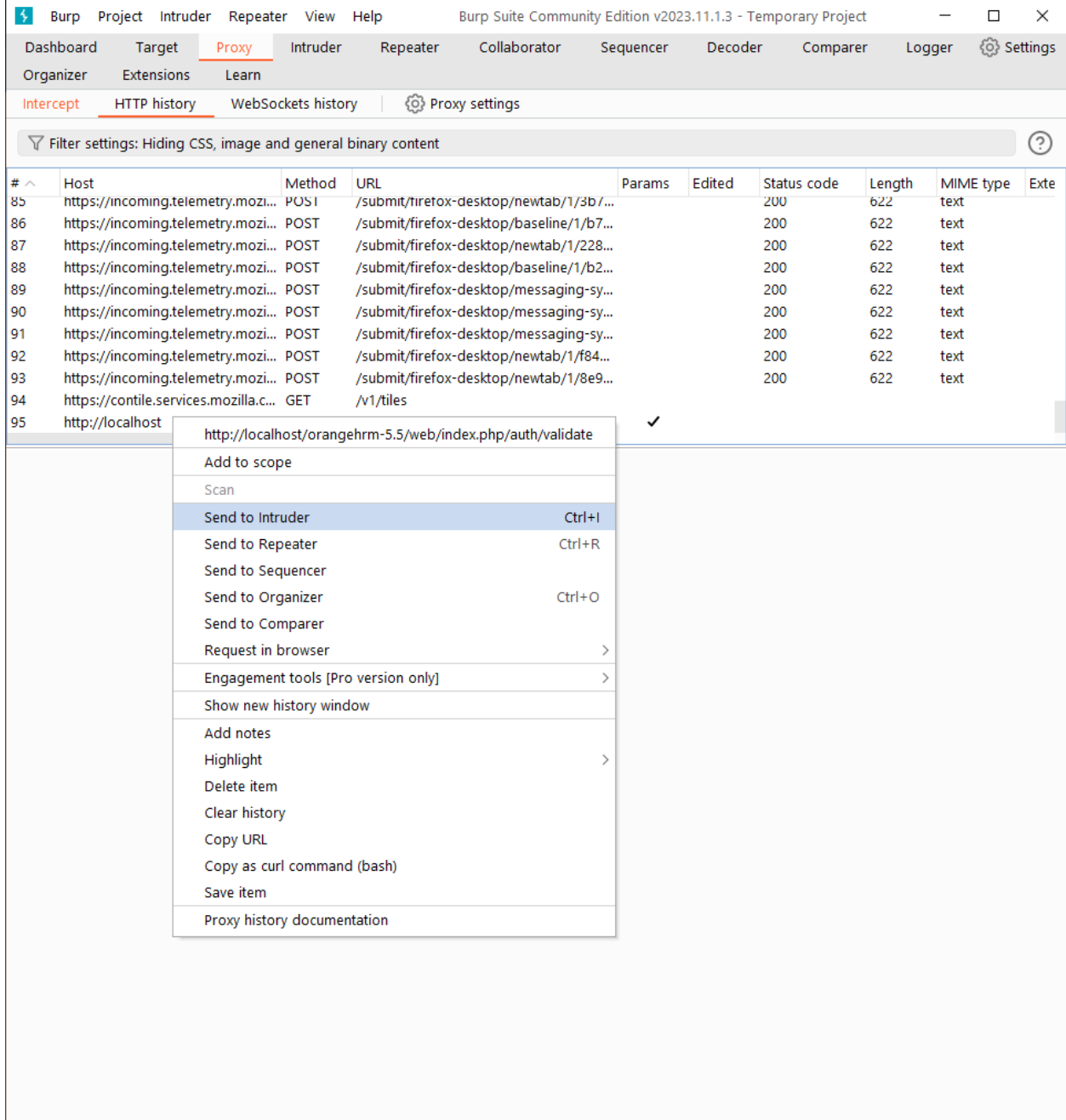
Step 04. Try to login using a random credentials



Step 05. Under the proxy tab move to HTTP history and search for the http request for login.



Step 06. Right click on the request and send it to intruder.



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'HTTP history' sub-tab is active, displaying a list of intercepted requests. The selected request (row 95) is a GET request to 'http://localhost'. A right-click context menu is open over this request, showing various actions. The 'Send to Intruder' option is highlighted, and a checkmark is visible next to the selected URL in the menu.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Ext
85	https://incoming.telemetry.moz...	POST	/submit/firefox-desktop/newtab/1/3b / ...			200	622	text	
86	https://incoming.telemetry.moz...	POST	/submit/firefox-desktop/baseline/1/b7...			200	622	text	
87	https://incoming.telemetry.moz...	POST	/submit/firefox-desktop/newtab/1/228...			200	622	text	
88	https://incoming.telemetry.moz...	POST	/submit/firefox-desktop/baseline/1/b2...			200	622	text	
89	https://incoming.telemetry.moz...	POST	/submit/firefox-desktop/messaging-sy...			200	622	text	
90	https://incoming.telemetry.moz...	POST	/submit/firefox-desktop/messaging-sy...			200	622	text	
91	https://incoming.telemetry.moz...	POST	/submit/firefox-desktop/messaging-sy...			200	622	text	
92	https://incoming.telemetry.moz...	POST	/submit/firefox-desktop/newtab/1/f84...			200	622	text	
93	https://incoming.telemetry.moz...	POST	/submit/firefox-desktop/newtab/1/8e9...			200	622	text	
94	https://contile.services.mozilla.c...	GET	/v1/tiles						
95	http://localhost		http://localhost/orangehrm-5.5/web/index.php/auth/validate						

- http://localhost/orangehrm-5.5/web/index.php/auth/validate
- Add to scope
- Scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Organizer Ctrl+O
- Send to Comparer
- Request in browser >
- Engagement tools [Pro version only] >
- Show new history window
- Add notes
- Highlight >
- Delete item
- Clear history
- Copy URL
- Copy as curl command (bash)
- Save item
- Proxy history documentation

Step 07. Move to intruder tab and then select the password and add marker

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The top menu bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'View', and 'Help'. The main toolbar contains 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Collaborator', 'Sequencer', 'Decoder', 'Comparer', 'Logger', and 'Settings'. Below the toolbar, there are tabs for 'Positions', 'Payloads', 'Resource pool', and 'Settings'. The 'Positions' tab is active, showing the 'Choose an attack type' section with a dropdown menu set to 'Sniper' and a 'Start attack' button. Below this is the 'Payload positions' section, which includes a 'Target' field set to 'http://localhost' and a checkbox 'Update Host header to match target' which is checked. The main area displays a list of 15 payload positions, each with a line number and a description. The 15th position is highlighted in blue and contains the text: `token=`
`dbdf7ef9fb82a97e8f0a406.dqJ0xB_pwhq1Meaa3zMHMyRLOFTEOVAawHzjfgkF4iQ.HME9gnzcmGjFQLb3hVsxeEFyqBWBp`
`wV7mi-5CVx2mGZEwT-UdIb1bHxYtw&username=sami_nayeem&password=1234`. To the right of the list are buttons for 'Add 5', 'Clear 5', 'Auto 5', and 'Refresh'. At the bottom, there is a search bar with the text 'Search' and a magnifying glass icon, and a 'Clear' button. The status bar at the bottom shows '0 payload positions' and 'Length: 761'.

Choose an attack type Start attack

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost ☒ Update Host header to match target

1 POST /orangehrm-5.5/web/index.php/auth/validate HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 168
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/orangehrm-5.5/web/index.php/auth/login
12 Cookie: _orangehrm=kqqpg6ttpgce1sn1am3gphkid3
13 Upgrade-Insecure-Requests: 1
14
15 token=
dbdf7ef9fb82a97e8f0a406.dqJ0xB_pwhq1Meaa3zMHMyRLOFTEOVAawHzjfgkF4iQ.HME9gnzcmGjFQLb3hVsxeEFyqBWBp
wV7mi-5CVx2mGZEwT-UdIb1bHxYtw&username=sami_nayeem&password=1234

0 payload positions Length: 761

Step 08. Move to payloads and paste some commonly used passwords and then click on the button named 'start attack'

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payloads' sub-tab is active, displaying the 'Payload sets' configuration. A 'Start attack' button is visible in the top right. Below, the 'Payload settings [Simple list]' section shows a list of payloads including 'root', '!@', 'wubao', 'password', '123456', and 'admin'. The 'Payload processing' section is empty, and the 'Payload encoding' section has a checkbox for 'URL-encode these characters' which is checked.

Payload sets Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 101
Payload type: Simple list Request count: 101

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste PublishThisListPlease
Load ... root
Remove !@
Clear wubao
Deduplicate password
123456
admin
Add Enter a new item
Add from list ... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule
Edit
Remove
Up
Down

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: \<>?+&*,;"'{}|^`#

Step 09. After completing the attack check for the behavior (status code and length) of every password. If you see any unusual behavior that might be the correct password. Then try to login using the password.

Burp Suite Session Hijacking

Step 01. Turn on the intercept

Step 02. Login to the system using the correct credentials

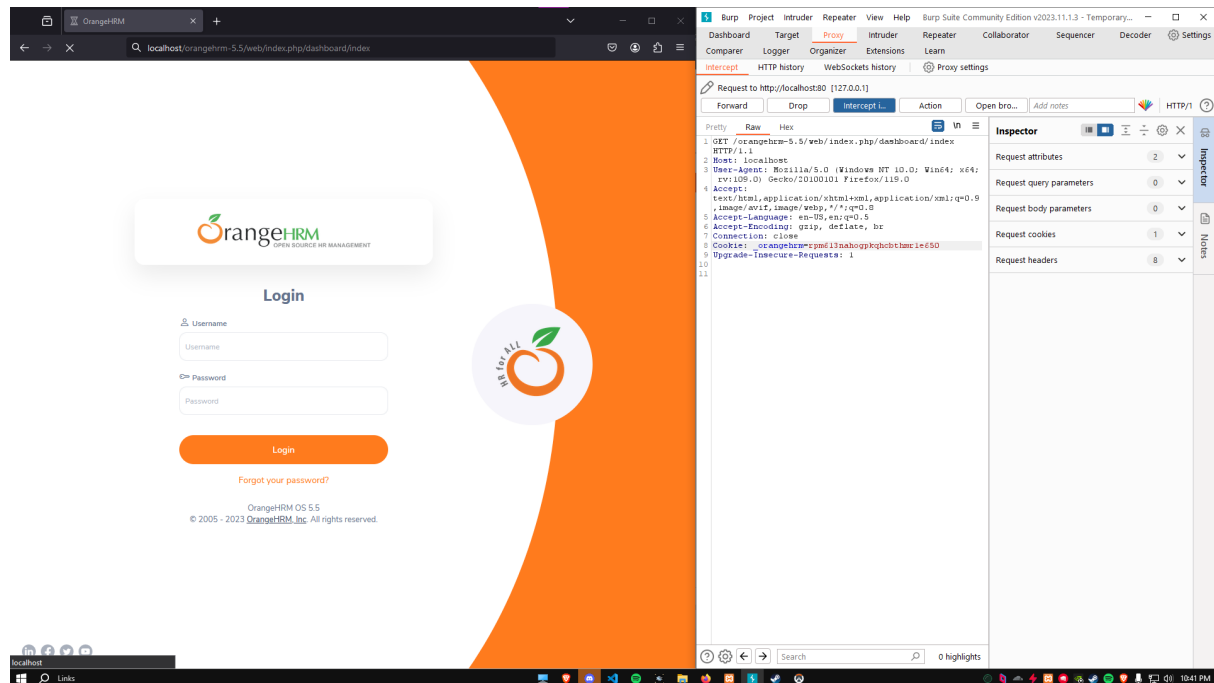
Step 03. Forward the requests in Burp Suite until the webpage is completely loaded.

Step 04. Collect the user cookie from Burp Suite

The screenshot displays the Burp Suite interface with a web browser window on the left and the Burp Suite application on the right. The browser window shows the OrangeHRM login page at `localhost/orangehrm-5.5/web/index.php/auth/login`. The page includes a login form with fields for Username (filled with `sami.nayem`) and Password (masked with dots), a Login button, and a link for "Forgot your password?". The footer of the page indicates "OrangeHRM OS 5.5" and "© 2005 - 2023 OrangeHRM, Inc. All rights reserved."

The Burp Suite application on the right shows the "Intercept" tab selected. The "Request to http://localhost80 [127.0.0.1]" is displayed. The "Raw" tab is active, showing the raw HTTP request. The request is a POST to `/orangehrm-5.5/web/index.php/auth/validate`. The request body is a JSON object containing user credentials and a session token. The "Inspector" tab on the right shows the "Selected text" field with the value `b71mb08ajcb2g2kaakp21pbj0mc`. The "Decoded from" dropdown is set to "URL encoding". The "Request attributes" section shows the "Cookie" attribute with the value `_orangehrm=b71mb08ajcb2g2kaakp21pbj0mc`. The "Request query parameters" section shows the "token" parameter with the value `token=b71mb08ajcb2g2kaakp21pbj0mc`. The "Request body parameters" section shows the "username" and "password" parameters with values `username=sami.nayem` and `password=sami14001602441585`.

Step 05. Logout from the system and then try to login using the collected user cookie.



Step 06. If the website is secured it will automatically redirect you to the login page, else you can login to the system.