

VULNERABILITY LABS

1. AUTHENTICATION
2. DOCUMENT OBJECT MODEL (DOM)
3. HTTP REQUEST SMUGGLING
4. CROSS – ORIGIN RESOURCE SHARING (CORS)
5. SQL INJECTION
6. CROSS – SITE SCRIPTING (XSS)
7. CROSS – SITE REQUEST FORGERY
8. SERVER – SIDE TEMPLATE INJECTION
9. COMMAND INJECTION
10. SERVER – SIDE REQUEST FORGERY (SSRF)

AUTHENTICATION

The screenshot shows the PortSwigger Web Security Academy interface. The top navigation bar includes the PortSwigger logo, a 'Log out' link, and a 'MY ACCOUNT' button. Below this is a secondary navigation bar with links for Products, Solutions, Research, Academy, and Support. The main content area is titled 'Web Security Academy > Authentication vulnerabilities > Password-based > Lab'. On the left, a blue sidebar lists various topics under 'Back to all topics', including 'What is authentication?', 'How vulnerabilities arise', 'Impact of vulnerable authentication', 'Vulnerabilities in password-based authentication', 'Vulnerabilities in multi-factor authentication', 'Vulnerabilities in other authentication mechanisms', 'Vulnerabilities in OAuth authentication', 'Securing your authentication mechanisms', and 'View all authentication labs'. The main content area displays the lab title 'Lab: Username enumeration via different responses' with a green 'APPRENTICE' badge and a 'LAB' icon. It states that the lab is vulnerable to username enumeration and password brute-force attacks. It lists two candidate lists: 'Candidate usernames' and 'Candidate passwords'. The instructions state: 'To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.' An 'ACCESS THE LAB' button is at the bottom.

DOCUMENT OBJECT MODEL (DOM)

The screenshot shows the PortSwigger Web Security Academy interface for a DOM-based lab. The top navigation bar is identical to the previous screenshot. The main content area is titled 'Web Security Academy > DOM-based > Open redirection > Lab'. The left sidebar lists topics under 'Back to all topics', including 'What is the DOM?', 'Taint flow', 'DOM-based XSS', 'Open redirection', 'Cookie manipulation', 'JavaScript injection', 'Document-domain manipulation', 'WebSocket-URL poisoning', 'Link manipulation', and 'Web message manipulation'. The main content area displays the lab title 'Lab: DOM-based open redirection' with a blue 'PRACTITIONER' badge and a 'LAB' icon. It states: 'This lab contains a DOM-based open-redirection vulnerability. To solve this lab, exploit this vulnerability and redirect the victim to the exploit server.' An 'ACCESS THE LAB' button is at the bottom. Below the button is a 'Solution' section with a dropdown arrow.

HTTP REQUEST SMUGGLING

The screenshot shows the PortSwigger Web Security Academy interface. The top navigation bar includes the PortSwigger logo, a 'Log out' link, and a 'MY ACCOUNT' button. Below this is a secondary navigation bar with links for Products, Solutions, Research, Academy, and Support. The main content area is titled 'Web Security Academy > Request smuggling > Lab'. On the left, a blue sidebar lists various topics, with 'What is HTTP request smuggling?' selected. The main content area displays the lab title 'Lab: HTTP request smuggling, basic CL.TE vulnerability' and a 'PRACTITIONER' badge. The lab description states: 'This lab involves a front-end and back-end server, and the front-end server doesn't support chunked encoding. The front-end server rejects requests that aren't using the GET or POST method. To solve the lab, smuggle a request to the back-end server, so that the next request processed by the back-end server appears to use the method `POST`.'

CROSS – ORIGIN RESOURCE SHARING (CORS)

The screenshot shows the PortSwigger Web Security Academy interface for a CORS lab. The top navigation bar includes the PortSwigger logo, a 'Log out' link, and a 'MY ACCOUNT' button. Below this is a secondary navigation bar with links for Products, Solutions, Research, Academy, and Support. The main content area is titled 'Web Security Academy > CORS > Lab'. On the left, a blue sidebar lists various topics, with 'What is CORS?' selected. The main content area displays the lab title 'Lab: CORS vulnerability with basic origin reflection' and an 'APPRENTICE' badge. The lab description states: 'This website has an insecure CORS configuration in that it trusts all origins. To solve the lab, craft some JavaScript that uses CORS to retrieve the administrator's API key and upload the code to your exploit server. The lab is solved when you successfully submit the administrator's API key. You can log in to your own account using the following credentials: `wiener:peter`'. An 'ACCESS THE LAB' button is visible at the bottom.

SQL INJECTION

Web Security Academy > SQL Injection > Lab

Back to all topics

What is SQL injection?

What is the impact of SQL injection?

Detecting SQL injection vulnerabilities

Examples of SQL injection

Examining the database

UNION attacks

Blind SQL injection

How to prevent SQL injection

SQL injection cheat sheet

View all SQL injection labs

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

APPRENTICE LAB 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

CROSS – SITE SCRIPTING (XSS)

PortSwigger

Log out MY ACCOUNT

Products Solutions Research Academy Support

Dashboard Learning paths Latest topics All content Hall of Fame Get started Get certified

Web Security Academy > Cross-site scripting > Reflected > Lab

Back to all topics

What is XSS?

How does XSS work?

Impact of an attack

Proof of concept

Testing

Reflected XSS

Stored XSS

DOM-based XSS

XSS contexts

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

CROSS – SITE REQUEST FORGERY

The screenshot shows the Web Security Academy interface. At the top, there is a navigation bar with links: Dashboard, Learning paths, Latest topics, All content, Hall of Fame, Get started, and Get certified. On the left, a blue sidebar contains a list of topics under 'What is CSRF?', 'Impact', 'How does CSRF work?', 'XSS vs CSRF', 'Constructing an attack', 'Delivering an exploit', and 'Defences'. The main content area is titled 'Lab: CSRF vulnerability with no defenses' and is labeled 'APPRENTICE' and 'LAB'. It states that the lab's email change functionality is vulnerable to CSRF and provides instructions on how to solve it by crafting an HTML payload. A hint box shows the credentials 'wiener:peter'. An 'ACCESS THE LAB' button is at the bottom.

SERVER – SIDE TEMPLATE INJECTION

The screenshot shows the PortSwigger Web Security Academy interface. At the top, there is a navigation bar with links: Products, Solutions, Research, Academy, and Support. On the left, a blue sidebar contains a list of topics under 'What is server-side template injection?', 'Impact of server-side template injection', 'How vulnerabilities arise', 'Constructing an attack', and 'Preventing vulnerabilities'. The main content area is titled 'Lab: Basic server-side template injection' and is labeled 'PRACTITIONER' and 'LAB'. It states that the lab is vulnerable to server-side template injection due to the unsafe construction of an ERB template and provides instructions on how to solve it by deleting the 'morale.txt' file. An 'ACCESS THE LAB' button is at the bottom.

COMMAND INJECTION

The screenshot shows the PortSwigger Web Security Academy interface. At the top, there's a navigation bar with the PortSwigger logo, 'Log out', and 'MY ACCOUNT'. Below this is a secondary navigation bar with links like 'Dashboard', 'Learning paths', 'Latest topics', 'All content', 'Hall of Fame', 'Get started', and 'Get certified'. The main content area is titled 'Web Security Academy > OS command injection > Lab'. On the left, a blue sidebar contains a list of topics: 'Back to all topics', 'What is command injection?', 'Injecting OS commands', 'Blind command injection vulnerabilities', 'Preventing', and 'View all OS command injection labs'. The main lab content is titled 'Lab: OS command injection, simple case' and is marked as 'APPRENTICE' and 'Solved'. It describes a vulnerability in a product stock checker where a shell command is executed. To solve the lab, the user is instructed to execute the 'whoami' command to determine the current user. An 'ACCESS THE LAB' button is at the bottom.

SERVER – SIDE REQUEST FORGERY (SSRF)

The screenshot shows the PortSwigger Web Security Academy interface for the 'Lab: Basic SSRF against the local server'. The layout is similar to the previous one, with the same top navigation bar and secondary navigation bar. The main content area is titled 'Web Security Academy > SSRF > Lab'. The left sidebar lists topics: 'Back to all topics', 'What is SSRF?', 'Impact', 'Common SSRF attacks', 'Circumventing common SSRF defenses', 'Blind SSRF vulnerabilities', 'Finding hidden attack surface for SSRF', 'URL validation bypass cheat sheet', and 'View all SSRF labs'. The main lab content is titled 'Lab: Basic SSRF against the local server' and is marked as 'APPRENTICE' and 'Solved'. It describes a stock check feature that fetches data from an internal system. To solve the lab, the user is instructed to change the stock check URL to 'http://localhost/admin' and delete the user 'carlos'. An 'ACCESS THE LAB' button is at the bottom.