CYBER SECURITY LAB 24

1.Web Application Penetration Testing of HTTP Methods, HTTP Requests & Response using BurpSuite

HTTP Methods :-

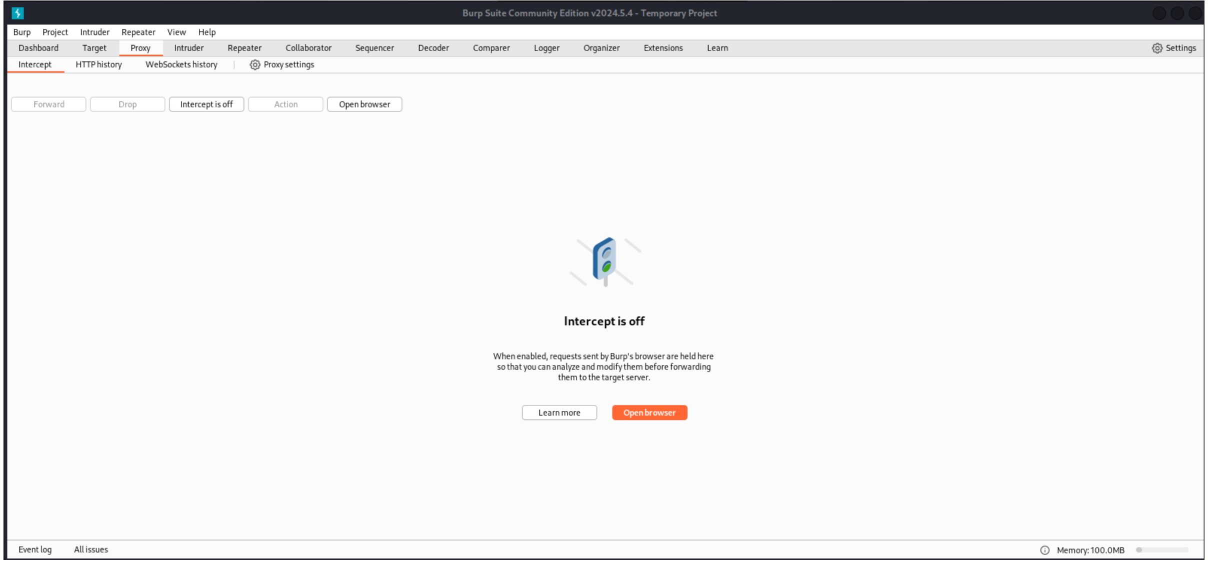
HTTP methods, also known as HTTP request methods, are actions that indicate the desired action to be performed on a resource identified by a URL. Each HTTP method has a specific purpose and semantic meaning.

This extension makes a OPTIONS request and determines if other HTTP methods than the original request are available. If there are other methods available, the request under Proxy/Http History

Here are the common HTTP methods:

- GET
- POST
- PUT
- TRACE
- DELETE
- PATCH
- HEAD

Step 1:Open the Burp suite, Go to proxy features.

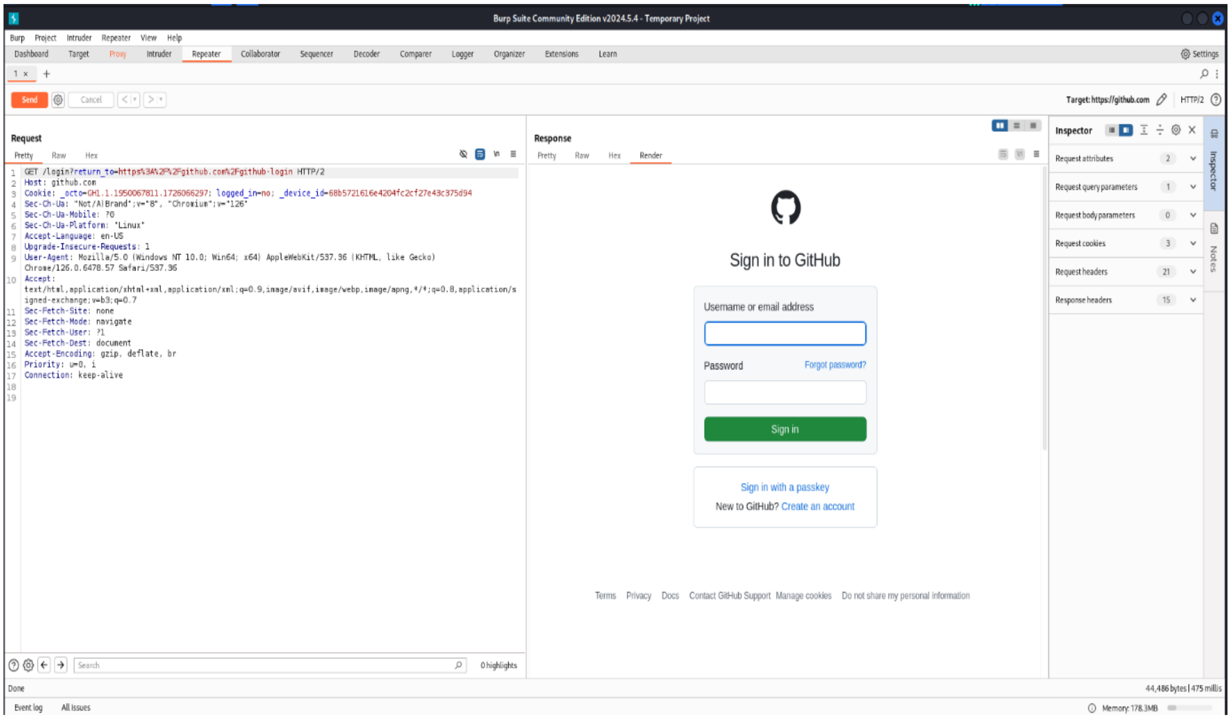


Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Step 2: Check for intercepted requests.

If you're seeing intercepted requests in the Proxy > Intercept tab, turn on interception.Send request to get response of current http method.


Burp Suite Community Edition v2024.5.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: https://github.com
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 3
Request headers 21
Response headers 15
Search
0 highlights
Done
44,486 bytes | 475 millis
Event log All issues
Memory: 178.3MB

```
GET /login?return_to=https%3A%2F%2Fgithub.com%2Fgithub-login HTTP/2
Host: github.com
Cookie: _octo=GH1.1.1950067811.1726066297; logged_in=no; _device_id=68b5721616e4204fc2cf27e43c375d94
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Sign in to GitHub

Username or email address

Password Forgot password?

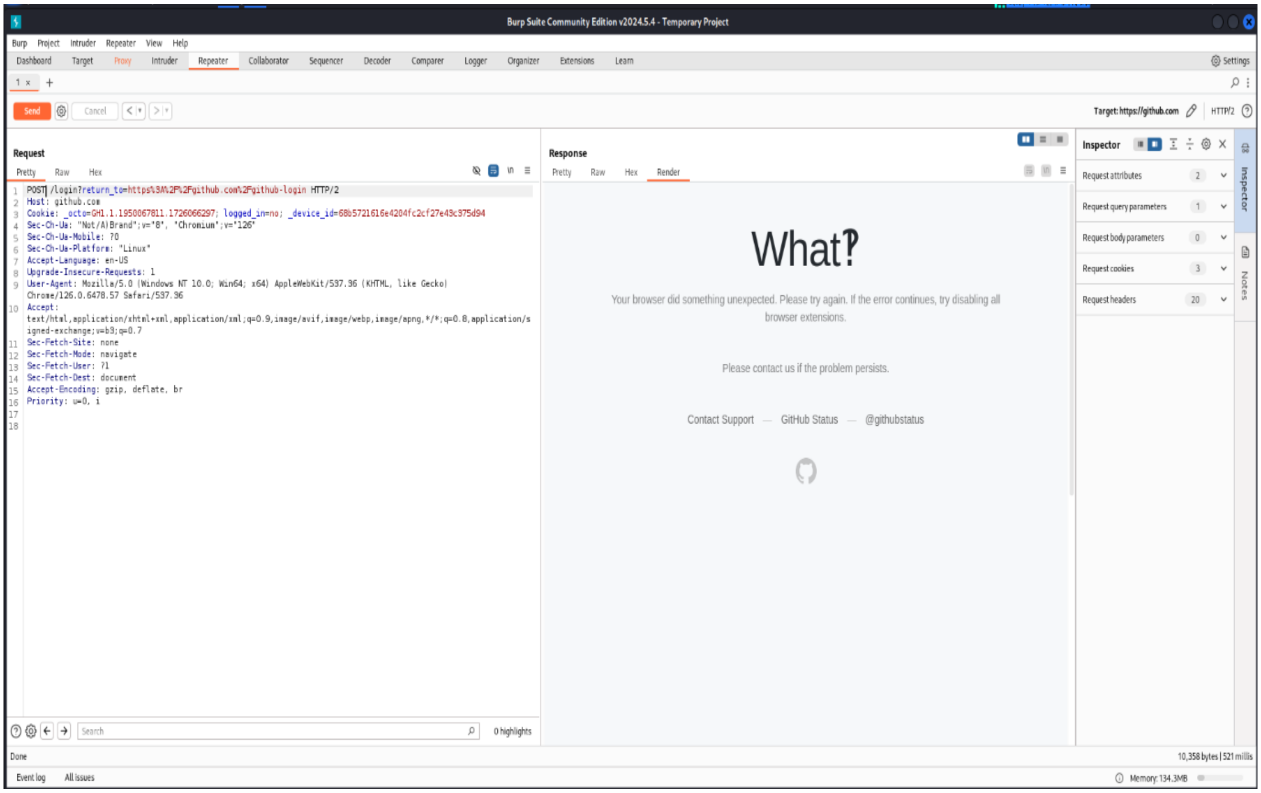
Sign in

Sign in with a passkey

New to GitHub? Create an account

Terms Privacy Docs Contact GitHub Support Manage cookies Do not share my personal information

Step 3: Change HTTP Method to check penetration testing of web application.


Burp Suite Community Edition v2024.5.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: https://github.com
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 3
Request headers 20
Search
0 highlights
Done
10,358 bytes | 521 millis
Event log All issues
Memory: 134.3MB

```
POST /login?return_to=https%3A%2F%2Fgithub.com%2Fgithub-login HTTP/2
Host: github.com
Cookie: _octo=GH1.1.1950067811.1726066297; logged_in=no; _device_id=68b5721616e4204fc2cf27e43c375d94
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

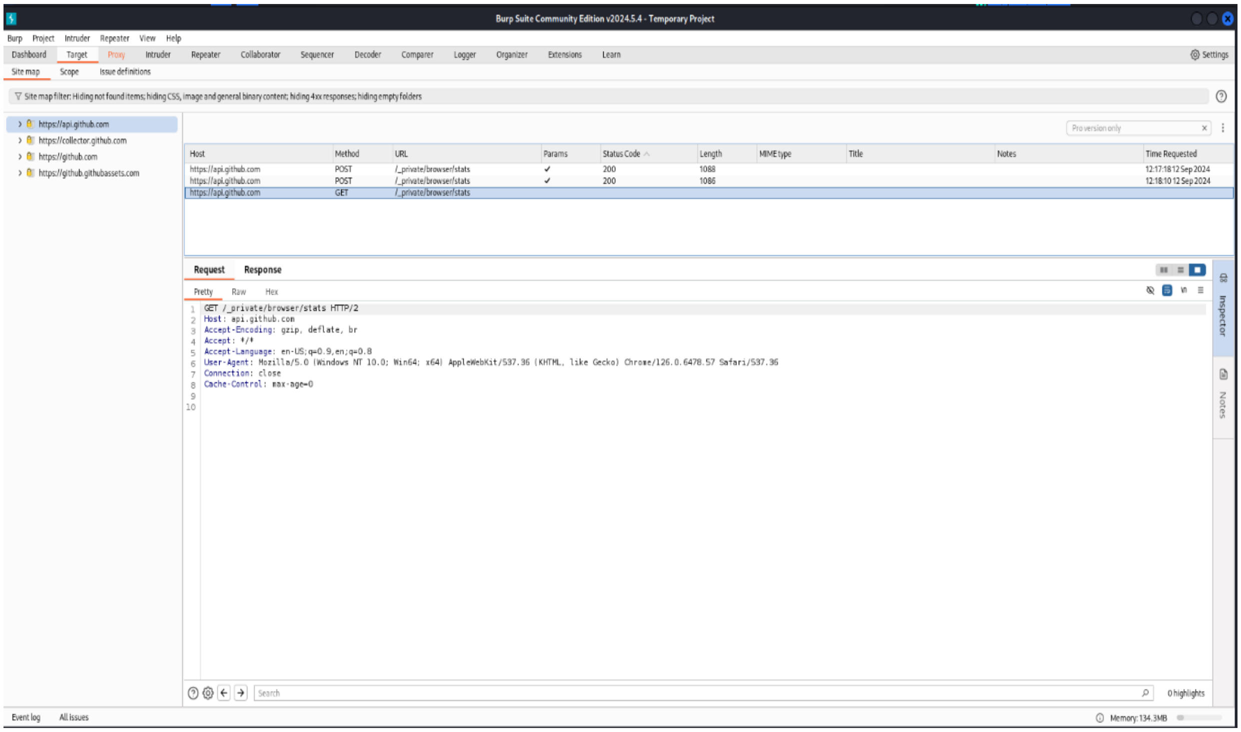
What?

Your browser did something unexpected. Please try again. If the error continues, try disabling all browser extensions.

Please contact us if the problem persists.

Contact Support — GitHub Status — @githubstatus

Step 4: Find target and set scope of URL or API to perform attacks.


Burp Suite Community Edition v2024.5.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Site map Scope Issue definitions
https://api.github.com
https://collector.github.com
https://github.com
https://github.githubassets.com
Pro version only
Request Response
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log All issues
Memory: 134.3MB

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status Code	Length	MIME type	Title	Notes	Time Requested
https://api.github.com	POST	/_private/browser/stats	✓	200	1088				12:17:18 12 Sep 2024
https://api.github.com	POST	/_private/browser/stats	✓	200	1086				12:18:10 12 Sep 2024
https://api.github.com	GET	/_private/browser/stats							

```
GET /_private/browser/stats HTTP/2
Host: api.github.com
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
Connection: close
Cache-Control: max-age=0


```