



API Security Risk Analysis Report

Security Risk Report

Prepared by:

NAGULAPALLI SRIVIDYA NARASIMHA

Cybersecurity Task 3

INTRODUCTION

This report presents a security risk analysis of the public test API, ReqRes (<https://reqres.in/>). APIs play a crucial role in modern web applications by enabling communication between systems. However, insecure APIs can lead to unauthorized access, data exposure, and cyberattacks. This analysis evaluates the security posture of the selected API and identifies potential risks.

OBJECTIVE

The objective of this task is to perform a read-only API Security Risk Analysis using public or demo APIs. The analysis focuses on identifying common security risks such as unauthenticated access, excessive data exposure, and missing security controls without exploiting or attacking the system. This task helps understand how API security audits are performed in real-world security consulting environments.

API SELECTED

API Name: ReqRes API

Base URL: <https://reqres.in/api>

Why this API?

- It is a public test API designed for learning and practice.
- It simulates real-world features like user login, registration, and data retrieval.
- It allows testing of authentication, authorization, and data exposure scenarios.
- It is suitable for academic security analysis without affecting real systems.

TOOLS & TESTING ENVIRONMENT

Postman

- Sending API requests
- Viewing responses
- Header inspection

Kali Linux Terminal

- Header analysis using curl command

Command Used:

- `curl -I https://reqres.in/api/posts`

TESTING PROCESS

- Reviewed API documentation in browser.
- Selected safe public API endpoints.
- Sent GET requests using Postman.
- Observed response data structure.
- Checked authentication requirements.
- Inspected headers and status codes.
- Identified potential security risks.
- Classified risk severity and documented observations.

ENDPOINTS TESTED

./posts Endpoint

Method: GET

Returns post objects with userId, title, body.

Accessible without authentication.

./users Endpoint

Method: GET

Returns user details such as name, email, phone, address, and company info.

./comments Endpoint

Method: GET

Returns comment records linked to posts

SECURITY FINDINGS

Finding 1- Unauthenticated Endpoint

All tested endpoints are publicly accessible without authentication.

Risk Level: Medium

Impact: Unauthorized users can access API data.

Finding 2 - Excessive Data Exposure

The users endpoint returns full user objects including contact and address details.

Risk Level: Medium

Impact: In real APIs this could lead to information leakage.

Finding 3 - Missing Rate Limiting Indicators

No clear rate-limiting information observed in responses.

Risk Level: Medium

Impact: API may be vulnerable to abuse through excessive requests.

Finding 4 - Public Demo Data

Data appears to be test/demo information.

Risk Level: Low

Impact: No real sensitive data exposure.

RISK SEVERITY TABLE

Identified Risk	Severity	Potential Impact
Unauthenticated Endpoint Access	High	Unauthorized users may access sensitive data
Excessive Data Exposure	Medium	More data than necessary is exposed to clients
Missing Rate Limiting	Medium	Brute-force and automated attacks possible
Demo / Public Data Exposure	Low	Public test data accessible without restrictions

REMEDIATION RECOMMENDATIONS

To improve API security, the following practices are recommended:

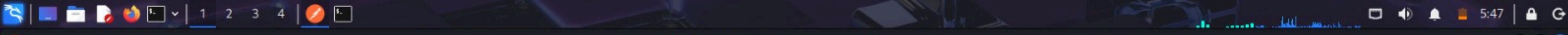
- Implement authentication tokens (API keys / OAuth).
- Return only required fields in responses.
- Enable rate limiting to prevent abuse.
- Apply input validation for request data.
- Use security headers consistently.

SCREENSHOTS

A screenshot of a Kali Linux terminal window titled "root@kali: /home/kali". The terminal displays the output of a curl command to https://reqres.in/api/posts, showing various HTTP headers including Content-Type: text/html; charset=UTF-8, Content-Length: 9031, and a long list of Sec-CH-UA-* headers. The terminal interface includes a top bar with icons for file operations and system status, and a bottom bar with session management buttons.

```
(root㉿kali)-[~/home/kali]
# curl -I https://reqres.in/api/posts
HTTP/2 403
date: Thu, 19 Feb 2026 10:57:36 GMT
content-type: text/html; charset=UTF-8
content-length: 9031
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-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platform, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform-Version, UA-Platform, UA
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-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platform, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform-Version, UA-Platform, UA
cross-origin-embedder-policy: require-corp
cross-origin-opener-policy: same-origin
cross-origin-resource-policy: same-origin
origin-agent-cluster: ?1
permissions-policy: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),gyroscope=(),hid=(),interest-cohort=(),magnetometer=(),microphone=(),payment=(),publickey-credentials-get=(),screen-wake-lock=(),serial=(),sync-xhr=(),usb=()
referrer-policy: same-origin
server-timing: chlray;desc="9d053e8b9d2e3978"
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
cache-control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
expires: Thu, 01 Jan 1970 00:00:01 GMT
report-to: {"endpoints": [{"url": "https://a.nel.cloudflare.com/report/v4?s=I6kRIx%2Fv8rcVV%2BovztQbgjq3GcR00RSNNSC509XTW8BAF4bPaut6st5r03yZm50gQGyFh%2F3Jfdt697rYWx3jB9dEes97Y5R4vY2ENLDDwZmCiMvi7WDIUC5R3Q%3D%3D"}], "group": "cf-nel", "max_age": 604800}
nel: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
server: cloudflare
cf-ray: 9d053e8b9d2e3978-MAA

(root㉿kali)-[~/home/kali]
#
```



https://reqres.in/api/users - My Workspace

File Edit View Help

Home Workspaces Explore

Search Postman

You are using the Lightweight API Client, sign in or create an account to work with collections, environments and unlock all free features in Postman.

History New Import

HTTP https://reqres.in/api/users

GET https://reqres.in/api/users

Save

Params Authorization Headers (6) Body Pre-request Script Tests Settings Cookies

Query Params

Key	Value
Key	Value

Body Cookies Headers (24) Test Results

Status: 403 Forbidden Time: 450 ms Size: 5.98 KB Save Response

Pretty Raw Preview Visualize HTML

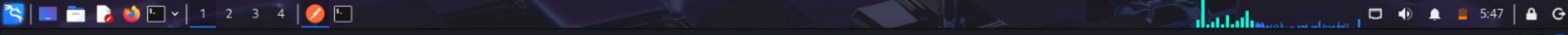
```
4 <head>
5   <title>Just a moment...</title>
6   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
7   <meta http-equiv="X-UA-Compatible" content="IE=Edge">
8   <meta name="robots" content="noindex,nofollow">
9   <meta name="viewport" content="width=device-width,initial-scale=1">
10  <style>
11    * {
12      box-sizing: border-box;
13      margin: 0;
14      padding: 0
15    }
16
17  html {
18    line-height: 1.15;
19    -webkit-text-size-adjust: 100%;
20    color: #313131;
21    font-family: system-ui, -apple-system, BlinkMacSystemFont, "Segoe UI", Roboto, "Helvetica Neue", Arial, "Noto Sans", sans-serif, "Apple Color Emoji", "Segoe UI Emoji", "Segoe UI Symbol", "Noto Color Emoji"
22  }
23
24  body {
25    display: flex;
26    flex-direction: column;
27    height: 100vh;
28    min-height: 100vh
--
```

Create collections in Postman

Use collections to save your requests and share them with others.

Create a Collection

Console Not connected to a Postman account



https://reqres.in/api/users - My Workspace

File Edit View Help

Home Workspaces Explore

Search Postman

You are using the Lightweight API Client, sign in or create an account to work with collections, environments and unlock all free features in Postman.

History New Import

HTTP https://reqres.in/api/users

GET https://reqres.in/api/users

Save </>

Send Cookies

Query Params

Key	Value
Date	Thu, 19 Feb 2026 10:47:19 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-
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-
cross-origin-embedder-policy	require-corp
cross-origin-opener-policy	same-origin
cross-origin-resource-policy	same-origin
origin-agent-cluster	?1
permissions-policy	accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),gyr
referrer-policy	same-origin
server-timing	chlray;desc="9d052f7c0d25914f"
x-content-type-options	nosniff
x-frame-options	SAMEORIGIN
Cache-Control	private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Status: 403 Forbidden Time: 450 ms Size: 5.98 KB Save Response

Create collections in Postman

Use collections to save your requests and share them with others.

Create a Collection

Console Not connected to a Postman account

Kali Linux

reqres.in/api/comments

reqres.in/api/posts

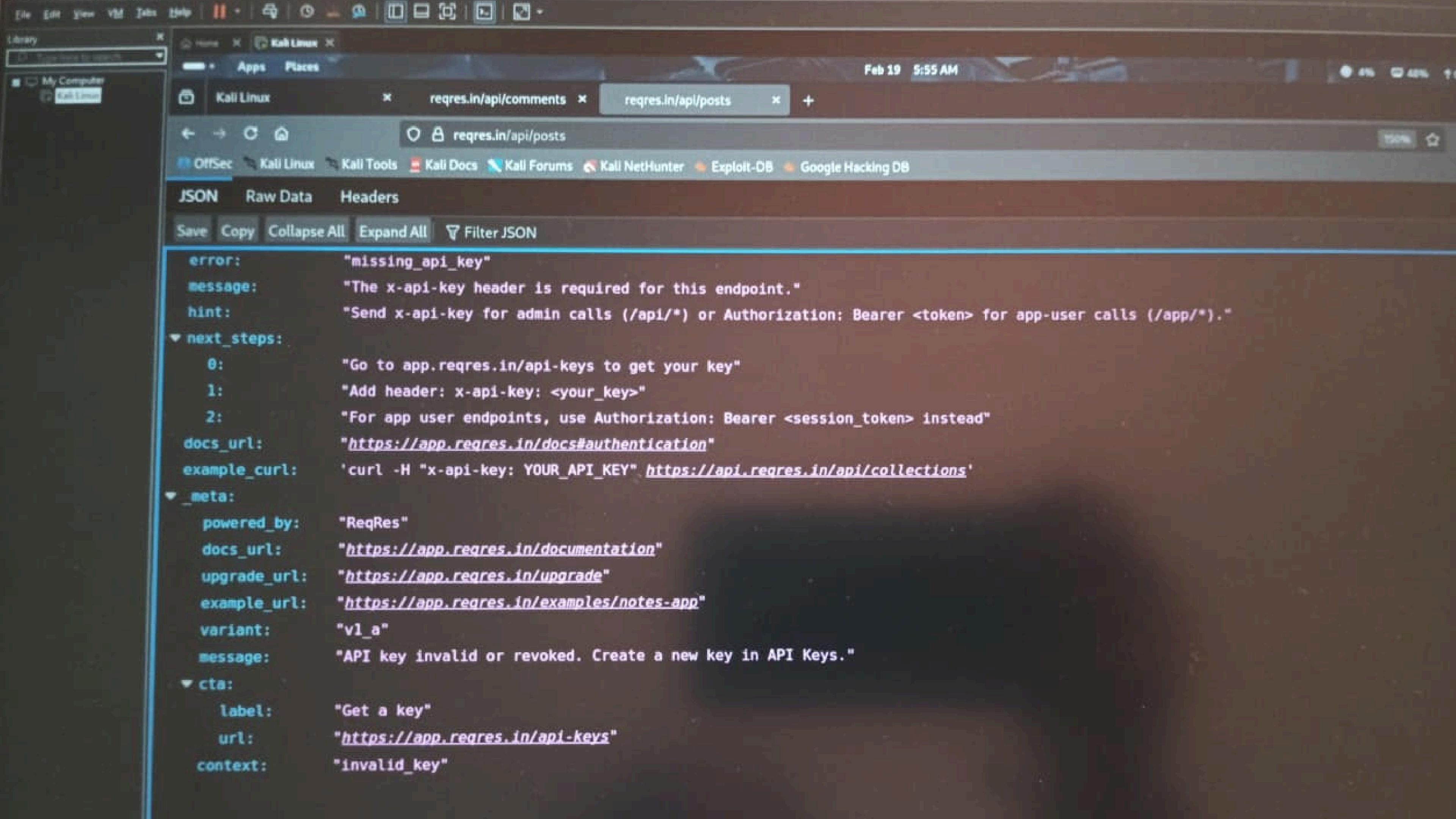
Feb 19 5:56 AM

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

```
error: "missing_api_key"
message: "The x-api-key header is required for this endpoint."
hint: "Send x-api-key for admin calls (/api/*) or Authorization: Bearer <token> for app-user calls (/app/*)."
next_steps:
  0: "Go to app.reqres.in/api-keys to get your key"
  1: "Add header: x-api-key: <your_key>"
  2: "For app user endpoints, use Authorization: Bearer <session_token> instead"
docs_url: "https://app.reqres.in/docs#authentication"
example_curl: 'curl -H "x-api-key: YOUR_API_KEY" https://api.reqres.in/api/collections'
meta:
  powered_by: "ReqRes"
  docs_url: "https://app.reqres.in/documentation"
  upgrade_url: "https://app.reqres.in/upgrade"
  example_url: "https://app.reqres.in/examples/notes-app"
  variant: "v1_a"
  message: "API key invalid or revoked. Create a new key in API Keys."
cta:
  label: "Get a key"
  url: "https://app.reqres.in/api-keys"
  context: "invalid_key"
```



CONCLUSION

This assessment demonstrated a basic API security review using safe and ethical testing methods. The API endpoints were openly accessible and highlighted common risks such as unauthenticated access and excessive data exposure. Although the API contains demo data, the analysis reflects real-world API security considerations and provides practical experience in documenting security risks professionally.