# API Security Testing Lab

Author: Harshal Harekar

Date: 28/10/2025

## Objective

Test API endpoints for BOLA, authentication flaws, GraphQL injection, and rate-limit bypass. Produce checklist, findings CSV, 50-word summary, and technical remediation.

## Tools

Burp Suite, Postman, sqlmap, curl, jq.

## Environment

PortSwigger Web Security Academy’s Labs

Attacker host with Burp as proxy.

## Steps

1. Access PortSwigger Web Security Academy’s IDOR Lab.

(IDOR is another name BOLA)

A screenshot of a computer

AI-generated content may be incorrect.

2. Enumerate and Find the API and test for BOLA

* In the lab’s web page, click around.
* Log in using the provided creds (wiener:peter)
* After logging in, Select the Live chat tab.
* Send a message and then select View transcript.
* Review the URL and observe that the transcripts are text files assigned a filename containing an incrementing number.

A screenshot of a computer

AI-generated content may be incorrect.

* Change the filename to 1.txt and review the text. Notice a password within the chat transcript.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Return to the main lab page and log in using the stolen credentials.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Log

|  |  |  |  |
| --- | --- | --- | --- |
| Test ID | Vulnerability | Severity | Target Endpoint |
| 1 | BOLA | Critical | /download-transcript/1.txt |

## Summary

The API security test targeted Broken Object Level Authorization (BOLA) vulnerabilities in the live chat transcript feature. By manipulating transcript filenames in the URL (e.g., changing to ‘1.txt’ ), unauthorized access to other users’ chat data was achieved. This exposed sensitive credentials due to predictable file naming and missing access controls. Manual testing with Burp Suite confirmed the flaw, enabling unauthorized login and validating the severity of the issue.