

Forum:[Hack Forums](#)

Thread: [API Security Testing Checklist \(Legal Lab Walkthrough\)](#)

Vectura - October 5, 2025, 10:06 am

API Security Testing Checklist (Legal Lab Walkthrough)

Intro: A practical checklist to test REST/GraphQL APIs for common security issues and to harden them: auth, rate limiting, input validation, and object-level access control — all in a local dev/staging lab.

Prerequisites: A local API server (sample app) or staging with test data

Tools: curl, Postman, Burp Suite (for authorized testing)

Steps (lab):

Map endpoints & auth flow — list all endpoints, methods, headers, and required scopes.

Test authentication enforcement — verify endpoints reject missing/invalid tokens.

Code # example: request without token

```
curl -i -X GET http://localhost:4000/api/users
```

Check object-level authorization — attempt to access another user's resource with a valid token in lab to verify proper checks.

Test rate limiting & throttling — generate controlled bursts and observe API responses and rate headers.

Input validation & JSON schema enforcement — send malformed JSON and verify server returns 4xx with sanitized messages.

Inspect CORS & security headers — ensure strict CORS policy and security headers (CSP, HSTS).

Hardening checklist for devs: Strict token validation and short TTLs

Object-level ACLs enforced server-side

Rate limiting & IP reputation checks

Input schema validation and output encoding

Audit logs with request IDs for tracing

Exercises: Use Postman to create automated tests that assert auth and ACL behavior for each endpoint.

Implement and test a per-IP rate limiter in your local API and measure throughput.

Note: Only test APIs in your dev/staging environment or with explicit permission.