Burp Suite Setup and configuration

Pre-condition:

1. Burp Suite should be installed.

Steps to install Burp Suite:

1. Visit the Official Website using any browser.
2. Click on Burp Suite Community Edition. (https://portswigger.net/burp/communitydownload)
3. Choose the Linux system and click the download CTA button.
4. Locate the Burp suite script file and open the terminal and install.

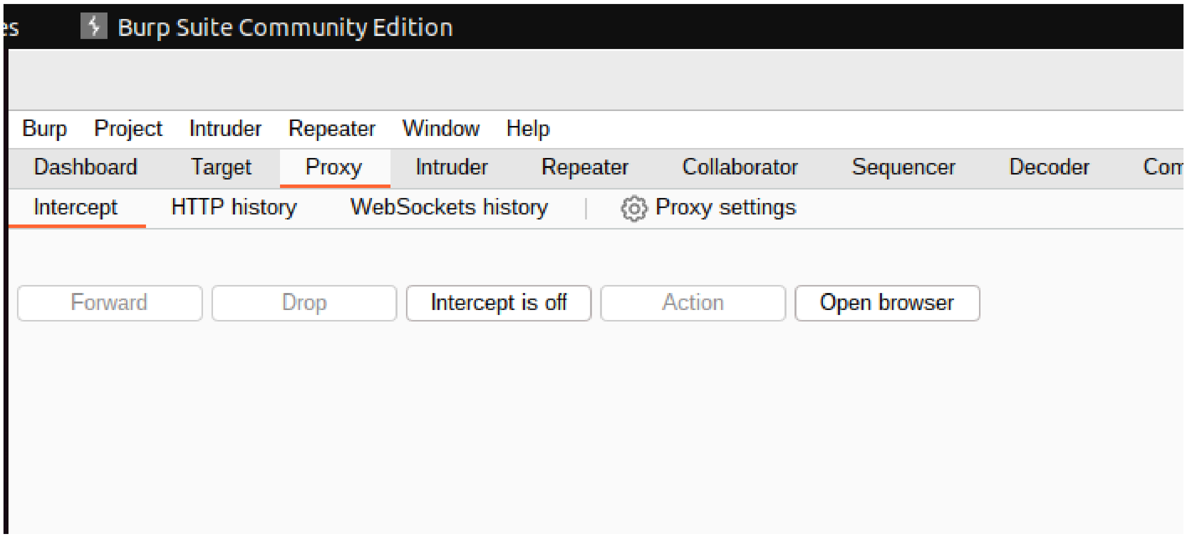
   Commands to run in terminal to install:

   - (*chmod +x burp suite file name*).
   - (*./burp-suite-file-name*) or (*sh burp-suite-file-name*).
5. Click the start Burp and now your project is loading.

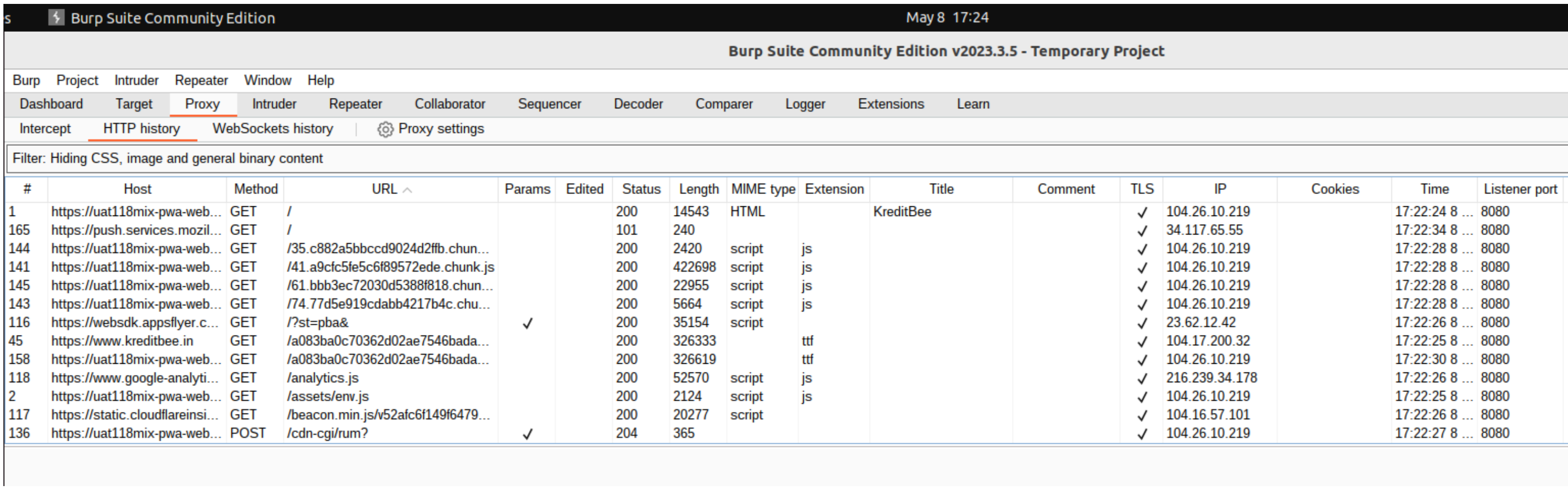
Method-1

Steps:

1. Launch Burp Suite.
2. Click on create and continue with Start Burp.
3. Click on proxy.



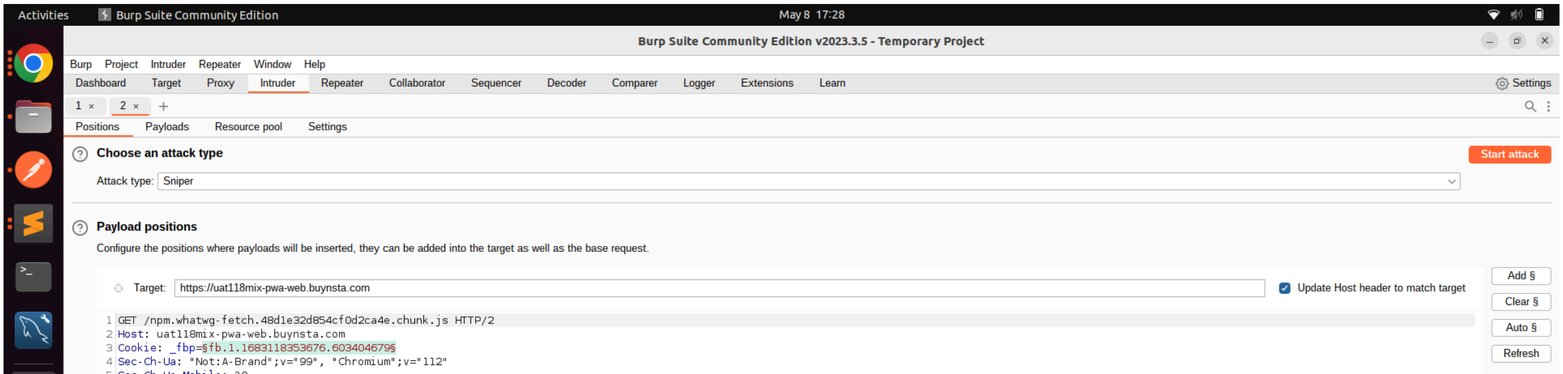
4. Click on the open browser and enter the url of the particular environment. (Eg:https://uat118mix-pwa-web.buynsta.com).
5. Login with valid credentials and continue till the requirement of the task.
6. Recorded HTTP requests will be in HTTP history.



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	https://uat118mix-pwa-web...	GET	/			200	14543	HTML		KreditBee		✓	104.26.10.219		17:22:24 8 ...	8080
165	https://push.services.mozil...	GET	/			101	240					✓	34.117.65.55		17:22:34 8 ...	8080
144	https://uat118mix-pwa-web...	GET	/35.c882a5bbccd9024d2ffb.chun...			200	2420	script	js			✓	104.26.10.219		17:22:28 8 ...	8080
141	https://uat118mix-pwa-web...	GET	/41.a9cfc5fe5c6f89572ede.chunk.js			200	422698	script	js			✓	104.26.10.219		17:22:28 8 ...	8080
145	https://uat118mix-pwa-web...	GET	/61.bbb3ec72030d5388f818.chun...			200	22955	script	js			✓	104.26.10.219		17:22:28 8 ...	8080
143	https://uat118mix-pwa-web...	GET	/74.77d5e919cdabb4217b4c.chu...			200	5664	script	js			✓	104.26.10.219		17:22:28 8 ...	8080
116	https://websdk.appsflyer.c...	GET	/?st=pba&	✓		200	35154	script				✓	23.62.12.42		17:22:26 8 ...	8080
45	https://www.kreditbee.in	GET	/a083ba0c70362d02ae7546bada...			200	326333		ttf			✓	104.17.200.32		17:22:25 8 ...	8080
158	https://uat118mix-pwa-web...	GET	/a083ba0c70362d02ae7546bada...			200	326619		ttf			✓	104.26.10.219		17:22:30 8 ...	8080
118	https://www.google-analyti...	GET	/analytics.js			200	52570	script	js			✓	216.239.34.178		17:22:26 8 ...	8080
2	https://uat118mix-pwa-web...	GET	/assets/env.js			200	2124	script	js			✓	104.26.10.219		17:22:25 8 ...	8080
117	https://static.cloudflareinsi...	GET	/beacon.min.js/v52afc6f149f6479...			200	20277	script				✓	104.16.57.101		17:22:26 8 ...	8080
136	https://uat118mix-pwa-web...	POST	/cdn-cgi/rum?	✓		204	365					✓	104.26.10.219		17:22:27 8 ...	8080

7. Click on the particular endpoint and of your task and right click and select send to intruder (Ctrl + I).
8. Now in the intruder page we can alter payloads with SQL injection commands and click on Start attack CTA button.



Choose an attack type

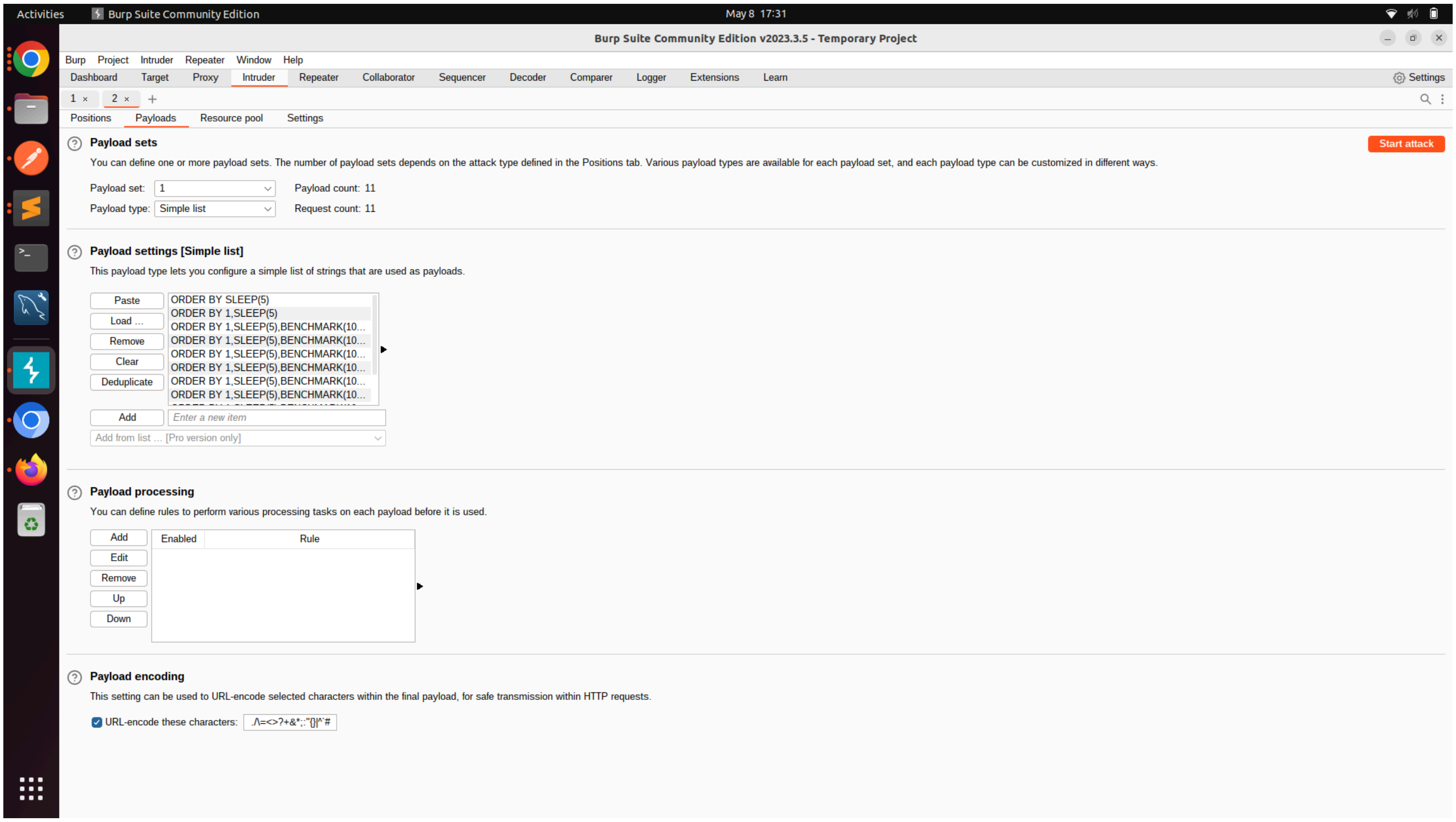
Attack type: Sniper

Payload positions

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

Target: https://uat118mix-pwa-web.buynsta.com ☑ Update Host header to match target

```
GET /npm.whatwg-fetch.48d1e32d854cf0d2ca4e.chunk.js HTTP/2
Host: uat118mix-pwa-web.buynsta.com
Cookie: _fbp=§fb.1.1683118353676.603404679§
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
```



Burp Suite Community Edition v2023.3.5 - Temporary Project

Intruder › Payloads

Payload sets

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: 11

Payload type: Simple list — Request count: 11

Payload settings [Simple list]

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

```
ORDER BY SLEEP(5)
ORDER BY 1,SLEEP(5)
ORDER BY 1,SLEEP(5),BENCHMARK(10...
ORDER BY 1,SLEEP(5),BENCHMARK(10...
ORDER BY 1,SLEEP(5),BENCHMARK(10...
ORDER BY 1,SLEEP(5),BENCHMARK(10...
ORDER BY 1,SLEEP(5),BENCHMARK(10...
ORDER BY 1,SLEEP(5),BENCHMARK(10...
```

Payload processing

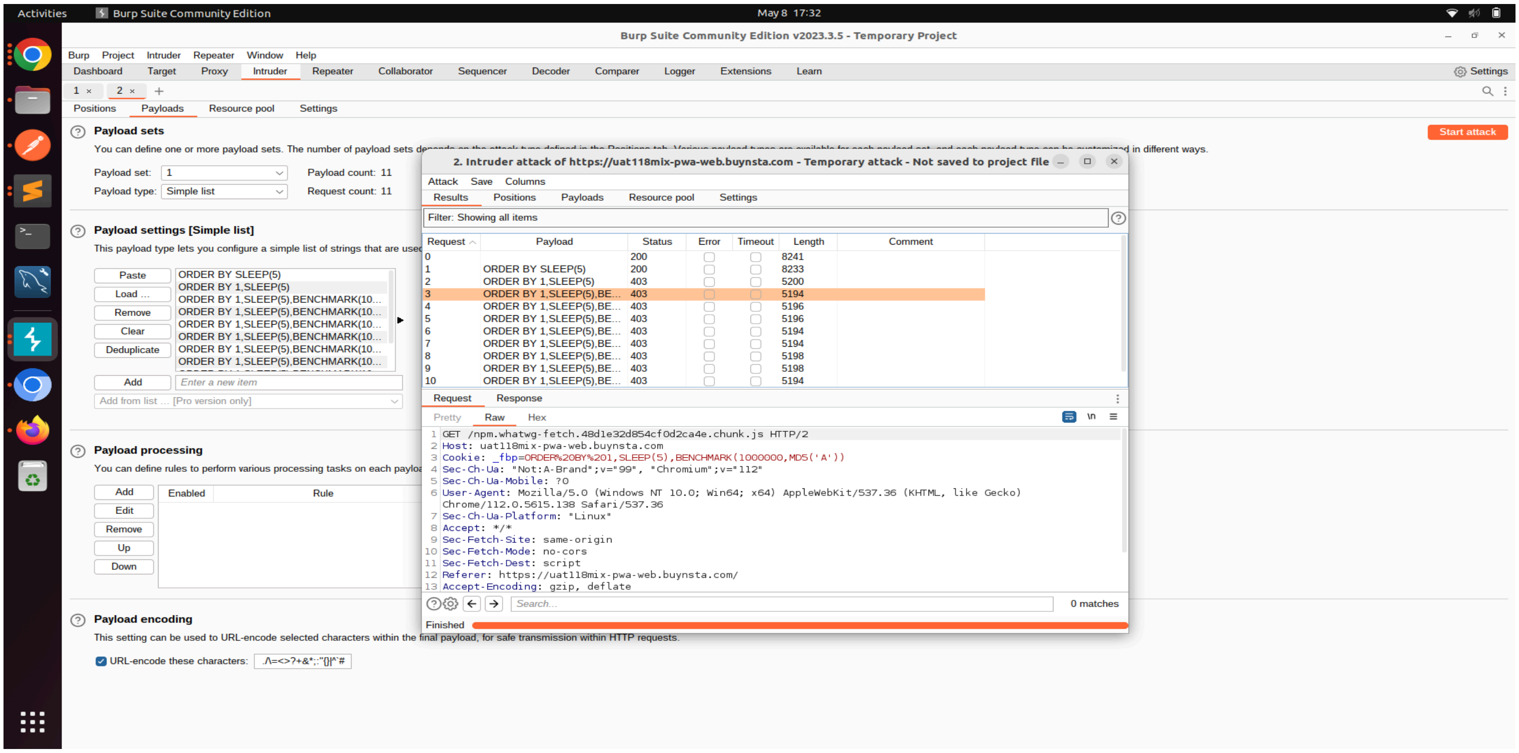
You can define rules to perform various processing tasks on each payload before it is used.

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: `./\=<>?+&*;:"{}|^`#`

9. Validate the results.



2. Intruder attack of https://uat118mix-pwa-web.buynsta.com - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	8241	
1	ORDER BY SLEEP(5)	200	☐	☐	8233	
2	ORDER BY 1,SLEEP(5)	403	☐	☐	5200	
3	ORDER BY 1,SLEEP(5),BE...	403	☐	☐	5194	
4	ORDER BY 1,SLEEP(5),BE...	403	☐	☐	5196	
5	ORDER BY 1,SLEEP(5),BE...	403	☐	☐	5196	
6	ORDER BY 1,SLEEP(5),BE...	403	☐	☐	5194	
7	ORDER BY 1,SLEEP(5),BE...	403	☐	☐	5194	
8	ORDER BY 1,SLEEP(5),BE...	403	☐	☐	5198	
9	ORDER BY 1,SLEEP(5),BE...	403	☐	☐	5198	
10	ORDER BY 1,SLEEP(5),BE...	403	☐	☐	5194	

Request — Raw

```
GET /npm.whatwg-fetch.48d1e32d854cf0d2ca4e.chunk.js HTTP/2
Host: uat118mix-pwa-web.buynsta.com
Cookie: _fbp=ORDER%20BY%201,SLEEP(5),BENCHMARK(1000000,MD5('A'))
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.138 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://uat118mix-pwa-web.buynsta.com/
Accept-Encoding: gzip, deflate
```

0 matches

Finished

SQL injection List: https://docs.google.com/spreadsheets/d/1qwUP1b3QMkaH5baQb2Ia8jcTHKUYPXkzgskgVa1Cif0/edit#gid=0

Method-2

Integrating BurpSuite with Postman:

1. Open a particular endpoint of the task in a web application.

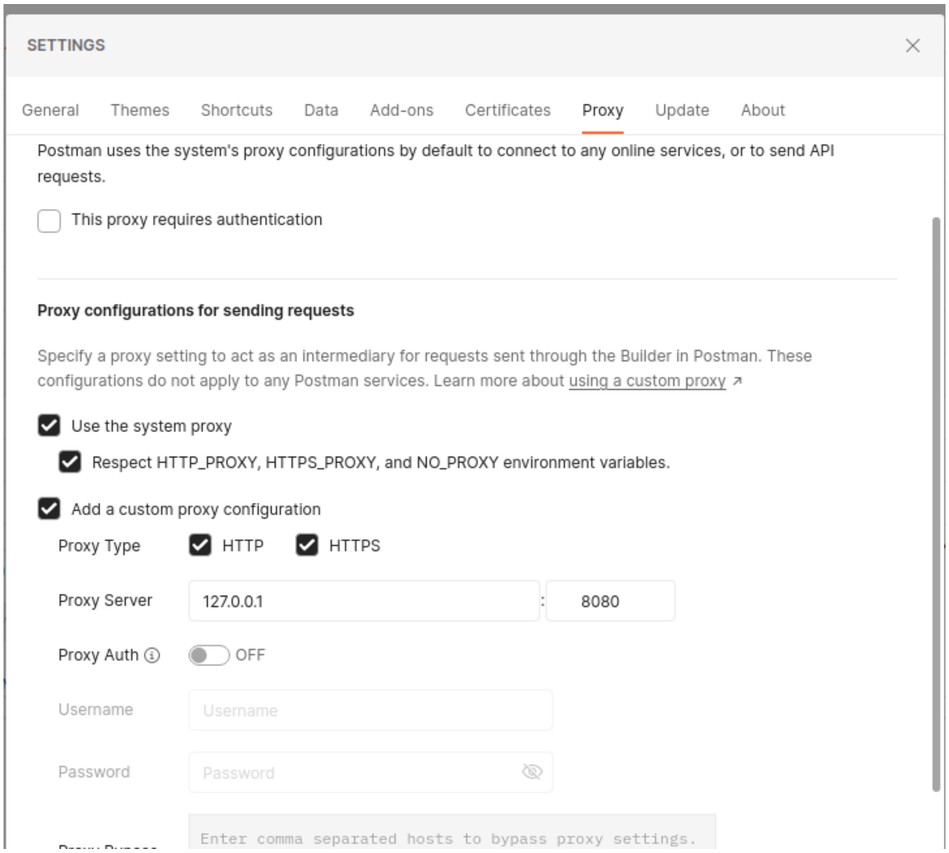
2.Enable Inspect mode and select network grid.

3.Take the CURL from the particular endpoint triggered in networks.

4.Import the copied CURL to Postman.

5.In Postman, click on settings.

6.Select proxy and click on Add a custom proxy configuration,
Proxy Server: **127.0.0.1**, Port : **8080.**



Postman uses the system's proxy configurations by default to connect to any online services, or to send API requests.

☐ This proxy requires authentication

Proxy configurations for sending requests

Specify a proxy setting to act as an intermediary for requests sent through the Builder in Postman. These configurations do not apply to any Postman services. Learn more about using a custom proxy ↗

☑ Use the system proxy

☑ Respect HTTP_PROXY, HTTPS_PROXY, and NO_PROXY environment variables.

☑ Add a custom proxy configuration

Proxy Type ☑ HTTP ☑ HTTPS

Proxy Server 127.0.0.1 : 8080

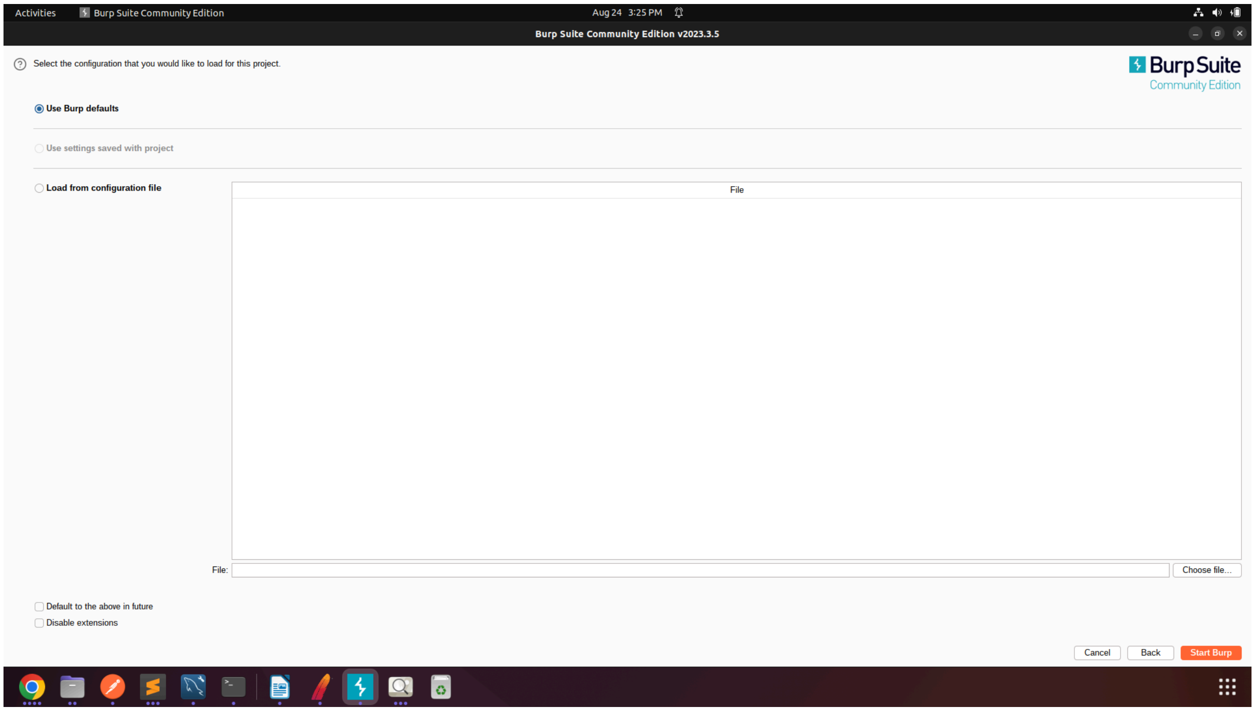
Proxy Auth ⓘ OFF

Username Username

Password Password

Proxy Bypass Enter comma separated hosts to bypass proxy settings.

7.Launch Burpsuite Application and click on start burp CTA button.



Burp Suite Community Edition v2023.3.5

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use settings saved with project

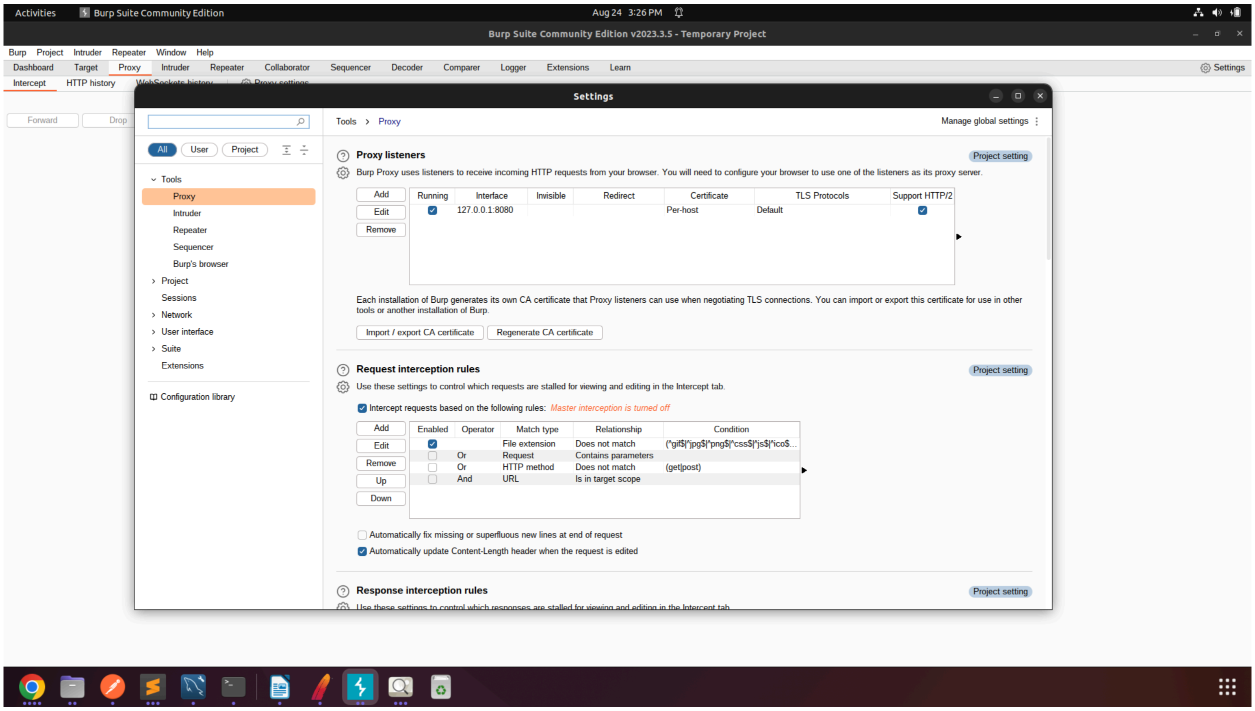
○ Load from configuration file

File:

□ Default to the above in future

□ Disable extensions

8.Click on proxy and proxy settings



Burp Suite Community Edition v2023.3.5 - Temporary Project

Settings

Tools › Proxy

Proxy listeners — Project setting

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

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support HTTP/2
☑	127.0.0.1:8080			Per-host	Default	☑

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

Request interception rules — Project setting

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

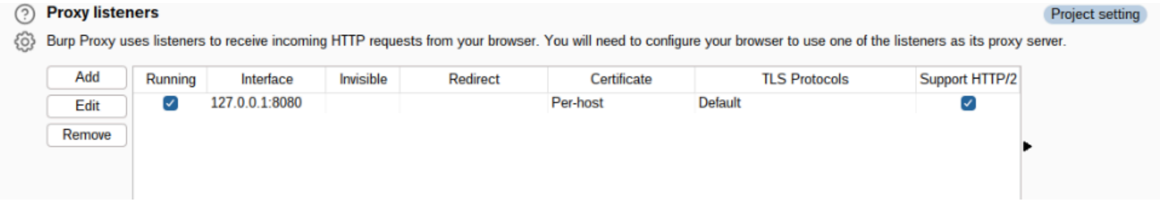
☑ Automatically update Content-Length header when the request is edited

Response interception rules — Project setting

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

Activities
Burp Suite Community Edition
Aug 24 3:26 PM
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop
All User Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
Sessions
Network
User interface
Suite
Extensions
Configuration library
Manage global settings
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate
Up
Down

9. Proxy should be mapped as same as like postman's proxy



Proxy listeners

Project setting

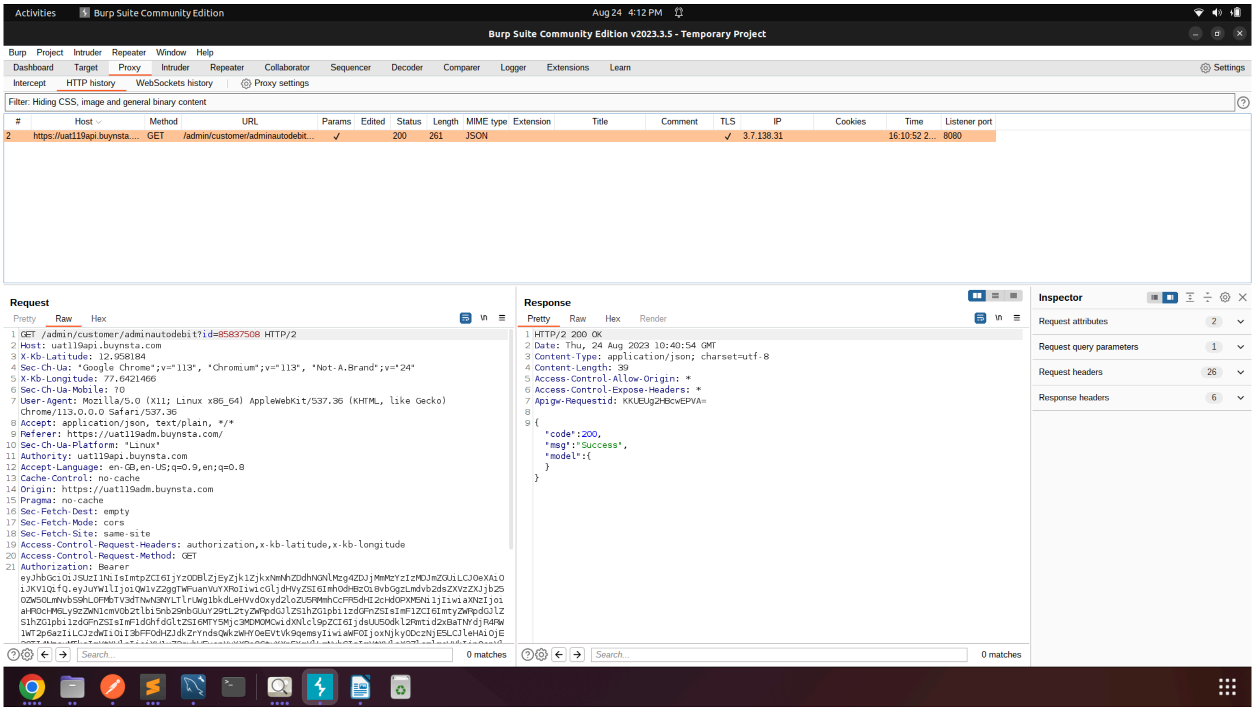
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Add · Edit · Remove

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support HTTP/2
☑	127.0.0.1:8080			Per-host	Default	☑

10. Launch the postman and trigger the request.

11. The triggered request will be recorded in HTTP History grid



Activities
Burp Suite Community Edition
Aug 24 4:12 PM
Burp Suite Community Edition v2023.3.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history
Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
2	https://uat119api.buynsta....	GET	/admin/customer/adminautodebit...	✓		200	261	JSON				✓	3.7.138.31		16:10:52 2...	8080

Request

```
GET /admin/customer/adminautodebit?id=85837508 HTTP/2
Host: uat119api.buynsta.com
X-Kb-Latitude: 12.958184
Sec-Ch-Ua: "Google Chrome";v="113", "Chromium";v="113", "Not-A.Brand";v="24"
X-Kb-Longitude: 77.6421466
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/113.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Referer: https://uat119adm.buynsta.com/
Sec-Ch-Ua-Platform: "Linux"
Authority: uat119api.buynsta.com
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cache-Control: no-cache
Origin: https://uat119adm.buynsta.com
Pragma: no-cache
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Access-Control-Request-Headers: authorization,x-kb-latitude,x-kb-longitude
Access-Control-Request-Method: GET
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6IjYzODBlZjEyZjk1ZjkxNmNhZDdhNGNlMzg4ZDJjMmMzYzIzMDJmZGUiLCJ0eXAiO
iJKV1QifQ.eyJuYW1lIjoiQW1vZ2ggTWFuanVuYXRoIiwicGljdHVyZSI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb25
0ZW50LmNvbS9hL0FMbTV3dTNwN3NYLTlrUWg1bkdLeHVvd0xyd2loZU5RMmhCcFR5dHI2cHd0PXM5Ni1jIiwiaXNzIjoi
aHR0cHM6Ly9zZWN1cmV0b2tlbi5nb29nbGUuY29tL2tyZWRpdGJlZS1hZG1pbi1zdGFnZSIsImF1ZCI6ImtyZWRpdGJlZ
S1hZG1pbi1zdGFnZSIsImF1dGhfdGltZSI6MTY5Mjc3MDM0MCwidXNlcl9pZCI6IjdsUU50dkl2RmtId2xBaTNYdjR4RW
1WT2p6azIiLCJzdWIiOiI3bFF0dHZJdkZrYndsQWkzWHY0eEVtVk9qemsyIiwiaWF0IjoxNjkyODczNjE5LCJleHAiOjE
```

Search... 0 matches

Response

```
HTTP/2 200 OK
Date: Thu, 24 Aug 2023 10:40:54 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 39
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: *
Apigw-Requestid: KKUEUg2HBcwEPVA=

{
  "code":200,
  "msg":"Success",
  "model":{
  }
}
```

Search... 0 matches

Inspector

Request attributes	2
Request query parameters	1
Request headers	26
Response headers	6

12. Send the particular request to Repeater *(Ctrl + r)*.

13.Modify key value parameters and test.