

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 INJECTION**
- 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.

Lab: SQL injection vulnerability allowing login bypass

APPRENTICELAB✓ Solved<

This lab contains a SQL injection vulnerability in the login function.

To solve the lab, perform a SQL injection attack that logs in to the application as the `administrator` user.

ACCESS THE LAB

Solution

Community solutions

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

APPRENTICELAB✓ Solved<

This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

ACCESS THE LAB

Solution

Community solutions

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.

Lab: Reflected XSS into HTML context with nothing encoded

APPRENTICE

LAB

Solved

This lab contains a simple reflected cross-site scripting vulnerability in the search functionality.

To solve the lab, perform a cross-site scripting attack that calls the `alert` function.

ACCESS THE LAB

Solution

Community solutions

Lab: Stored XSS into HTML context with nothing encoded

APPRENTICE

LAB

Solved

This lab contains a stored cross-site scripting vulnerability in the comment functionality.

To solve this lab, submit a comment that calls the `alert` function when the blog post is viewed.

ACCESS THE LAB

Solution

Community solutions

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.

Lab: Web cache poisoning with an unkeyed header

PRACTITIONER
LAB Solved



This lab is vulnerable to web cache poisoning because it handles input from an unkeyed header in an unsafe way. An unsuspecting user regularly visits the site's home page. To solve this lab, poison the cache with a response that executes `alert(document.cookie)` in the visitor's browser.

Hint



ACCESS THE LAB

Solution



Community solutions



Lab: Web cache poisoning with an unkeyed cookie

PRACTITIONER
LAB Solved



This lab is vulnerable to web cache poisoning because cookies aren't included in the cache key. An unsuspecting user regularly visits the site's home page. To solve this lab, poison the cache with a response that executes `alert(1)` in the visitor's browser.

ACCESS THE LAB

Solution



Community solutions



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**

Lab: JWT authentication bypass via unverified signature

APPRENTICE
LAB Solved

This lab uses a JWT-based mechanism for handling sessions. Due to implementation flaws, the server doesn't verify the signature of any JWTs that it receives.

To solve the lab, modify your session token to gain access to the admin panel at `/admin`, then delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

Tip

We recommend familiarizing yourself with [how to work with JWTs in Burp Suite](#) before attempting this lab.

ACCESS THE LAB

Solution

Community solutions

Lab: JWT authentication bypass via flawed signature verification

APPRENTICE
LAB Solved

This lab uses a JWT-based mechanism for handling sessions. The server is insecurely configured to accept unsigned JWTs.

To solve the lab, modify your session token to gain access to the admin panel at `/admin`, then delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

Tip

We recommend familiarizing yourself with [how to work with JWTs in Burp Suite](#) before attempting this lab.

ACCESS THE LAB

Solution

Community solutions