SECURITY AUDIT REPORT API VULNERABILITY ASSESSMENT

Executive Summary

The security audit of the API endpoint **https://reqres.in/** was conducted to identify potential misconfigurations and information leaks. The assessment revealed that while the API has robust **Bot Mitigation** and **Clickjacking** protections in place, it suffers from Insecure **CORS policies and Infrastructure Leakage** that could be exploited in a targeted attack.

Technical Findings

Finding A: Insecure CORS Configuration (High Risk)

- **Observation:** The header Access-Control-Allow-Origin: http://localhost:5173 was identified.
- **Description:** The API explicitly trusts requests coming from a local development server (Vite default port).
- **Impact:** An attacker could host a malicious website that, if visited by a developer with a local server running on that port, could perform unauthorized actions or leak sensitive data via the developer's authenticated session.
- **Recommendation:** Remove localhost from the allowed origins in production. Use a strict allow-list of verified production domains.

Finding B: Infrastructure Information Leakage (Medium Risk)

- **Observation:** The header Via: 1.1 heroku-router was detected.
- **Description:** Although the service is behind Cloudflare, the Via header confirms that the underlying application is hosted on Heroku.
- **Impact:** This reduces the effort required for an attacker to perform "fingerprinting." They can now focus on Heroku-specific vulnerabilities or platform-specific bypasses.
- **Recommendation:** Configure the server or the Cloudflare WAF to strip the Via and X-Request-Id headers before the response reaches the client.

Finding C: Successful Bot Mitigation (Positive Finding)

- **Observation:** Attempting to automate requests via Postman triggered a **403 Forbidden** with **cf-mitigated: challenge.**
- **Description:** The Cloudflare WAF correctly identified the request as automated/non-browser traffic and issued a security challenge.
- **Impact:** This protects the API from large-scale scraping and automated brute-force attacks.

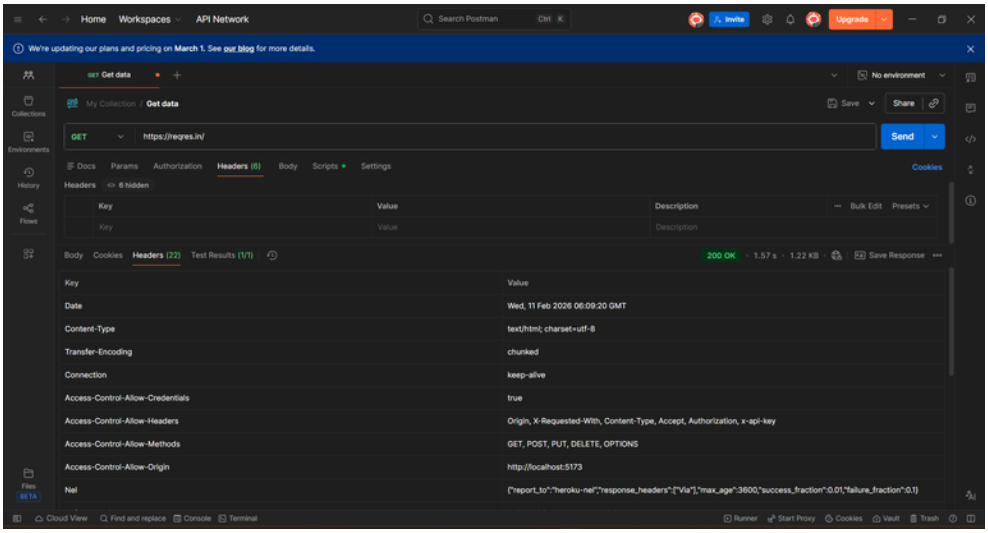
Evidence Summary Table

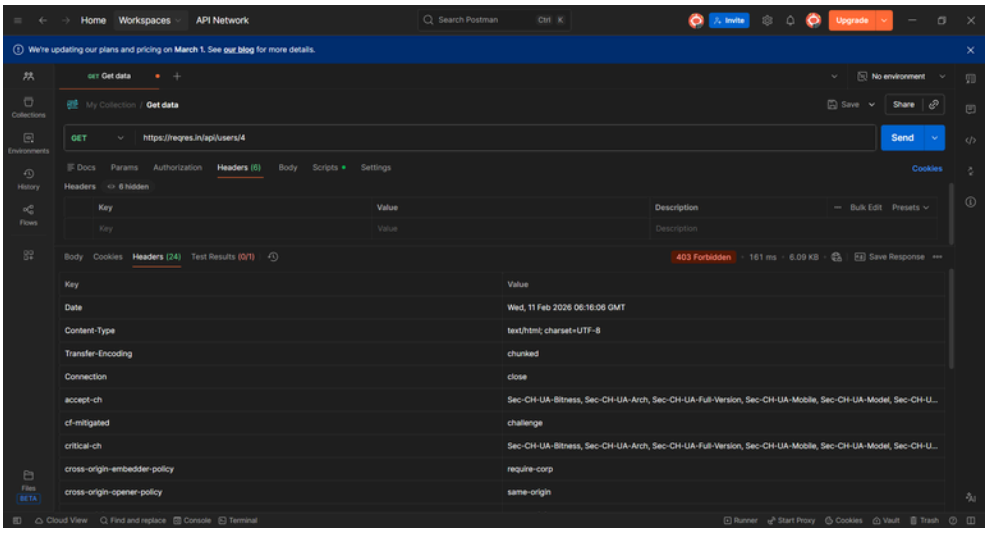
Header	Value / Result	Security Status
Access-Control-Allow-Origin	http://localhost:5173	❌ **Vulnerable**
Via	1.1 heroku-router	⚠️ **Information Leak**
X-Frame-Options	DENY / SAMEORIGIN	✅ **Secure**
X-Content-Type-Options	nosniff	✅ **Secure**
WAF Status	cf-mitigated: challenge	✅ **Active Defense**

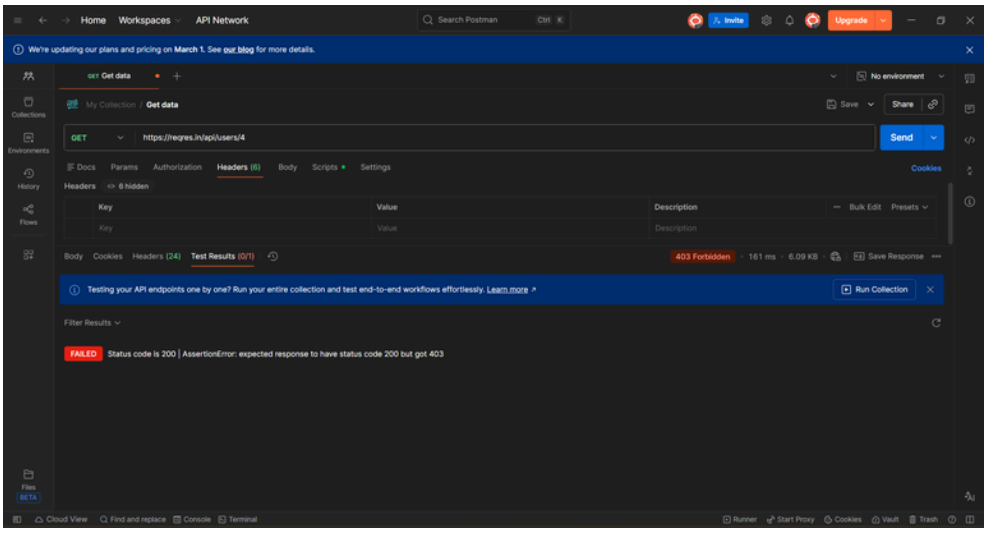
Final Recommendation

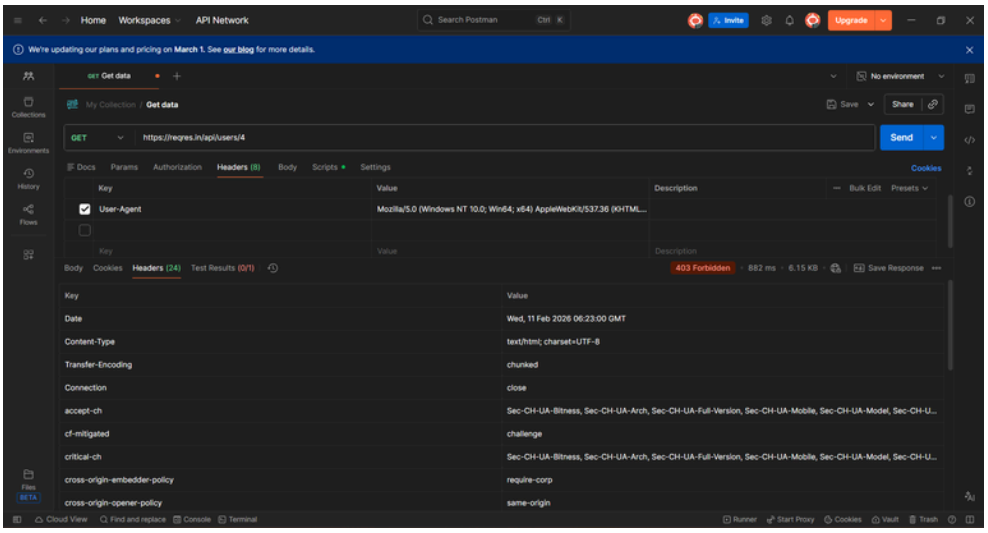
To complete the security hardening of this API, the development team should prioritize fixing the **CORS policy** and masking the backend infrastructure headers. The current **anti-bot** measures are performing as expected and should be maintained.

EVIDENCES






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.
GET Get data
No environment
My Collection / Get data
Save
Share
GET
https://reqres.in/api/users/4
Send
Docs
Params
Authorization
Headers (6)
Body
Scripts
Settings
Cookies
Headers 8 hidden
Key
Value
Description
Bulk Edit
Presets
Body
Cookies
Headers (24)
Test Results (0/1)
403 Forbidden
161 ms
6.09 KB
Save Response
Testing your API endpoints one by one? Run your entire collection and test end-to-end workflows effortlessly. Learn more
Run Collection
Filter Results
FAILED
Status code is 200 | AssertionError: expected response to have status code 200 but got 403
Collections
Environments
History
Flows
Files
BETA
Cloud View
Find and replace
Console
Terminal
Runner
Start Proxy
Cookies
Vault
Trash


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.
GET Get data
No environment
My Collection / Get data
Save
Share
GET
https://reqres.in/api/users/4
Send
Docs
Params
Authorization
Headers (8)
Body
Scripts
Settings
Cookies
Key
Value
Description
Bulk Edit
Presets
User-Agent
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...
Body
Cookies
Headers (24)
Test Results (0/1)
403 Forbidden
882 ms
6.15 KB
Save Response
Key
Value
Date
Wed, 11 Feb 2026 06:23:00 GMT
Content-Type
text/html; charset=UTF-8
Transfer-Encoding
chunked
Connection
close
accept-ch
Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-U...
cf-mitigated
challenge
critical-ch
Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-U...
cross-origin-embedder-policy
require-corp
cross-origin-opener-policy
same-origin
Collections
Environments
History
Flows
Files
BETA
Cloud View
Find and replace
Console
Terminal
Runner
Start Proxy
Cookies
Vault
Trash