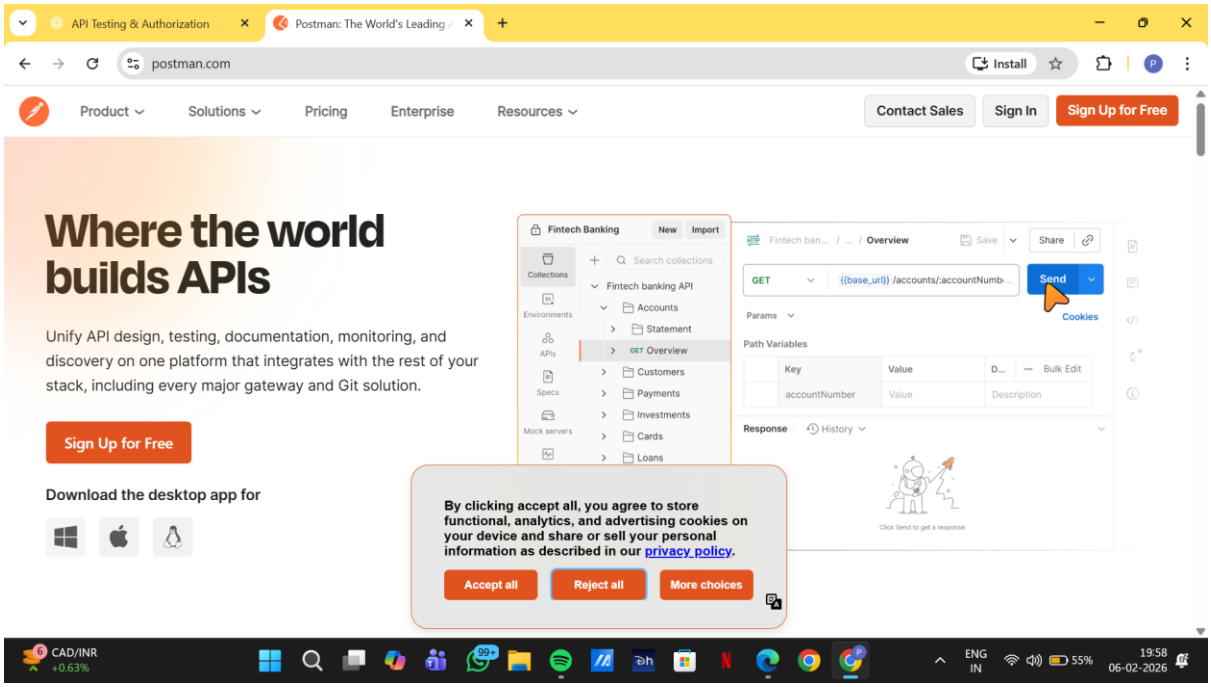
Task 13: Secure API Testing & Authorization Validation

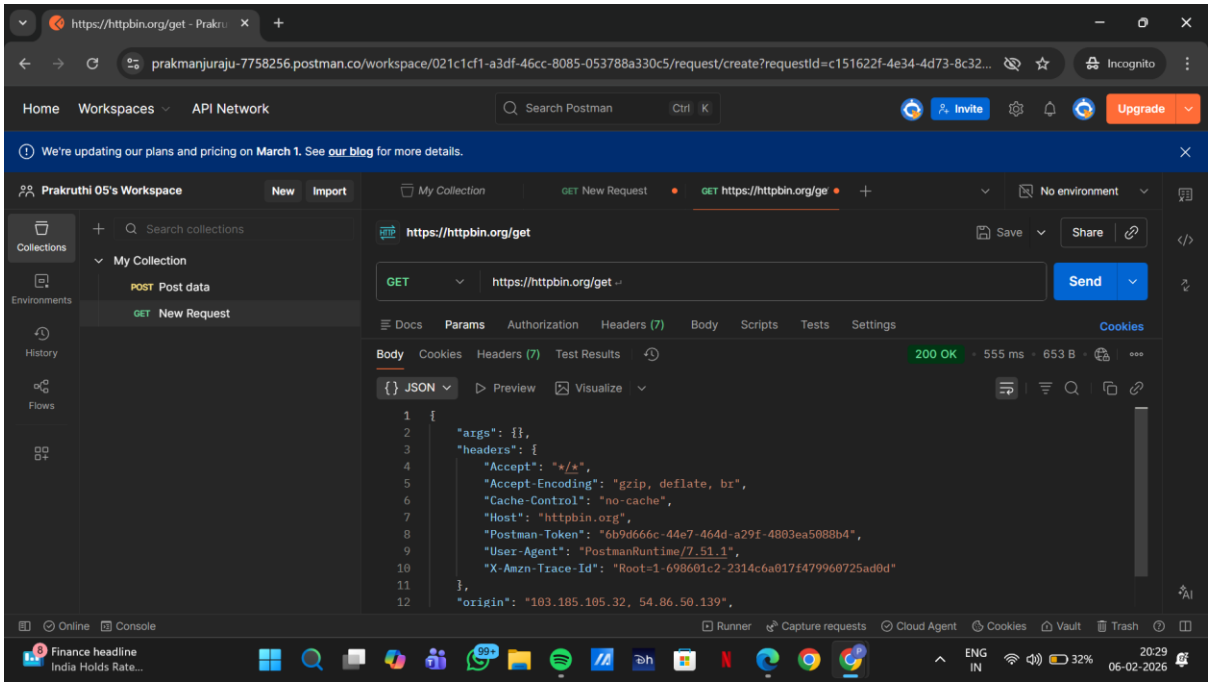
Tools: Primary: Postman

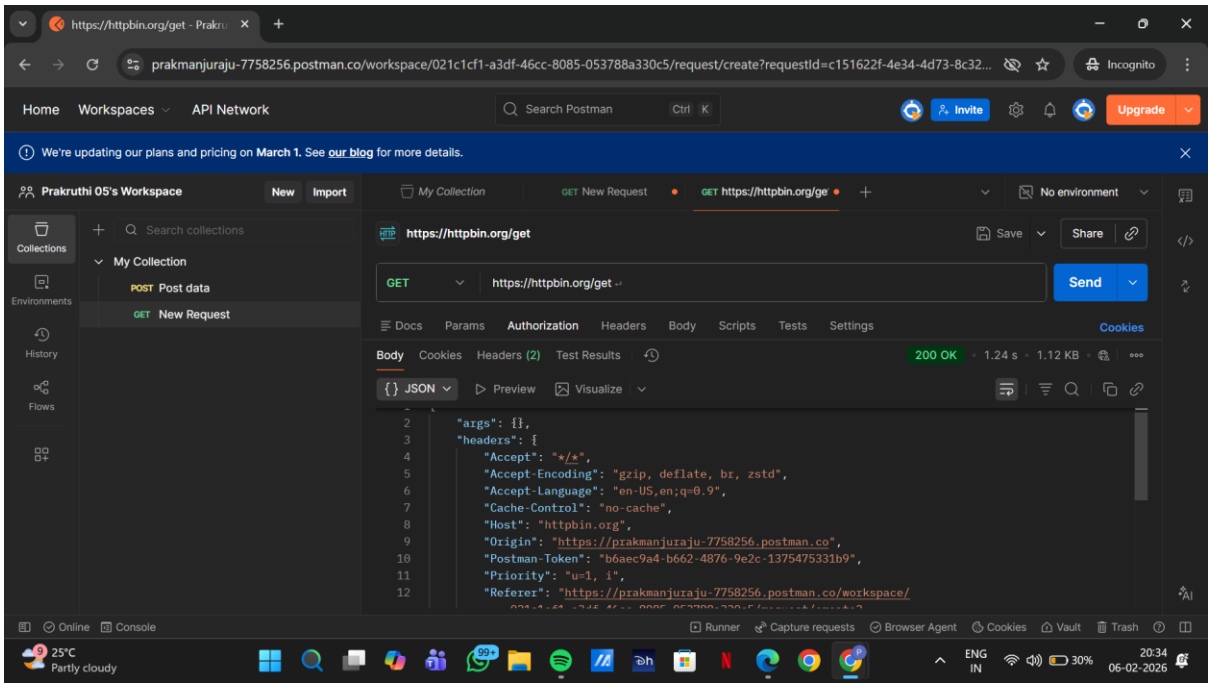
Alternatives: cURL, Insomnia

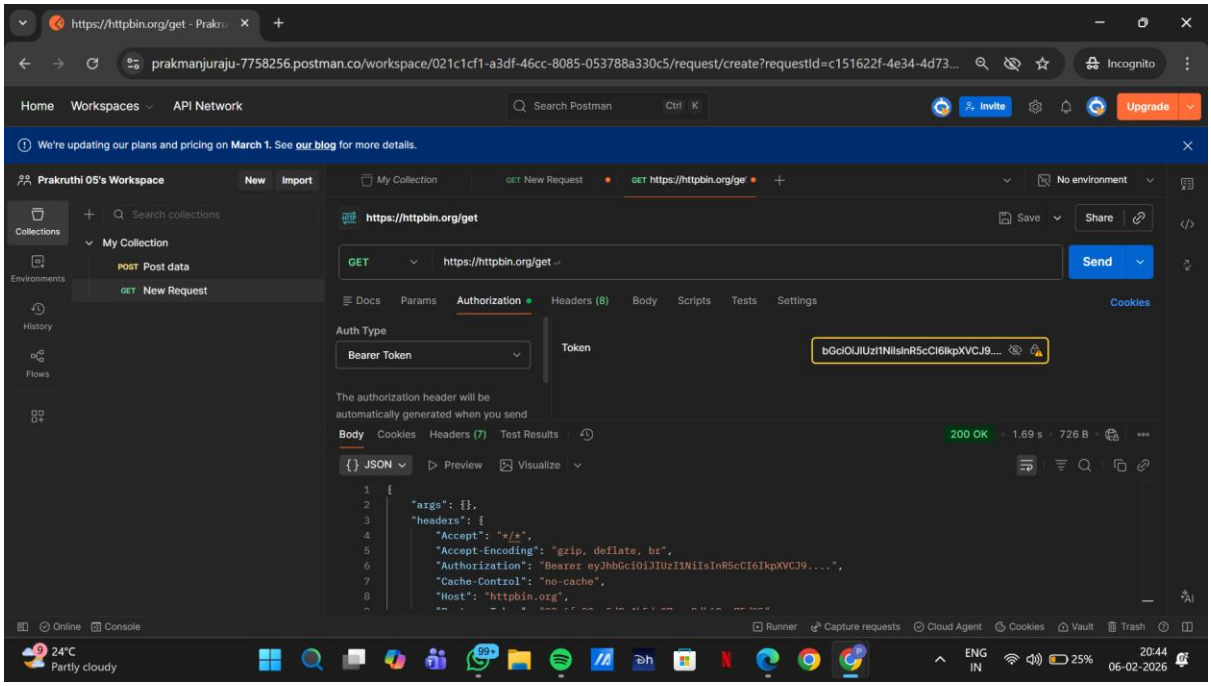
Hints / Mini Guide:

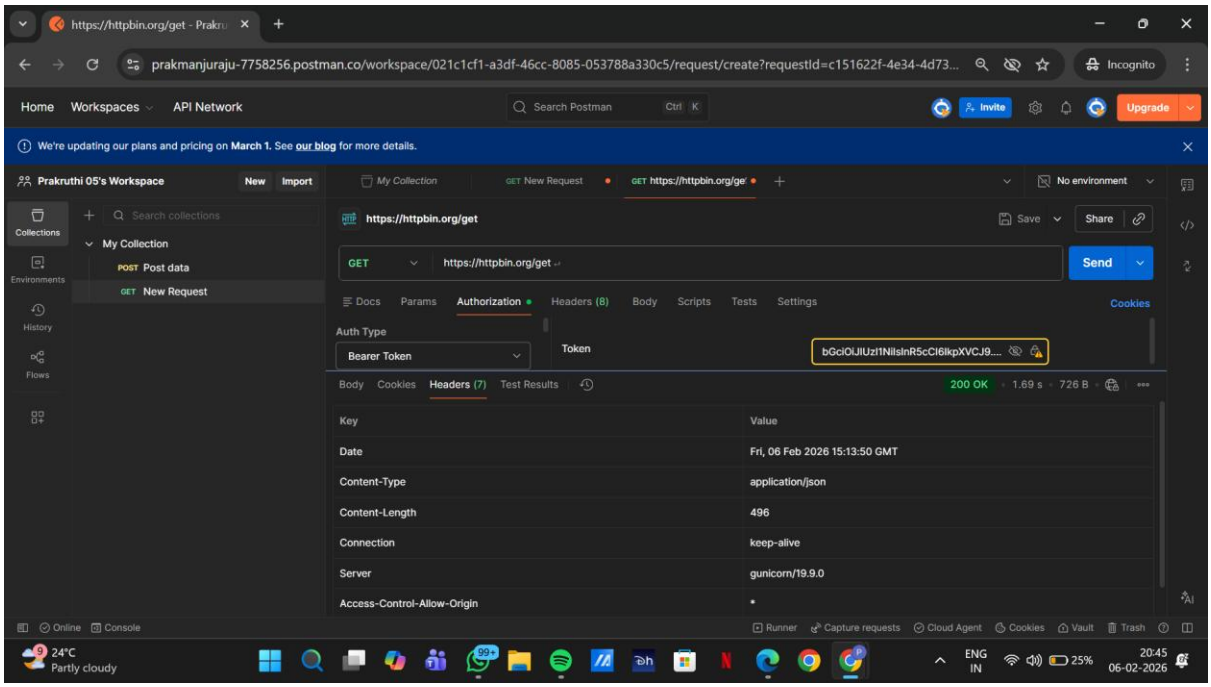
1.Understand how REST APIs work and how applications use HTTP methods such as GET, POST, PUT, and DELETE to communicate with backend servers.
2.Configure an API in Postman by setting the endpoint URL, headers, and request body based on the API documentation.
3.Test API authentication by sending requests with valid and invalid credentials to observe access behavior.
4.Remove authentication headers and resend requests to check if the API improperly allows unauthenticated access.
5.Modify resource identifiers in the request to test for broken authorization issues.
6.Send malformed or unexpected input values to observe input validation handling.
7.Perform multiple rapid requests to check whether rate limiting is enforced.
8.Review HTTP response codes and error messages for security weaknesses.

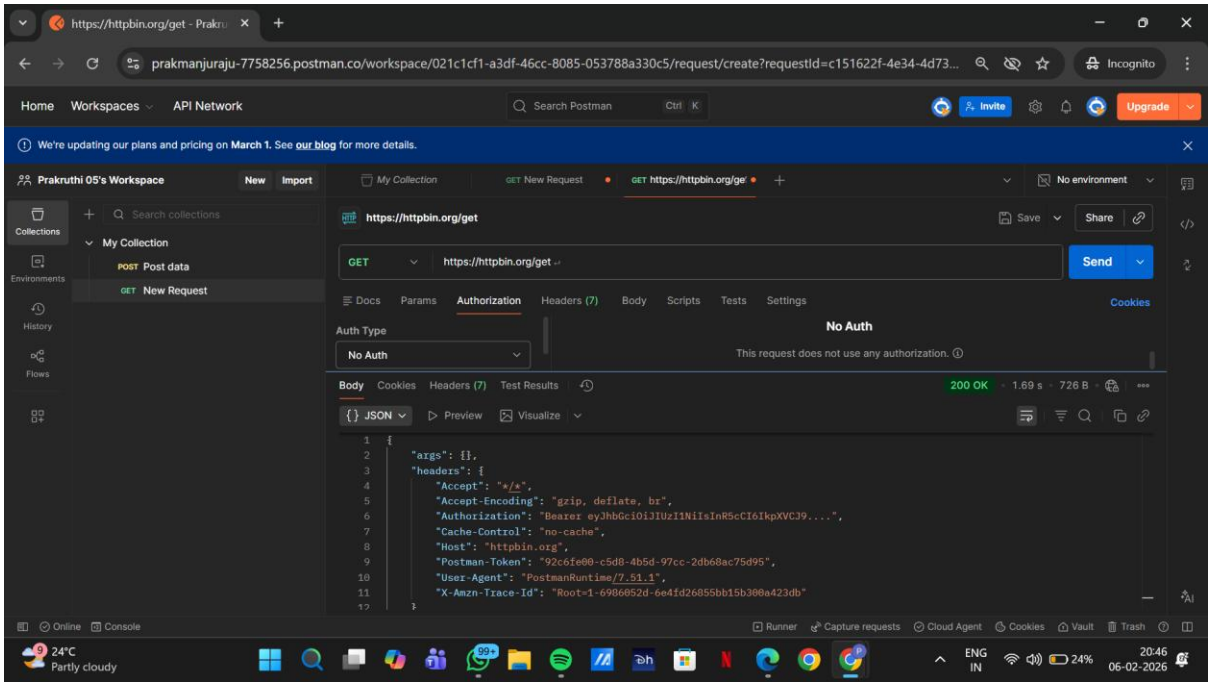


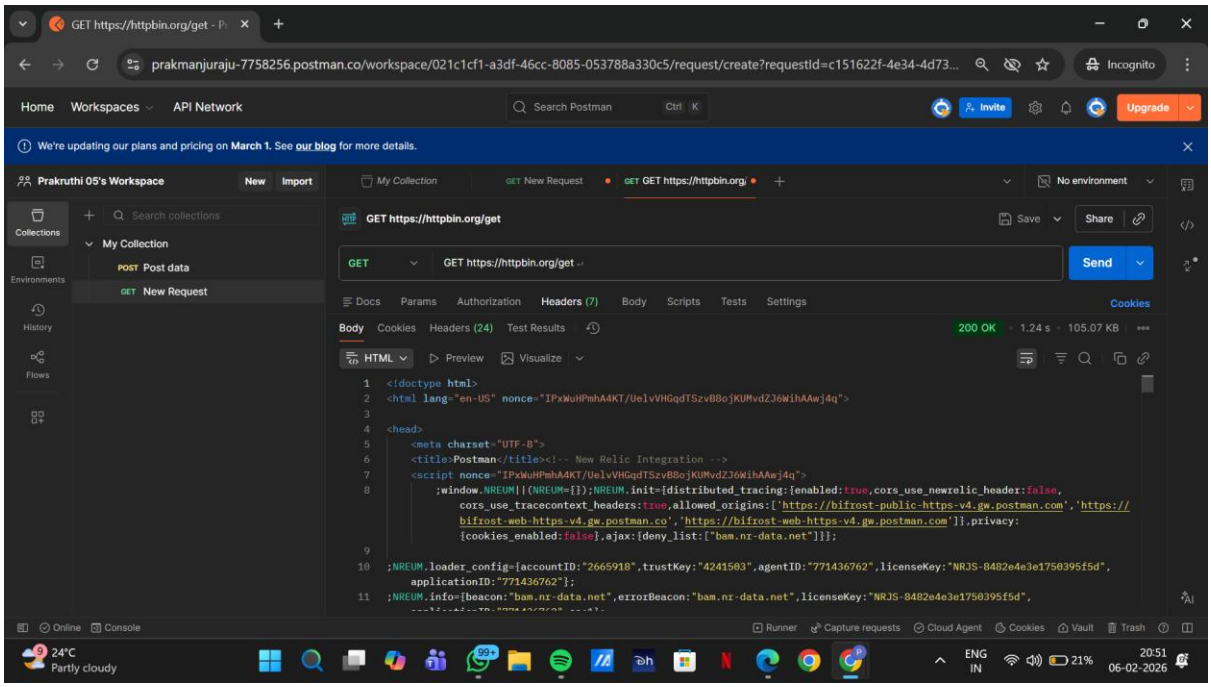

https://httpbin.org/get - Prakru
prakmanjuraju-7758256.postman.co/workspace/021c1cf1-a3df-46cc-8085-053788a330c5/request/create?requestId=c151622f-4e34-4d73-8c32...
Incognito
Home
Workspaces
API Network
Search Postman
Ctrl K
Invite
Upgrade
We're updating our plans and pricing on March 1. See our blog for more details.
Prakruthi 05's Workspace
New
Import
My Collection
GET New Request
GET https://httpbin.org/ge
No environment
Collections
Environments
History
Flows
Search collections
My Collection
POST Post data
GET New Request
https://httpbin.org/get
Save
Share
GET
https://httpbin.org/get
Send
Docs
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Body
Cookies
Headers (7)
Test Results
200 OK
555 ms
653 B
JSON
Preview
Visualize
{
"args": {},
"headers": {
"Accept": "*/*",
"Accept-Encoding": "gzip, deflate, br",
"Cache-Control": "no-cache",
"Host": "httpbin.org",
"Postman-Token": "6b9d666c-44e7-464d-a29f-4803ea5088b4",
"User-Agent": "PostmanRuntime/7.51.1",
"X-Amzn-Trace-Id": "Root=1-698601c2-2314c6a017f479960725ad0d"
},
"origin": "103.185.105.32, 54.86.50.139",
Online
Console
Runner
Capture requests
Cloud Agent
Cookies
Vault
Trash
Finance headline
India Holds Rate...
ENG
IN
32%
20:29
06-02-2026

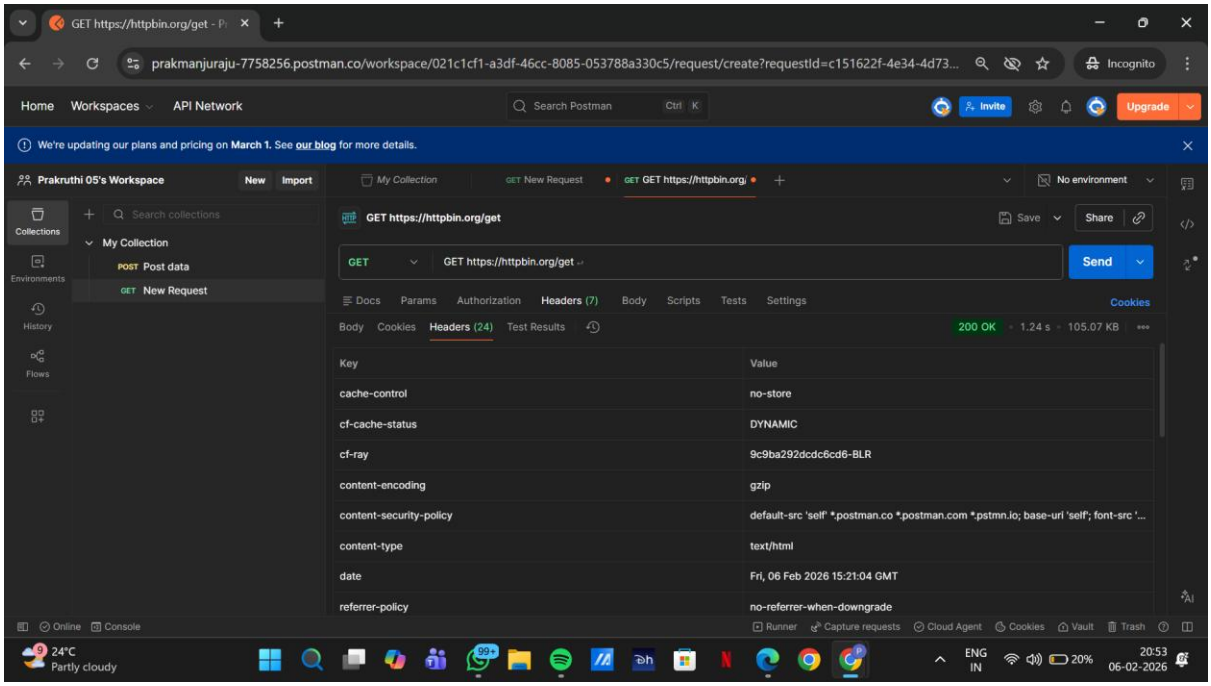

https://httpbin.org/get - Prakru
prakmanjuraju-7758256.postman.co/workspace/021c1cf1-a3df-46cc-8085-053788a330c5/request/create?requestId=c151622f-4e34-4d73-8c32...
Incognito
Home
Workspaces
API Network
Search Postman
Ctrl K
Invite
Upgrade
We're updating our plans and pricing on March 1. See our blog for more details.
Prakruthi 05's Workspace
New
Import
My Collection
GET New Request
GET https://httpbin.org/ge
No environment
Collections
Environments
History
Flows
Search collections
My Collection
POST Post data
GET New Request
https://httpbin.org/get
Save
Share
GET
https://httpbin.org/get
Send
Docs
Params
Authorization
Headers
Body
Scripts
Tests
Settings
Cookies
Body
Cookies
Headers (2)
Test Results
200 OK
1.24 s
1.12 KB
JSON
Preview
Visualize
"args": {},
"headers": {
"Accept": "*/*",
"Accept-Encoding": "gzip, deflate, br, zstd",
"Accept-Language": "en-US,en;q=0.9",
"Cache-Control": "no-cache",
"Host": "httpbin.org",
"Origin": "https://prakmanjuraju-7758256.postman.co",
"Postman-Token": "b6aec9a4-b662-4876-9e2c-1375475331b9",
"Priority": "u=1, i",
"Referer": "https://prakmanjuraju-7758256.postman.co/workspace/
Online
Console
Runner
Capture requests
Browser Agent
Cookies
Vault
Trash
25°C
Partly cloudy
ENG
IN
30%
20:34
06-02-2026

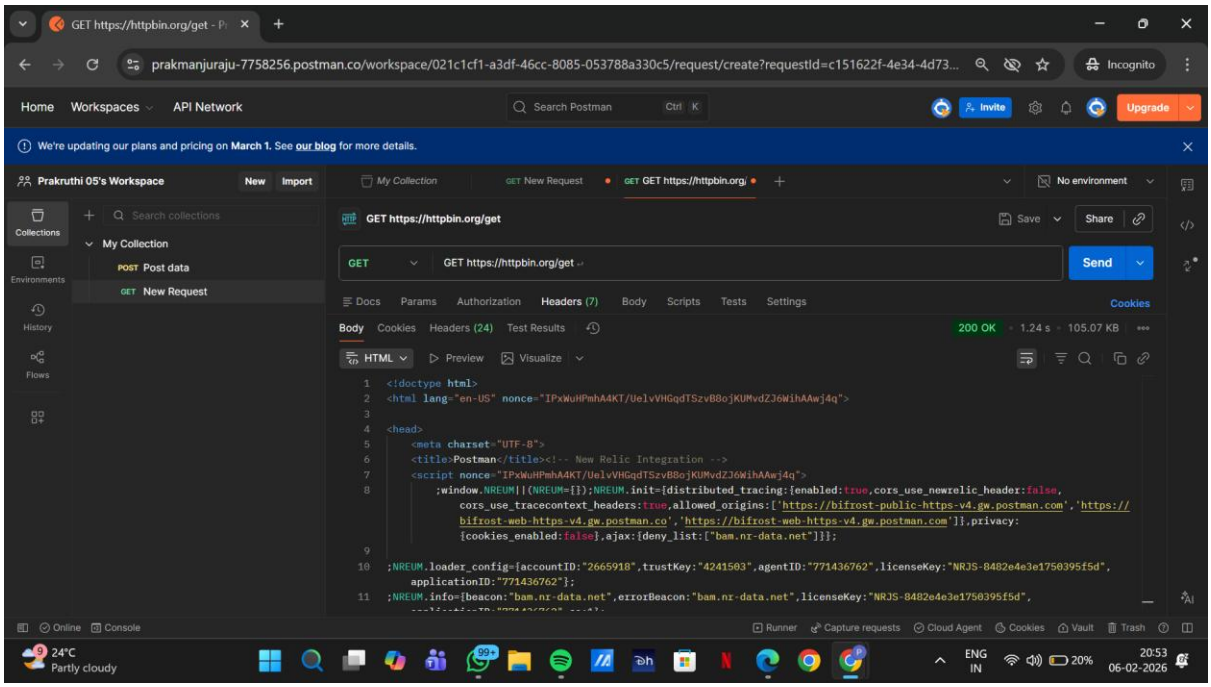

https://httpbin.org/get - Prakru
prakmanjuraju-7758256.postman.co/workspace/021c1cf1-a3df-46cc-8085-053788a330c5/request/create?requestId=c151622f-4e34-4d73...
Incognito
Home
Workspaces
API Network
Search Postman
Ctrl K
Invite
Upgrade
We're updating our plans and pricing on March 1. See our blog for more details.
Prakruthi 05's Workspace
New
Import
My Collection
GET New Request
GET https://httpbin.org/ge
No environment
Collections
Environments
History
Flows
Search collections
My Collection
POST Post data
GET New Request
https://httpbin.org/get
Save
Share
GET
https://httpbin.org/get
Send
Docs
Params
Authorization
Headers (8)
Body
Scripts
Tests
Settings
Cookies
Auth Type
Bearer Token
Token
bGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9....
The authorization header will be automatically generated when you send
Body
Cookies
Headers (7)
Test Results
200 OK
1.69 s
726 B
{ } JSON
Preview
Visualize
{
"args": {},
"headers": {
"Accept": "*/*",
"Accept-Encoding": "gzip, deflate, br",
"Authorization": "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9....",
"Cache-Control": "no-cache",
"Host": "httpbin.org",
Online
Console
Runner
Capture requests
Cloud Agent
Cookies
Vault
Trash
24°C
Partly cloudy
ENG
IN
25%
20:44
06-02-2026


https://httpbin.org/get - Prakru
prakmanjuraju-7758256.postman.co/workspace/021c1cf1-a3df-46cc-8085-053788a330c5/request/create?requestId=c151622f-4e34-4d73...
Incognito
Home
Workspaces
API Network
Search Postman
Ctrl K
Invite
Upgrade
We're updating our plans and pricing on March 1. See our blog for more details.
Prakruthi 05's Workspace
New
Import
My Collection
GET New Request
GET https://httpbin.org/ge
No environment
Collections
Environments
History
Flows
Search collections
My Collection
POST Post data
GET New Request
https://httpbin.org/get
Save
Share
GET
https://httpbin.org/get
Send
Docs
Params
Authorization
Headers (8)
Body
Scripts
Tests
Settings
Cookies
Auth Type
Bearer Token
Token
bGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9....
Body
Cookies
Headers (7)
Test Results
200 OK
1.69 s
726 B
Key
Value
Date
Fri, 06 Feb 2026 15:13:50 GMT
Content-Type
application/json
Content-Length
496
Connection
keep-alive
Server
gunicorn/19.9.0
Access-Control-Allow-Origin
*
Online
Console
Runner
Capture requests
Cloud Agent
Cookies
Vault
Trash
24°C
Partly cloudy
ENG
IN
25%
20:45
06-02-2026


https://httpbin.org/get - Prakru
prakmanjuraju-7758256.postman.co/workspace/021c1cf1-a3df-46cc-8085-053788a330c5/request/create?requestId=c151622f-4e34-4d73...
Incognito
Home
Workspaces
API Network
Search Postman
Ctrl K
Invite
Upgrade
We're updating our plans and pricing on March 1. See our blog for more details.
Prakruthi 05's Workspace
New
Import
My Collection
GET New Request
GET https://httpbin.org/ge
No environment
Collections
Environments
History
Flows
Search collections
My Collection
POST Post data
GET New Request
https://httpbin.org/get
Save
Share
GET
https://httpbin.org/get
Send
Docs
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Auth Type
No Auth
No Auth
This request does not use any authorization.
Body
Cookies
Headers (7)
Test Results
200 OK
1.69 s
726 B
{ } JSON
Preview
Visualize
{
"args": {},
"headers": {
"Accept": "*/*",
"Accept-Encoding": "gzip, deflate, br",
"Authorization": "Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9....",
"Cache-Control": "no-cache",
"Host": "httpbin.org",
"Postman-Token": "92c6fe00-c5d8-4b5d-97cc-2db68ac75d95",
"User-Agent": "PostmanRuntime/7.51.1",
"X-Amzn-Trace-Id": "Root=1-6986052d-6e4fd26855bb15b300a423db"
}
Online
Console
Runner
Capture requests
Cloud Agent
Cookies
Vault
Trash
24°C
Partly cloudy
ENG
IN
24%
20:46
06-02-2026


GET https://httpbin.org/get - Pr
prakmanjuraju-7758256.postman.co/workspace/021c1cf1-a3df-46cc-8085-053788a330c5/request/create?requestId=c151622f-4e34-4d73...
Incognito
Home
Workspaces
API Network
Search Postman
Ctrl K
Invite
Upgrade
We're updating our plans and pricing on March 1. See our blog for more details.
Prakruthi 05's Workspace
New
Import
My Collection
GET New Request
GET GET https://httpbin.org/
No environment
Collections
Environments
History
Flows
Search collections
My Collection
POST Post data
GET New Request
GET https://httpbin.org/get
Save
Share
GET
GET https://httpbin.org/get
Send
Docs
Params
Authorization
Headers (7)
Body
Scripts
Tests
Settings
Cookies
Body
Cookies
Headers (24)
Test Results
200 OK
1.24 s
105.07 KB
HTML
Preview
Visualize
<!doctype html>
<html lang="en-US" nonce="IPxWuHPmhA4KT/UelvVHGqdTSzvB8ojKUMvdZJ6WihAAwj4q">
<head>
<meta charset="UTF-8">
<title>Postman</title><!-- New Relic Integration -->
<script nonce="IPxWuHPmhA4KT/UelvVHGqdTSzvB8ojKUMvdZJ6WihAAwj4q">
;window.NREUM||(NREUM={});NREUM.init={distributed_tracing:{enabled:true,cors_use_newrelic_header:false,
cors_use_tracecontext_headers:true,allowed_origins:['https://bifrost-public-https-v4.gw.postman.com','https://
bifrost-web-https-v4.gw.postman.co','https://bifrost-web-https-v4.gw.postman.com']},privacy:
{cookies_enabled:false},ajax:{deny_list:["bam.nr-data.net"]}};
;NREUM.loader_config={accountID:"2665918",trustKey:"4241503",agentID:"771436762",licenseKey:"NRJS-8482e4e3e1750395f5d",
applicationID:"771436762"};
;NREUM.info={beacon:"bam.nr-data.net",errorBeacon:"bam.nr-data.net",licenseKey:"NRJS-8482e4e3e1750395f5d",
Online
Console
Runner
Capture requests
Cloud Agent
Cookies
Vault
Trash
24°C
Partly cloudy
ENG
IN
21%
20:51
06-02-2026





In Task 13, we performed secure API testing using Postman to understand how REST APIs communicate with backend servers through HTTP methods such as GET and POST. We configured API requests by setting correct endpoints, headers, and request bodies, and tested authentication by sending requests with valid, invalid, and missing credentials to observe access behavior. Authorization testing was carried out by modifying resource identifiers to identify potential Broken Object Level Authorization issues. We further evaluated input validation by sending malformed and unexpected inputs, performed multiple rapid requests to assess rate-limiting enforcement, and reviewed HTTP response codes and error messages for potential security weaknesses. Overall, this task provided hands-on experience in identifying common API security misconfigurations aligned with OWASP API Top 10 risks.