

Assignment 1: Vulnerability Labs

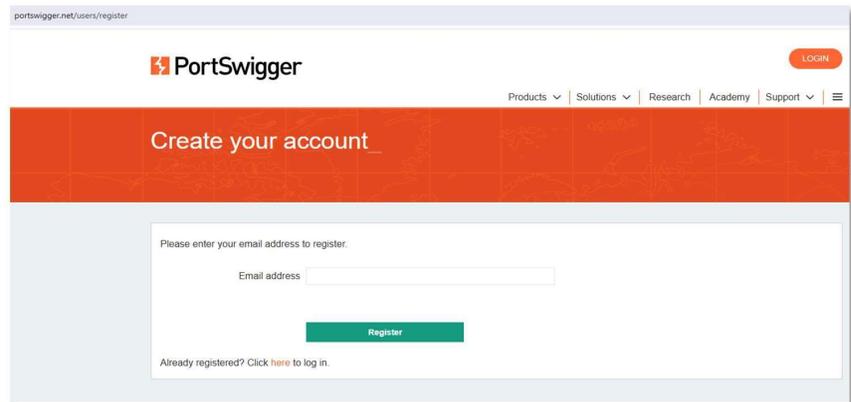
Version: February 17, 2026

COSC 3371
Spring 2026

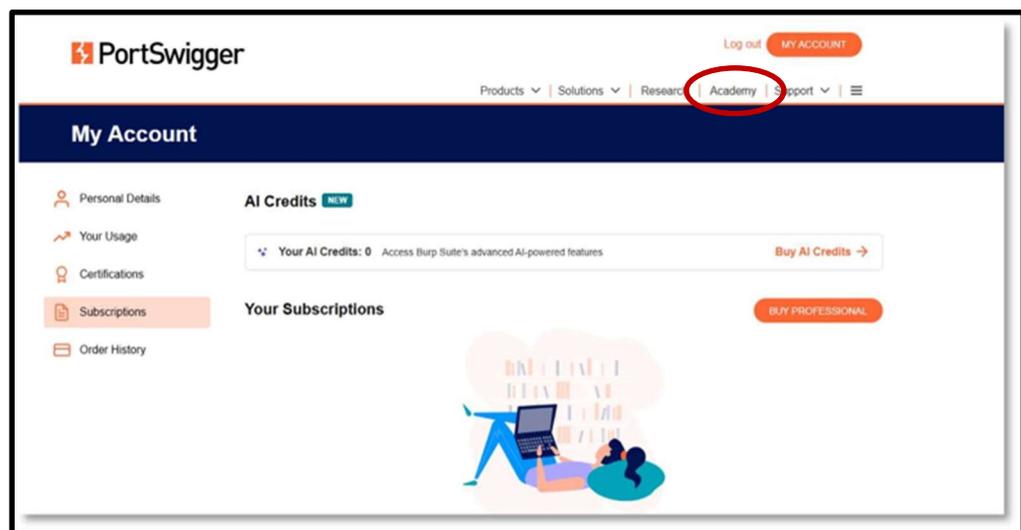
[1] Objectives: The goal of this assignment is to build your practical understanding of common web application vulnerabilities by working through guided labs on the PortSwigger Web Security Academy platform. The best way to learn about vulnerabilities is by trying them. These safe, structured exercises will help you recognize insecure coding patterns, understand how attackers exploit them, and strengthen your ability to design and implement more secure systems.

[2] Description: Follow the instructions below. The website will provide plenty of help.

1. Register an account at <https://portswigger.net/users/register>.



2. Use your UH email to register.
3. Log in using your credentials.



4. Click on "Academy" in the top right corner. You will see your dashboard.

Welcome back!

Learn to secure the web one step at a time, with our practical, interactive learning materials. Covering the latest research, and completely free.

New topic: Web cache deception



Learn how to discover and exploit web cache deception vulnerabilities using new powerful techniques that exploit RFC ambiguities, bypassing the limitations of web cache deception attacks you may already be familiar with. Content and labs based on Gotta cache em all: bending the rules of web cache exploitation, first presented by PortSwigger Research at Black Hat USA 2024.

[Learn more](#)

Your learning progress

NEW! Ready to keep learning? Pick up where you left off, or start a new path ... [VIEW ALL PATHS](#)

<p>My progress 1 of 29</p> <p>PRACTITIONER</p> <p>API testing</p> <p>View progress RESUME</p>	<p>My progress 6 of 51</p> <p>PRACTITIONER</p> <p>SQL Injection</p> <p>View progress RESUME</p>
--	--

Your level

Ne **NEWBIE** Solve 57 more labs to become an apprentice.

See where you rank

- [Check out our Hall of Fame](#)

Hall of Fame high flyers

- [Read three of our user journeys](#)

Find your next topic

- [View all topics](#)

Your certifications

NOT READY You're not ready to

Level progress

2 of 59 Apprentice	2 of 171 Practitioner	0 of 39 Expert
-----------------------	--------------------------	-------------------

Vulnerability labs

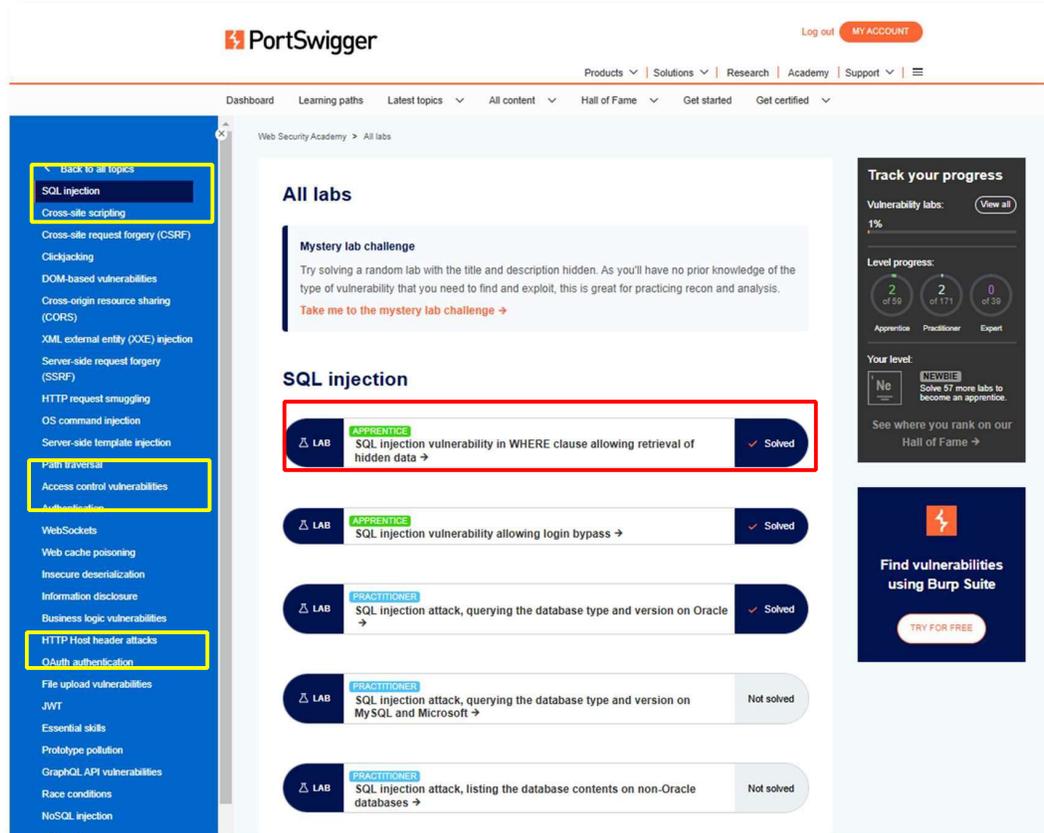
1% [VIEW ALL](#)

Exam preparation steps **NOT READY**

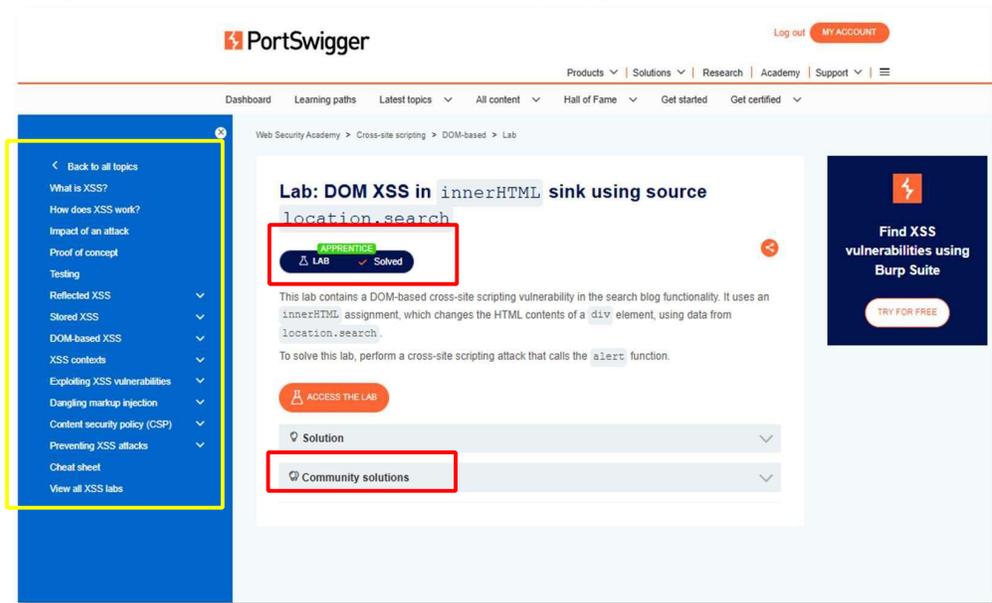
The labs you choose to complete must be "Practitioner" level or higher.

1 of 23	1 of 8	0 of 5	0 of 1
---------	--------	--------	--------

5. Find "Vulnerability labs" on your dashboard and click the "VIEW ALL" button.



6. All the labs are on the left side of the topic list. You're encouraged to practice with all of them. Each topic's labs have different difficulty levels, so you can start with the easiest.
7. You will find information about this lab and explanations of the key concepts in each lab. If you are stuck somewhere, don't panic! You can always find community support.



8. We pick up the following topics. Here are the required labs:

	Lab topics	
1	SQL injection	Top 2
2	Cross-site Scripting	Top 6
3	Cross-site request forgery (CSRF)	Top 1
4	Clickjacking	Top 3
5	HTTP request smuggling	Top 1
6	OS command injection	Top 1
7	Access Control Vulnerabilities	Top 5
8	Authentication	Top 3
9	File upload vulnerabilities	Top 2
10	Information Disclosure	Top 3 (optional)
11	OAuth Authentication	Top 1 (optional)
12	Web LLM attacks	Top 1 (optional)
	Total	29 labs

9. If you find these labs too easy, try more advanced blue-labeled "Practitioner" or purple-labeled "Expert" labs. Have fun! !

[3] Submission: Write a report summarizing the work you did for each lab topic. You are welcome to do more than what is required. In that case, please include a description of the work you completed. You are encouraged to suggest labs you find important or interesting. The instructor is seeking input for future classes. Please submit a short report (about one page), screenshots of your completed required lab topics, and your dashboard showing your progress bar. Save all your screenshots in a single file, convert it to a PDF, and upload it to Canvas. The upload instructions will be posted on the class website. The instructor may ask you to show your work on the website. Have fun!un!

[4] Deadline: 11:59 pm, Monday, April 27, 2026.

Your learning progress

The dashboard displays the following information:

- Ready to keep learning?** Pick up where you left off, or start a new path ... (VIEW ALL PATHS)
- API testing (Practitioner level):** 1 of 29 labs completed. View progress → RESUME →
- SQL injection (Practitioner level):** 6 of 51 labs completed. View progress → RESUME →
- Your level:** NEWBIE. Solve 52 more labs to become an apprentice. (Ne icon)
- Level progress:**
 - Apprentice: 7 of 59
 - Practitioner: 2 of 171
 - Expert: 0 of 39