PORTSWIGGER LABS ASSIGNMENT NO: 5

Name: ABHIJITH B
Email ID: abhijithbalagopal@gmail.com
Submission Date: 28-10-2025
Batch: CSA-JUNE-2025

LABS COMPLETED

1. SQL INECTION
2. CROSS-SITE SCRIPTING (XSS)
3. WEB CACHE POISONING
4. JWT (JSON WEB TOKEN)

1. SQL INJECTION

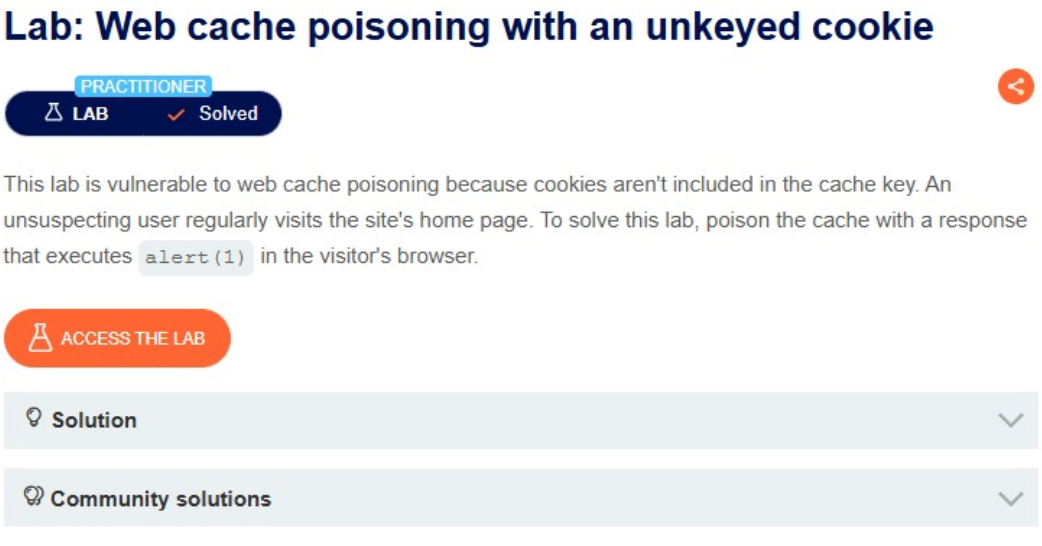
SQL injection (SQLi) is a web-security vulnerability that lets an attacker manipulate the SQL queries your application sends to its database. If app builds SQL by directly concatenating user input, an attacker can supply input that changes the meaning of the query — potentially reading, modifying, or deleting data, or even executing administrative commands on the database.

2. CROSS-SITE SCRIPTING (XSS)

Cross-Site Scripting (XSS) is a web security vulnerability that allows an attacker to inject **malicious scripts (usually JavaScript)** into web pages that other users view. When the victim's browser loads the affected page, the malicious script executes in the victim's context — often giving the attacker access to sensitive information or control over the user's session.

3. WEB CACHE POISONING

Web Cache Poisoning is a web security vulnerability where an attacker tricks a caching server (like a CDN or reverse proxy) into storing a malicious or manipulated version of a response. Once the cache is poisoned, **all users who request the cached resource** will receive the attacker's malicious version — making this a powerful, large-scale attack.



4. JWT (JSON WEB TOKEN)

JWT (JSON Web Token) is a compact, URL-safe way to represent **claims** securely between two parties — typically used for **authentication and authorization** in web applications and APIs. It's a digitally signed token that allows servers to verify a user's identity **without storing session data on the server**