🔹 Task 13: Secure API Testing & Authorization Validation

By : NROUPSINH GOHIL

🛠 Tools Used

- **Primary:** Postman

📌 Objective

To test REST APIs for **authentication**, **authorization**, **input validation**, and **rate-limiting** issues, and map findings to **OWASP API Security Risks**.

🔍 Understanding REST APIs

REST APIs allow applications to communicate using HTTP methods:

Method	Purpose
GET	Retrieve data
POST	Create data
PUT	Update data
DELETE	Remove data

APIs commonly use **tokens, API keys, or Bearer authentication** to restrict access.

⚙️ Practical Testing Performed (Step-by-Step)

1️⃣ API Configuration in Postman

- Configured API endpoint URL
- Added headers:
    - Authorization: Bearer <token>
    - Content-Type: application/json

✔ Valid requests returned **200 OK**

2️⃣ Authentication Testing

- Sent requests with:
    - ✅ Valid token → Access granted
    - ❌ Invalid token → **401 Unauthorized**

- ❌ No token → **401 Unauthorized**

✔ Authentication properly enforced

3️⃣ Authorization Testing (Broken Object Level Authorization)

- Modified resource IDs in requests
  - Example: /api/users/101 → /api/users/102

⚠️ **Observation:**
Unauthorized access was allowed for modified IDs in some cases.

🚨 **Vulnerability Identified:** Broken Authorization

4️⃣ Unauthenticated Access Test

- Removed Authorization header
- Resent request

✔ API correctly denied access
❌ If access allowed → Critical misconfiguration

5️⃣ Input Validation Testing

- Sent malformed inputs:

```
{
 "username": "admin' OR '1'='1",
 "email": "<script>alert(1)</script>"
}
```

⚠️ **Observation:**
API accepted unexpected inputs without validation.

🚨 **Risk:** Injection / XSS through API

6️⃣ Rate Limiting Test

- Sent multiple rapid requests

⚠️ **Observation:**
No rate-limit error received (No 429 status)

🚨 **Risk:** Brute-force & DoS vulnerability

7️⃣ HTTP Response Code Analysis

Code Meaning

200 Success

401 Unauthorized

403 Forbidden

429 Too Many Requests

500 Server Error

✔ Error messages revealed excessive internal details → **Information Disclosure Risk**

🧠 Vulnerabilities Identified & OWASP API Mapping

Vulnerability	OWASP API Risk
Broken Authorization	API1:2023
No Rate Limiting	API4:2023
Weak Input Validation	API8:2023
Excessive Error Info	API7:2023

🔐 Security Recommendations

- Enforce **strict authorization checks**
- Validate all user input (server-side)
- Implement **rate limiting**
- Use generic error messages
- Log suspicious API activity

📄 Deliverables

✅ Files Included

- API Security Testing Report
- README.md