1️⃣ STEP 1: Test GET Request (Basic API Working)

▶ Action

1. Method: **GET**
2. URL:

https://reqres.in/api/users?page=1

3. Click **Send**

✓ Result

- Status: 200 OK
- JSON user data displayed

📌 *This confirms the API endpoint is reachable.*

2️⃣ STEP 2: Test POST Request (Authentication)

▶ Action

1. Method: **POST**
2. URL:

https://reqres.in/api/login

3. Go to **Body → raw → JSON**
4. Paste:

```
{
 "email": "eve.holt@reqres.in",
 "password": "cityslicka"
}
```

5. Click **Send**

✓ Result

- Status: 200 OK
- Token received

📌 *Authentication successful.*

3️⃣ STEP 3: Test Invalid Authentication

▶ Action

Change password:

{

"email": "eve.holt@reqres.in",

"password": "wrongpassword"

}

Click **Send**

❌ **Result**

- Status: 400 Bad Request
- Error message shown

📌 *API blocks invalid credentials.*

4️⃣ **STEP 4: Remove Authentication (Security Test)**

▶ **Action**

1. Remove **Body data**
2. Click **Send**

✓ **Expected Result**

- 401 Unauthorized or 403 Forbidden

⚠️ **If API still allows access → Security flaw**

5️⃣ **STEP 5: Broken Authorization (IDOR Test)**

▶ **Action**

1. Method: **GET**
2. URL:

https://reqres.in/api/users/2

3. Click **Send**

Now change:

https://reqres.in/api/users/1

🔍 **Observation**

- Are you accessing another user's data?

📌 *If no authorization check → IDOR vulnerability*

6️⃣ STEP 6: Input Validation Test

▶ Action

1. Method: **POST**
2. URL:

https://reqres.in/api/register

3. Body → raw → JSON

```
{
 "email": "<script>alert(1)</script>",
 "password": "123"
}
```

4. Click **Send**

🔍 Observe

- Error messages?
- Script execution?
- Stack trace?

⚠️ *Improper validation = Injection risk*

7️⃣ STEP 7: Rate Limiting Test

▶ Action

1. Click **Send** repeatedly (10–15 times quickly)

✓ Secure API

- 429 Too Many Requests

❌ Insecure API

- Always 200 OK

📌 *No rate limit = brute force risk*

8️⃣ STEP 8: Analyze HTTP Response Codes

Code	Meaning	Security Check
200	OK	Success

Code	Meaning	Security Check
400	Bad Request	Input validation
401	Unauthorized	Auth enforced
403	Forbidden	Access denied
429	Too Many Requests	Rate limiting
500	Server Error	Info leakage

📝 STEP 9: Write Practical Report (IMPORTANT)

Example format:

API Tested: /api/login

Method: POST

Test Case: Invalid credentials

Response Code: 400

Observation: API rejected invalid login

Result: Secure