CYBER SECURITY INTERNSHIP

Ministry of MSME, Govt. of India

Task 13

SECURE API TESTING & AUTHORIZATION VALIDATION

JASHMI KS

Secure API testing is the process of verifying that an Application Programming Interface (API) is protected against unauthorized access, data leakage, and misuse. It ensures that only legitimate users and applications can interact with backend services in a controlled and secure manner.

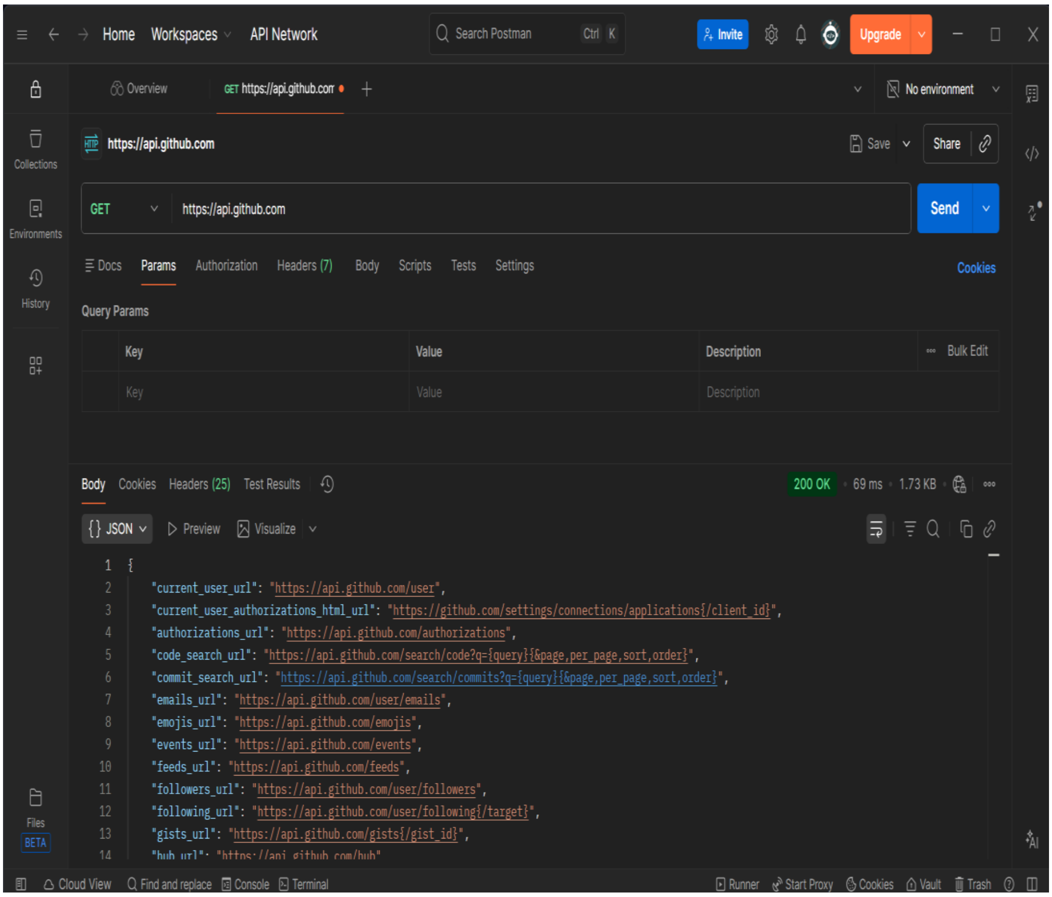
Secure API testing focuses on validating authentication, authorization, input validation, rate limiting, and error handling mechanisms implemented in the API.

Objectives of Secure API Testing

- Prevent unauthorized access to sensitive data
- Ensure proper identity verification
- Protect backend systems from attacks
- Detect security misconfigurations
- Validate compliance with security standards

REST API Requests in Postman:

GET:

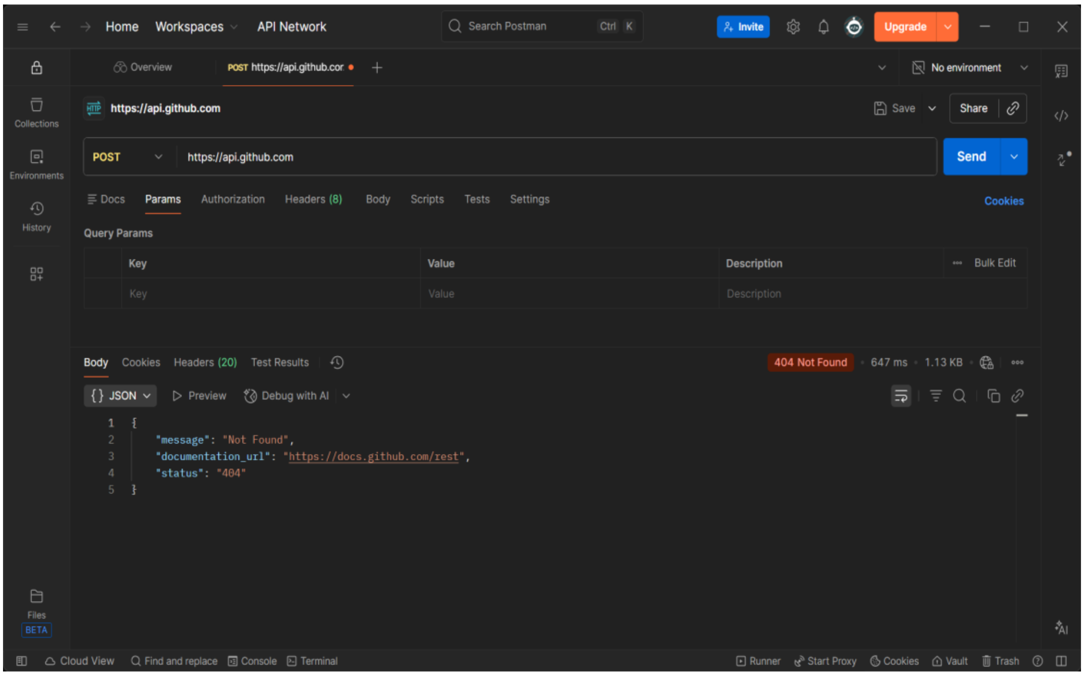


GET https://api.github.com

200 OK · 69 ms · 1.73 KB

```
{
    "current_user_url": "https://api.github.com/user",
    "current_user_authorizations_html_url": "https://github.com/settings/connections/applications{/client_id}",
    "authorizations_url": "https://api.github.com/authorizations",
    "code_search_url": "https://api.github.com/search/code?q={query}{&page,per_page,sort,order}",
    "commit_search_url": "https://api.github.com/search/commits?q={query}{&page,per_page,sort,order}",
    "emails_url": "https://api.github.com/user/emails",
    "emojis_url": "https://api.github.com/emojis",
    "events_url": "https://api.github.com/events",
    "feeds_url": "https://api.github.com/feeds",
    "followers_url": "https://api.github.com/user/followers",
    "following_url": "https://api.github.com/user/following{/target}",
    "gists_url": "https://api.github.com/gists{/gist_id}",
    "hub_url": "https://api.github.com/hub"
```

POST:



https://api.github.com

POST https://api.github.com

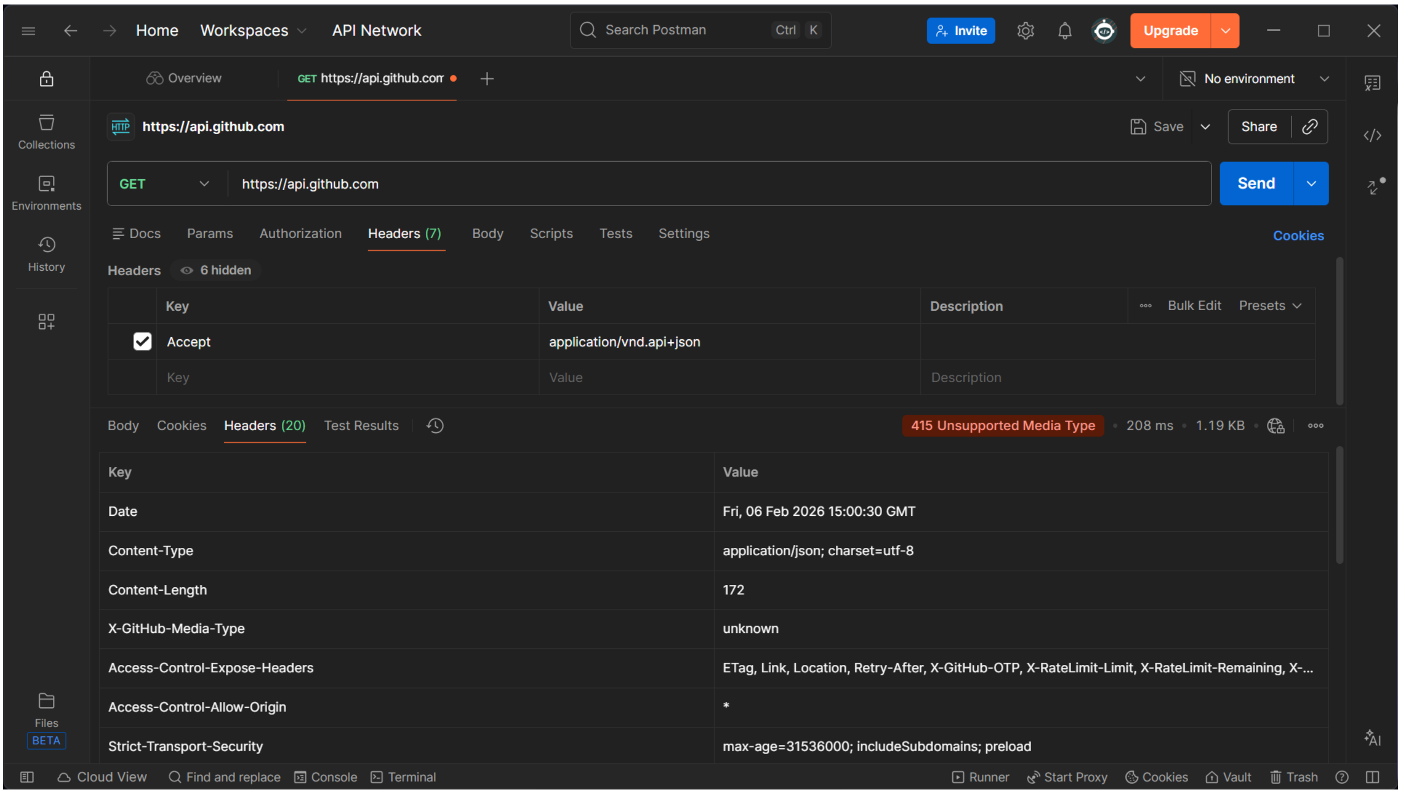
Query Params

Key	Value	Description

404 Not Found · 647 ms · 1.13 KB

```
{
    "message": "Not Found",
    "documentation_url": "https://docs.github.com/rest",
    "status": "404"
}
```

Configuring an API Request in Postman:



https://api.github.com

GET https://api.github.com

Headers (7)

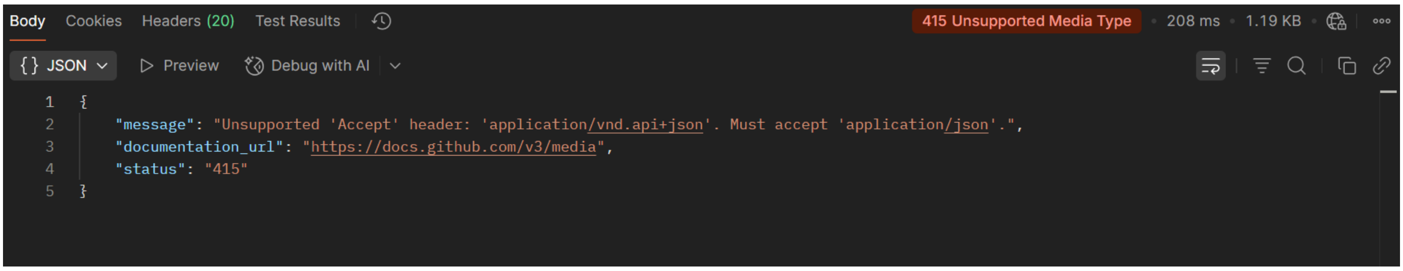
Headers 6 hidden

	Key	Value	Description
☑	Accept	application/vnd.api+json	

415 Unsupported Media Type · 208 ms · 1.19 KB

Headers (20)

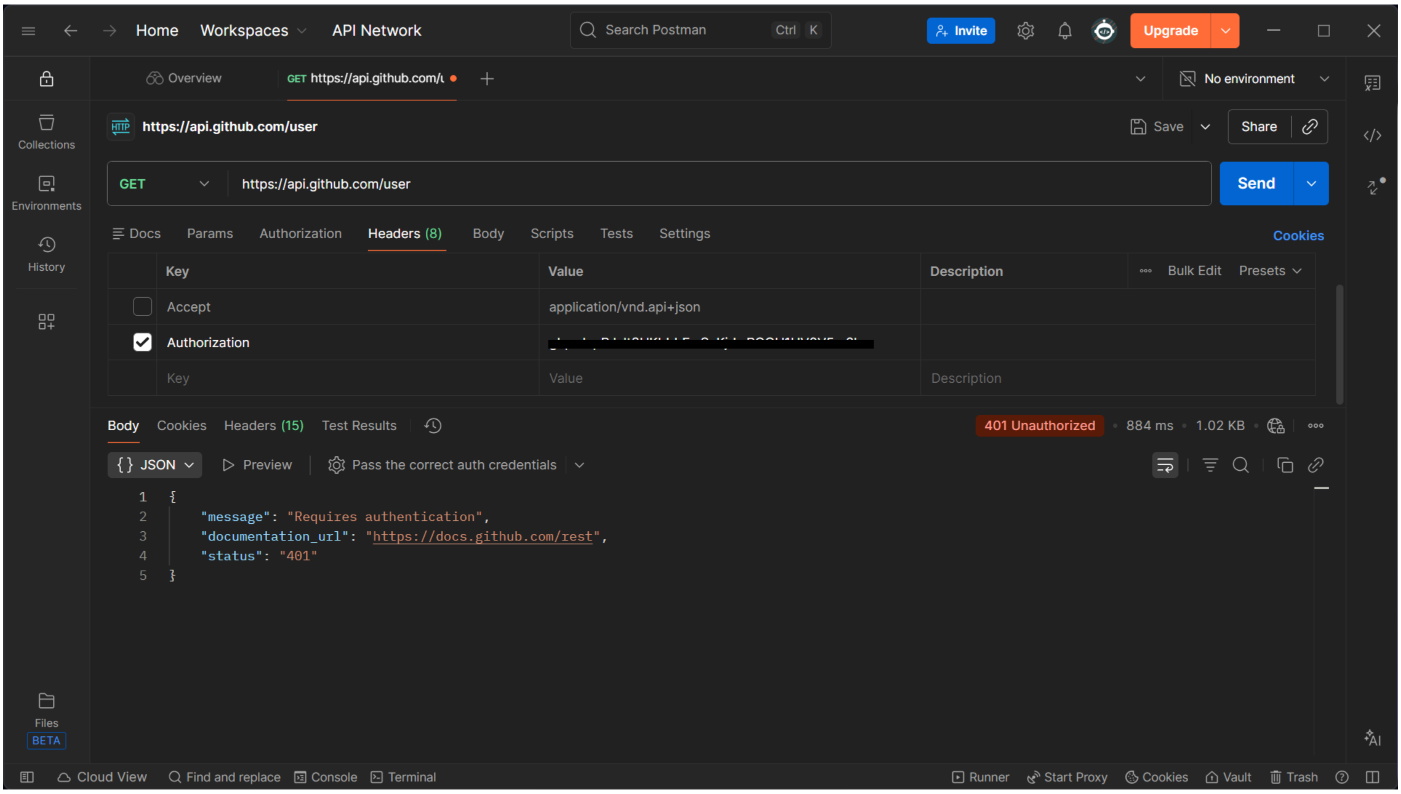
Key	Value
Date	Fri, 06 Feb 2026 15:00:30 GMT
Content-Type	application/json; charset=utf-8
Content-Length	172
X-GitHub-Media-Type	unknown
Access-Control-Expose-Headers	ETag, Link, Location, Retry-After, X-GitHub-OTP, X-RateLimit-Limit, X-RateLimit-Remaining, X-...
Access-Control-Allow-Origin	*
Strict-Transport-Security	max-age=31536000; includeSubdomains; preload



415 Unsupported Media Type · 208 ms · 1.19 KB

```
{
    "message": "Unsupported 'Accept' header: 'application/vnd.api+json'. Must accept 'application/json'.",
    "documentation_url": "https://docs.github.com/v3/media",
    "status": "415"
}
```

Testing Authentication (Valid vs Invalid Token):



https://api.github.com/user

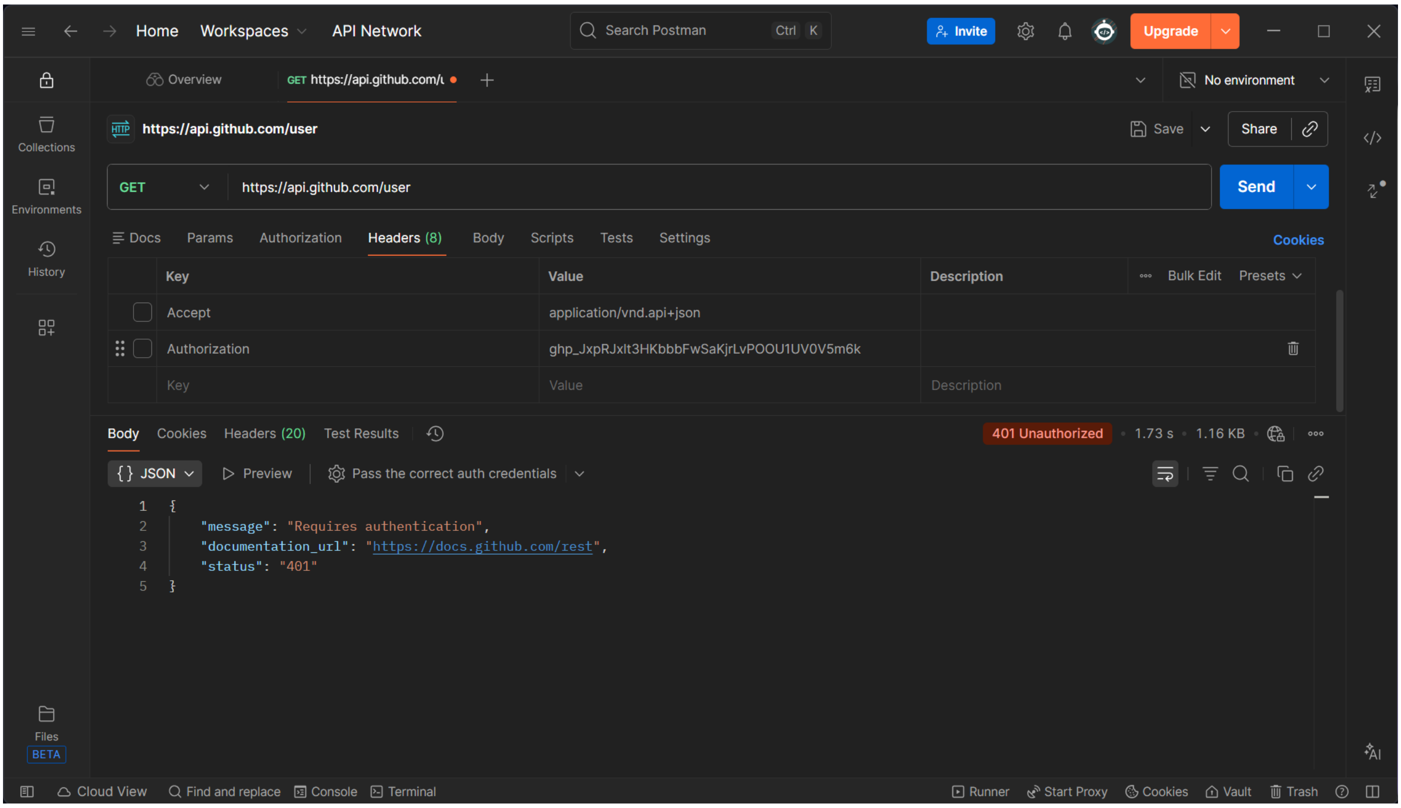
GET https://api.github.com/user

	Key	Value	Description
□	Accept	application/vnd.api+json	
☑	Authorization	[redacted]	
	Key	Value	Description

401 Unauthorized • 884 ms • 1.02 KB

```
{
    "message": "Requires authentication",
    "documentation_url": "https://docs.github.com/rest",
    "status": "401"
}
```

Testing Unauthenticated Access:



https://api.github.com/user

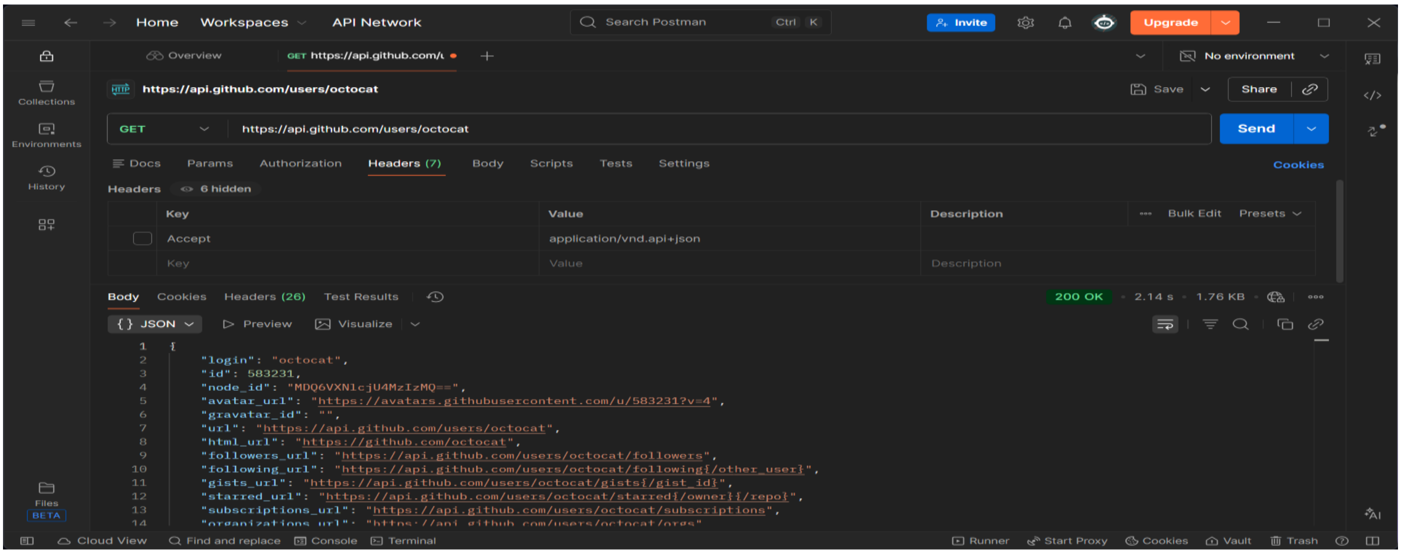
GET https://api.github.com/user

	Key	Value	Description
□	Accept	application/vnd.api+json	
□	Authorization	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	
	Key	Value	Description

401 Unauthorized • 1.73 s • 1.16 KB

```
{
    "message": "Requires authentication",
    "documentation_url": "https://docs.github.com/rest",
    "status": "401"
}
```

Testing Authorization (IDOR Check):


GET https://api.github.com/users/octocat

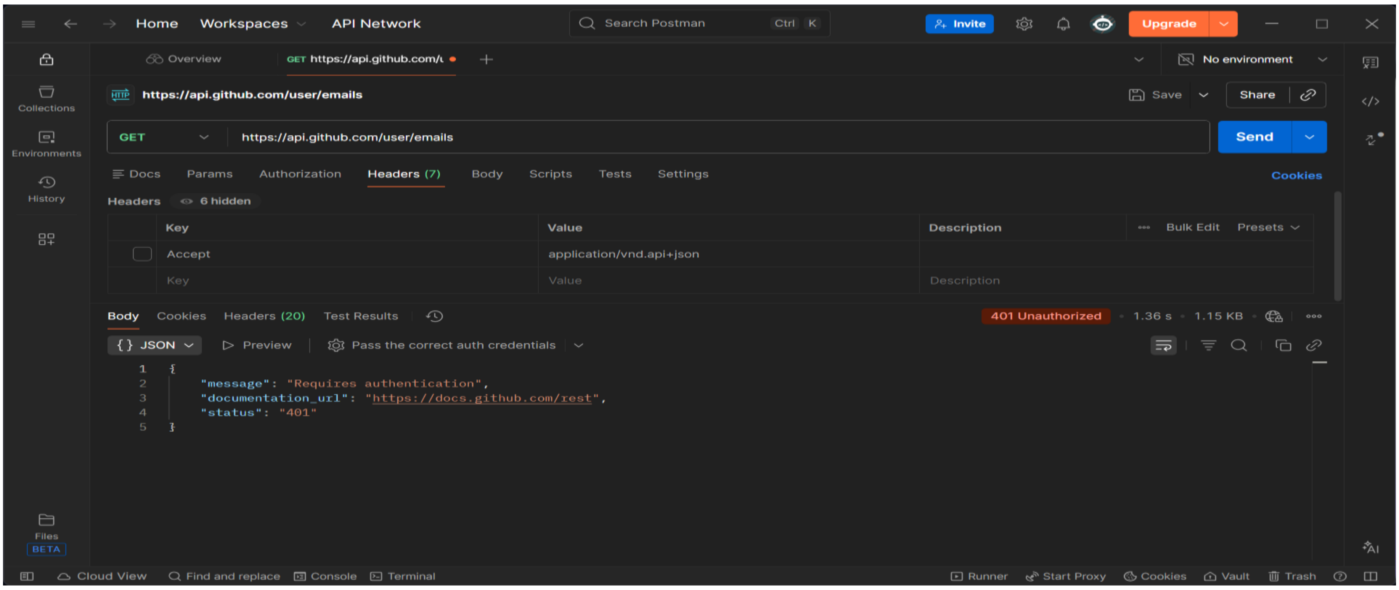
Headers (7) — 6 hidden

Key	Value	Description
Accept	application/vnd.api+json	

Body — Headers (26) — 200 OK · 2.14 s · 1.76 KB

```
{
    "login": "octocat",
    "id": 583231,
    "node_id": "MDQ6VXNlcjU4MzIzMQ==",
    "avatar_url": "https://avatars.githubusercontent.com/u/583231?v=4",
    "gravatar_id": "",
    "url": "https://api.github.com/users/octocat",
    "html_url": "https://github.com/octocat",
    "followers_url": "https://api.github.com/users/octocat/followers",
    "following_url": "https://api.github.com/users/octocat/following{/other_user}",
    "gists_url": "https://api.github.com/users/octocat/gists{/gist_id}",
    "starred_url": "https://api.github.com/users/octocat/starred{/owner}{/repo}",
    "subscriptions_url": "https://api.github.com/users/octocat/subscriptions",
    "organizations_url": "https://api.github.com/users/octocat/orgs"
```

Private:


GET https://api.github.com/user/emails

Headers (7) — 6 hidden

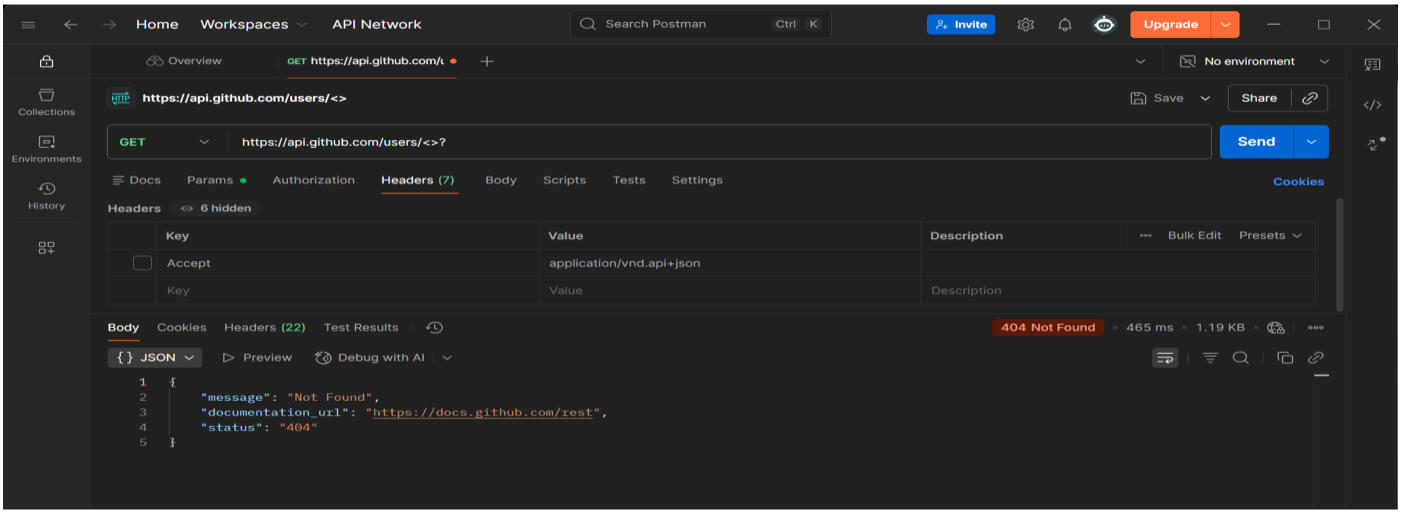
Key	Value	Description
Accept	application/vnd.api+json	

Body — Headers (20) — 401 Unauthorized · 1.36 s · 1.15 KB

Pass the correct auth credentials

```
{
    "message": "Requires authentication",
    "documentation_url": "https://docs.github.com/rest",
    "status": "401"
}
```

Input Validation Testing:


GET https://api.github.com/users/<>?

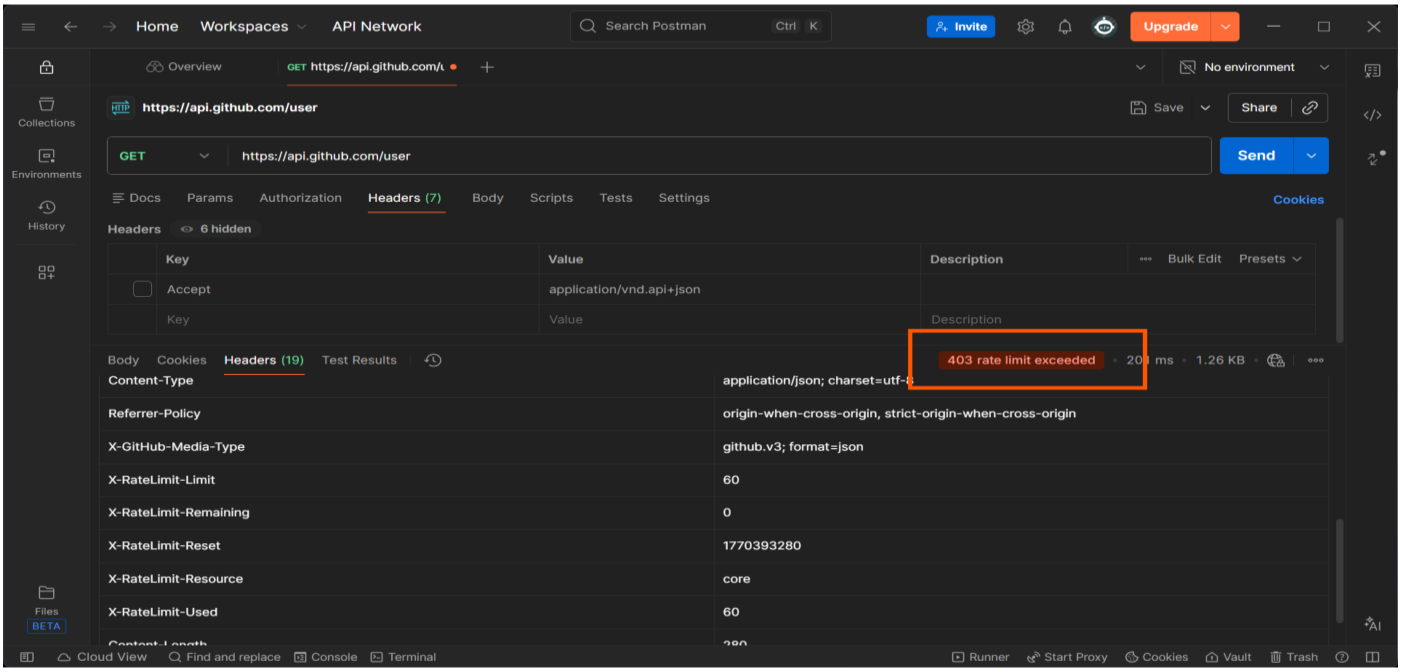
Headers (7) — 6 hidden

Key	Value	Description
Accept	application/vnd.api+json	

Body — Headers (22) — 404 Not Found · 465 ms · 1.19 KB

```
{
    "message": "Not Found",
    "documentation_url": "https://docs.github.com/rest",
    "status": "404"
}
```

Rate Limiting Test:



https://api.github.com/user

GET https://api.github.com/user

Headers 6 hidden

	Key	Value	Description
□	Accept	application/vnd.api+json	
	Key	Value	Description

403 rate limit exceeded • 20[illegible] ms • 1.26 KB

Content-Type	application/json; charset=utf-8
Referrer-Policy	origin-when-cross-origin, strict-origin-when-cross-origin
X-GitHub-Media-Type	github.v3; format=json
X-RateLimit-Limit	60
X-RateLimit-Remaining	0
X-RateLimit-Reset	1770393280
X-RateLimit-Resource	core
X-RateLimit-Used	60
Content-Length	280

Review HTTP Response Codes

Common GitHub API Codes:

Code	Meaning
200	Success
401	Unauthorized
403	Forbidden / Rate limit
404	Not Found
422	Validation error