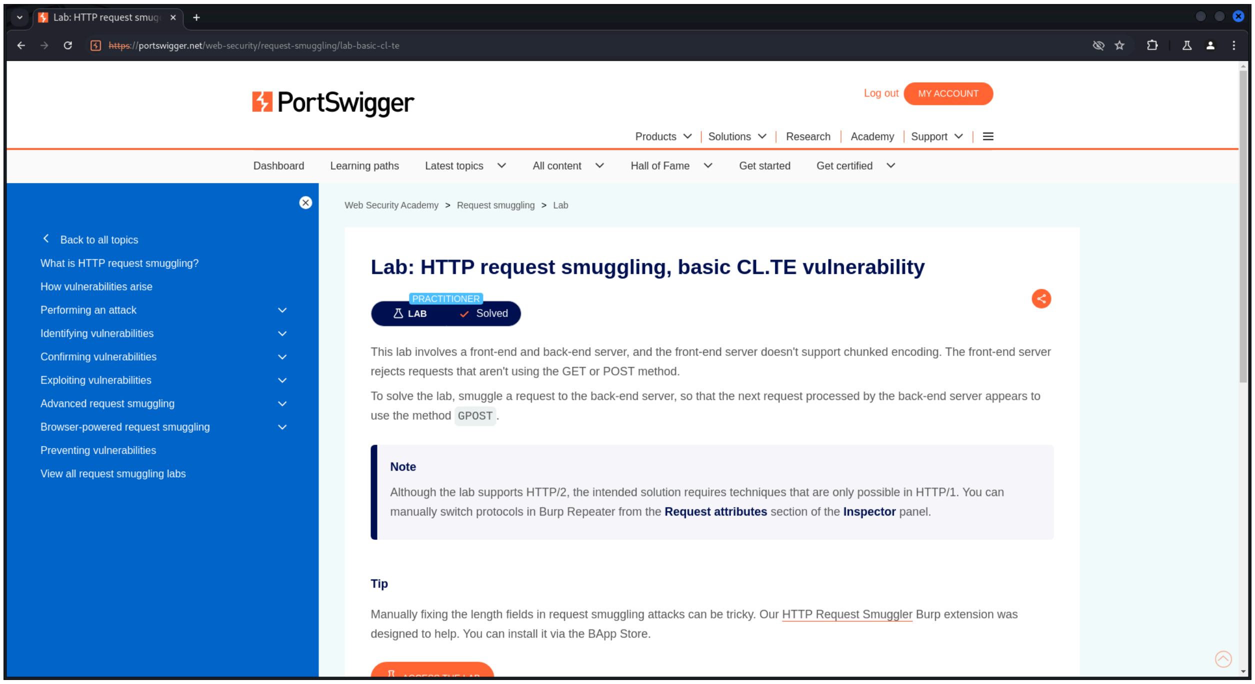
PortSwigger web academy Labs

Akshay C

HTTP request smuggling


Lab: HTTP request smug
https://portswigger.net/web-security/request-smuggling/lab-basic-cl-te
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What is HTTP request smuggling?
How vulnerabilities arise
Performing an attack
Identifying vulnerabilities
Confirming vulnerabilities
Exploiting vulnerabilities
Advanced request smuggling
Browser-powered request smuggling
Preventing vulnerabilities
View all request smuggling labs
Web Security Academy > Request smuggling > Lab
PRACTITIONER
LAB
✓ Solved

Lab: HTTP request smuggling, basic CL.TE vulnerability

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.

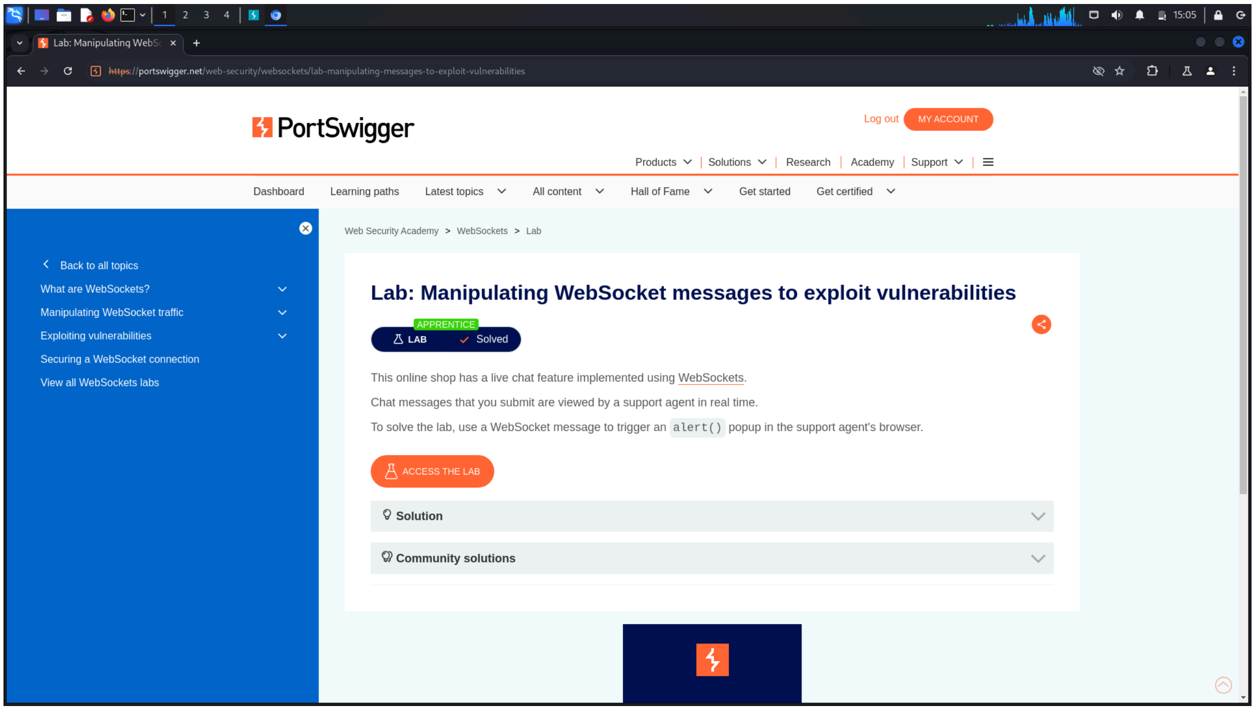
To solve the lab, smuggle a request to the back-end server, so that the next request processed by the back-end server appears to use the method `GPOST`.

> **Note**
>
> Although the lab supports HTTP/2, the intended solution requires techniques that are only possible in HTTP/1. You can manually switch protocols in Burp Repeater from the **Request attributes** section of the **Inspector** panel.

Tip

Manually fixing the length fields in request smuggling attacks can be tricky. Our HTTP Request Smuggler Burp extension was designed to help. You can install it via the BApp Store.

WebSockets



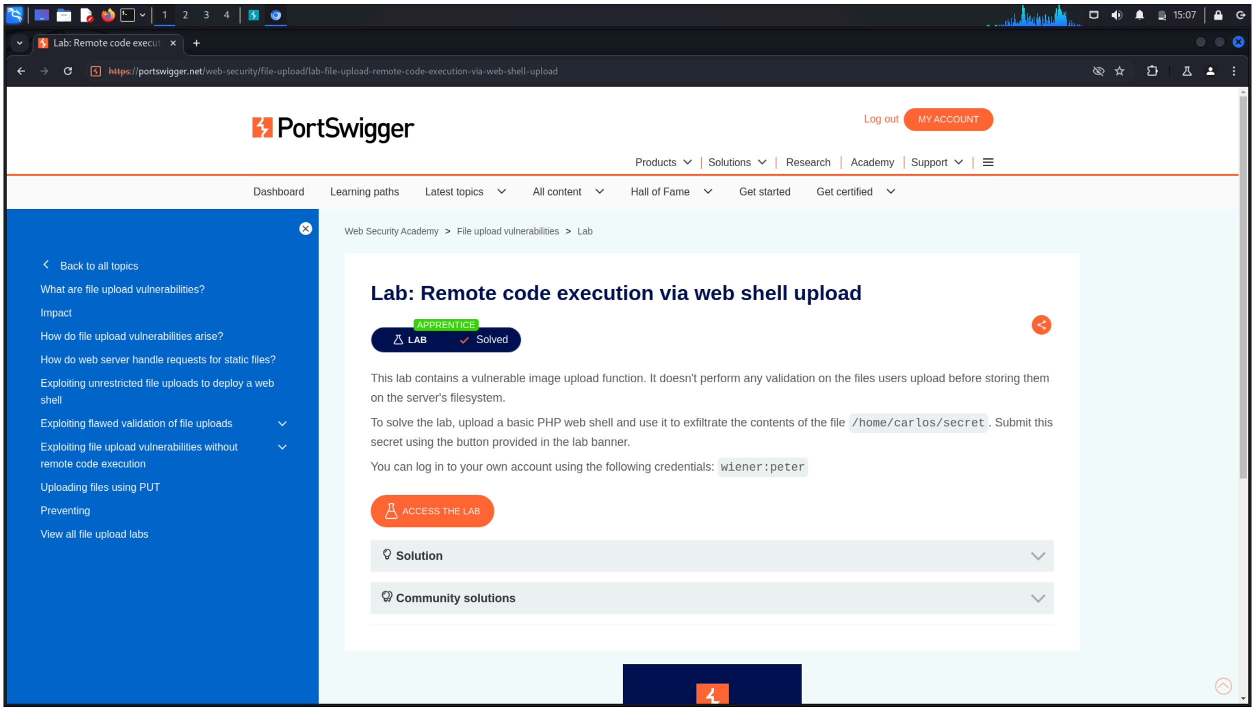
Lab: Manipulating WebSocket messages to exploit vulnerabilities

This online shop has a live chat feature implemented using WebSockets.

Chat messages that you submit are viewed by a support agent in real time.

To solve the lab, use a WebSocket message to trigger an `alert()` popup in the support agent's browser.

File upload vulnerabilities


Lab: Remote code execu
https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload
15:07
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What are file upload vulnerabilities?
Impact
How do file upload vulnerabilities arise?
How do web server handle requests for static files?
Exploiting unrestricted file uploads to deploy a web shell
Exploiting flawed validation of file uploads
Exploiting file upload vulnerabilities without remote code execution
Uploading files using PUT
Preventing
View all file upload labs
Web Security Academy > File upload vulnerabilities > Lab
APPRENTICE
LAB
✓ Solved
ACCESS THE LAB
Solution
Community solutions

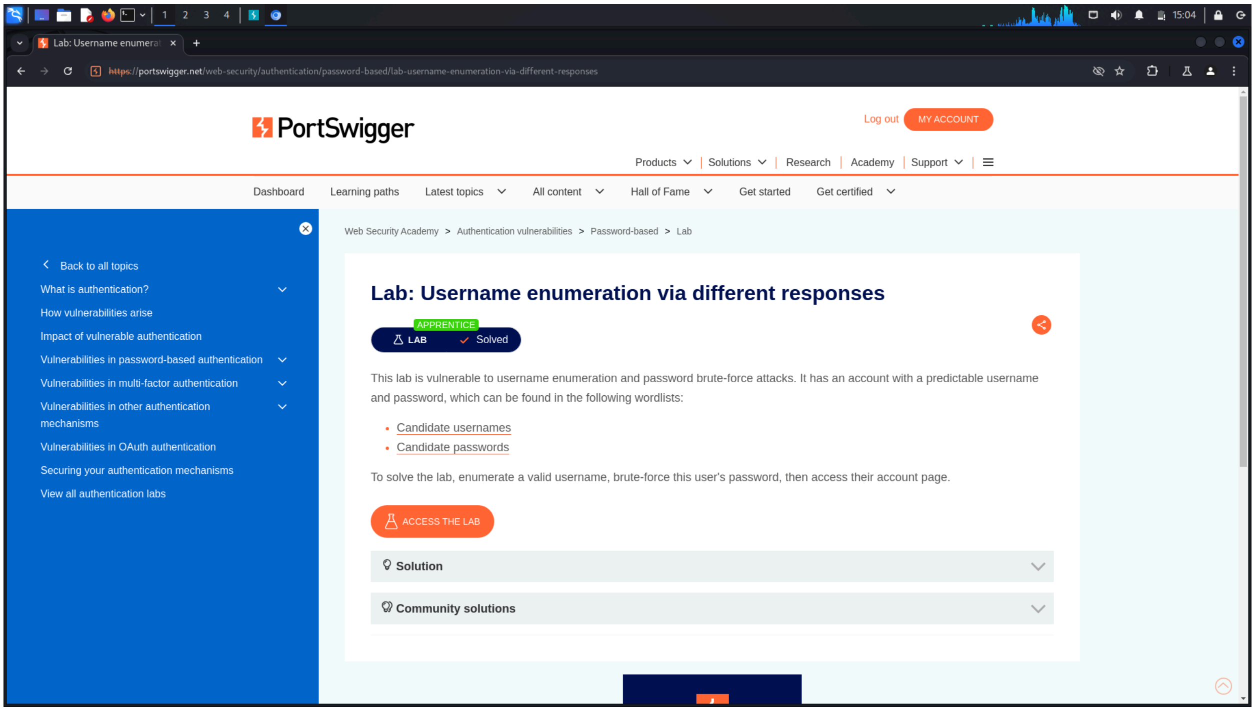
Lab: Remote code execution via web shell upload

This lab contains a vulnerable image upload function. It doesn't perform any validation on the files users upload before storing them on the server's filesystem.

To solve the lab, upload a basic PHP web shell and use it to exfiltrate the contents of the file `/home/carlos/secret`. Submit this secret using the button provided in the lab banner.

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

Authentication vulnerabilites


Lab: Username enumera
https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses
15:04
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
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
View all authentication labs
Web Security Academy > Authentication vulnerabilities > Password-based > Lab
APPRENTICE
LAB
✓ Solved
ACCESS THE LAB
Solution
Community solutions

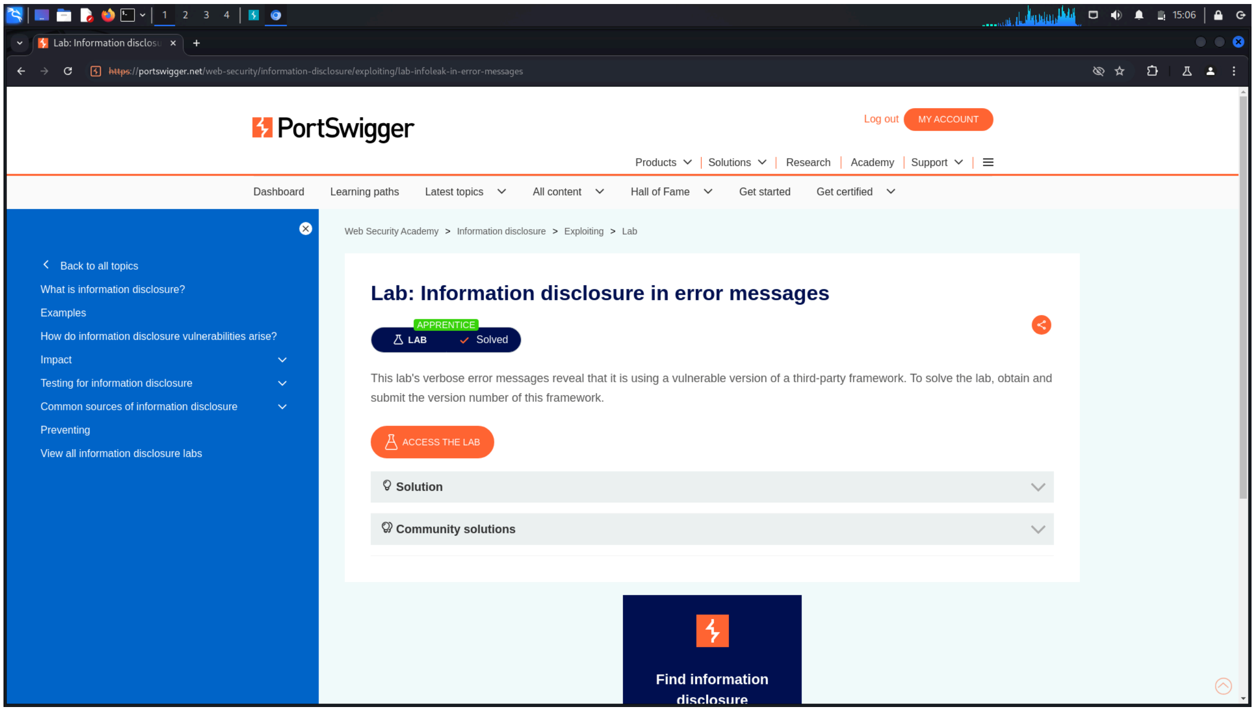
Lab: Username enumeration via different responses

This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- Candidate usernames
- Candidate passwords

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

Information disclosure

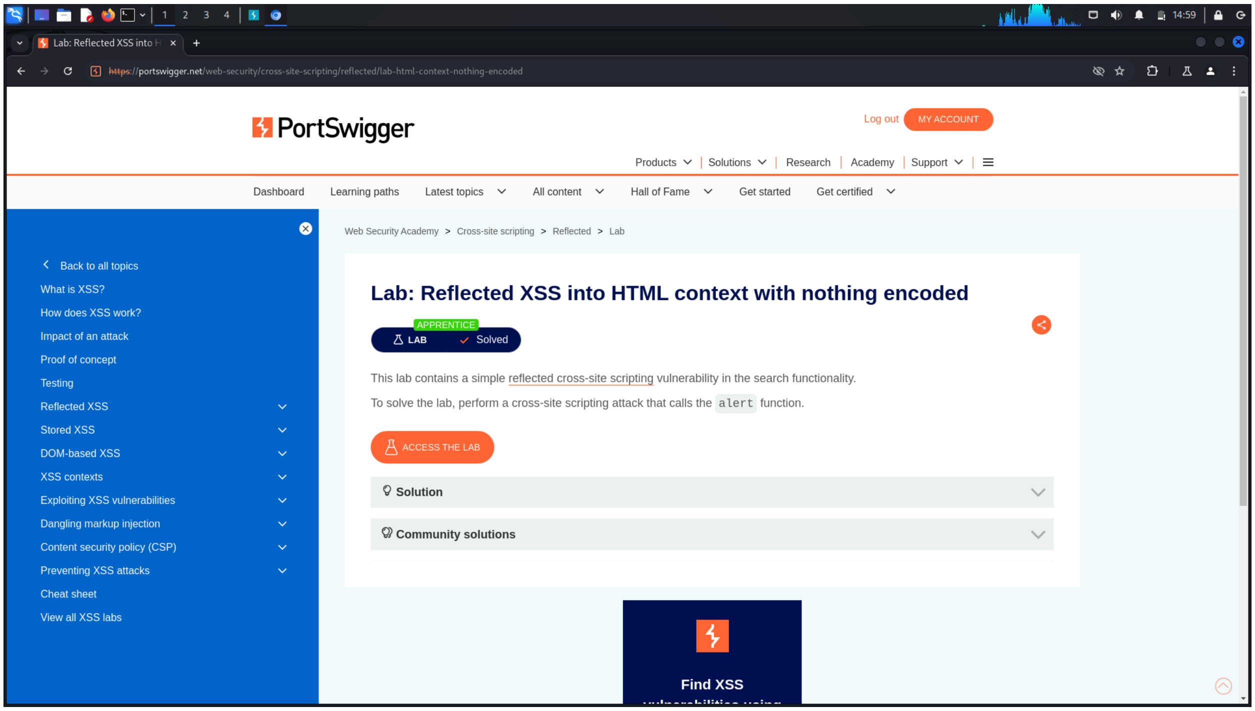

Lab: Information disclosu
https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-error-messages
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What is information disclosure?
Examples
How do information disclosure vulnerabilities arise?
Impact
Testing for information disclosure
Common sources of information disclosure
Preventing
View all information disclosure labs
Web Security Academy > Information disclosure > Exploiting > Lab

Lab: Information disclosure in error messages

This lab's verbose error messages reveal that it is using a vulnerable version of a third-party framework. To solve the lab, obtain and submit the version number of this framework.

ACCESS THE LAB
Solution
Community solutions
Find information
disclosure
15:06

Cross-site scripting(XSS)

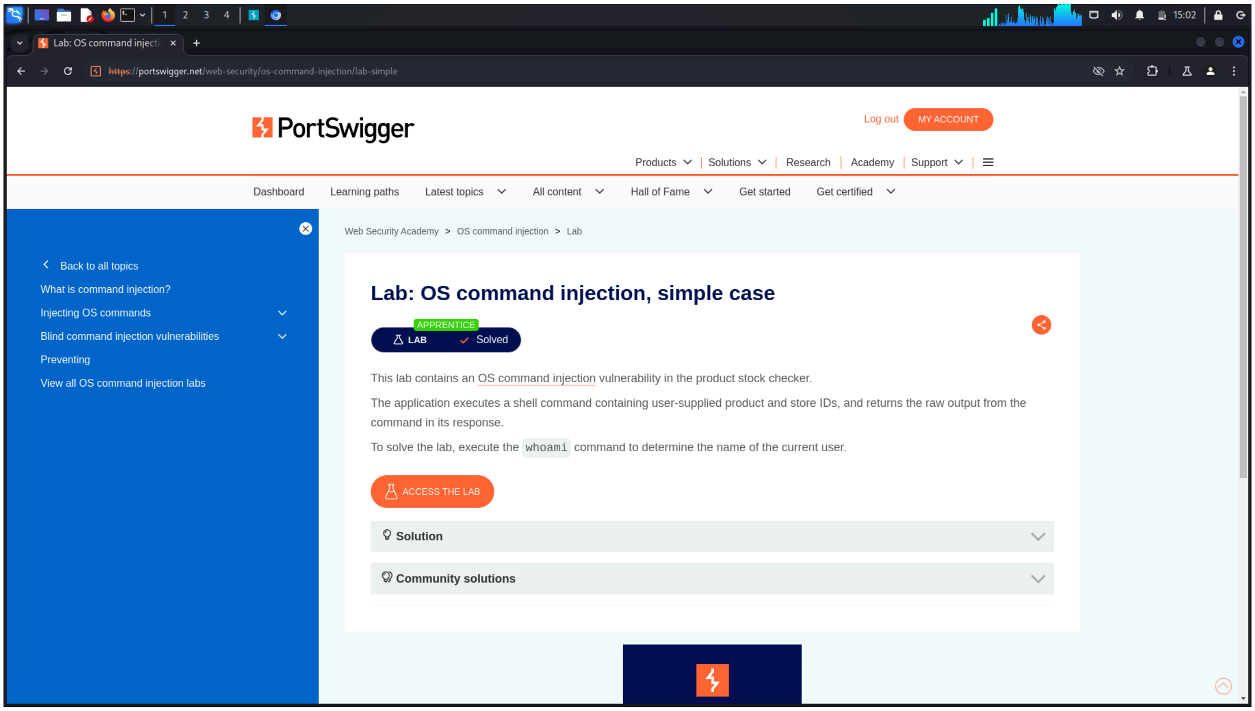


Lab: Reflected XSS into HTML context with nothing encoded

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.

OS command injection



Lab: OS command injection, simple case

APPRENTICE LAB ✓ Solved

This lab contains an OS command injection vulnerability in the product stock checker.

The application executes a shell command containing user-supplied product and store IDs, and returns the raw output from the command in its response.

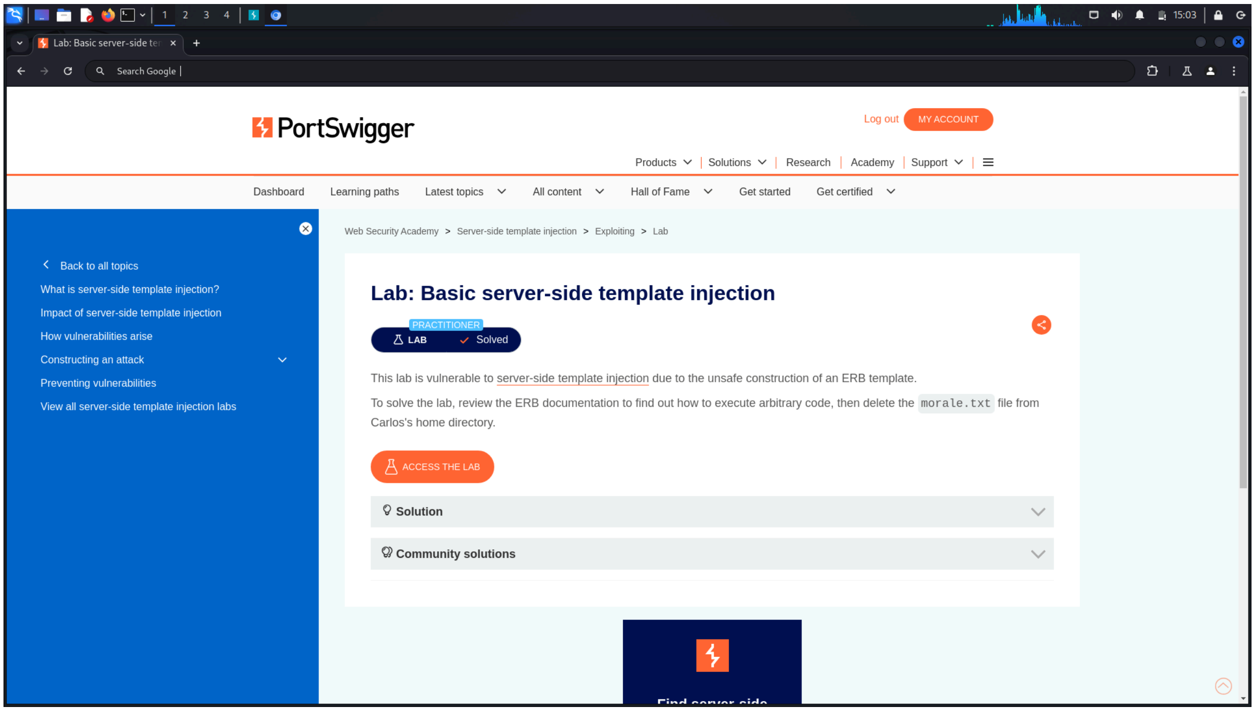
To solve the lab, execute the `whoami` command to determine the name of the current user.

ACCESS THE LAB

Solution

Community solutions

Server-side template injection


Lab: Basic server-side te
Search Google
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What is server-side template injection?
Impact of server-side template injection
How vulnerabilities arise
Constructing an attack
Preventing vulnerabilities
View all server-side template injection labs
Web Security Academy > Server-side template injection > Exploiting > Lab

Lab: Basic server-side template injection

PRACTITIONER LAB ✓ Solved

This lab is vulnerable to server-side template injection due to the unsafe construction of an ERB template.

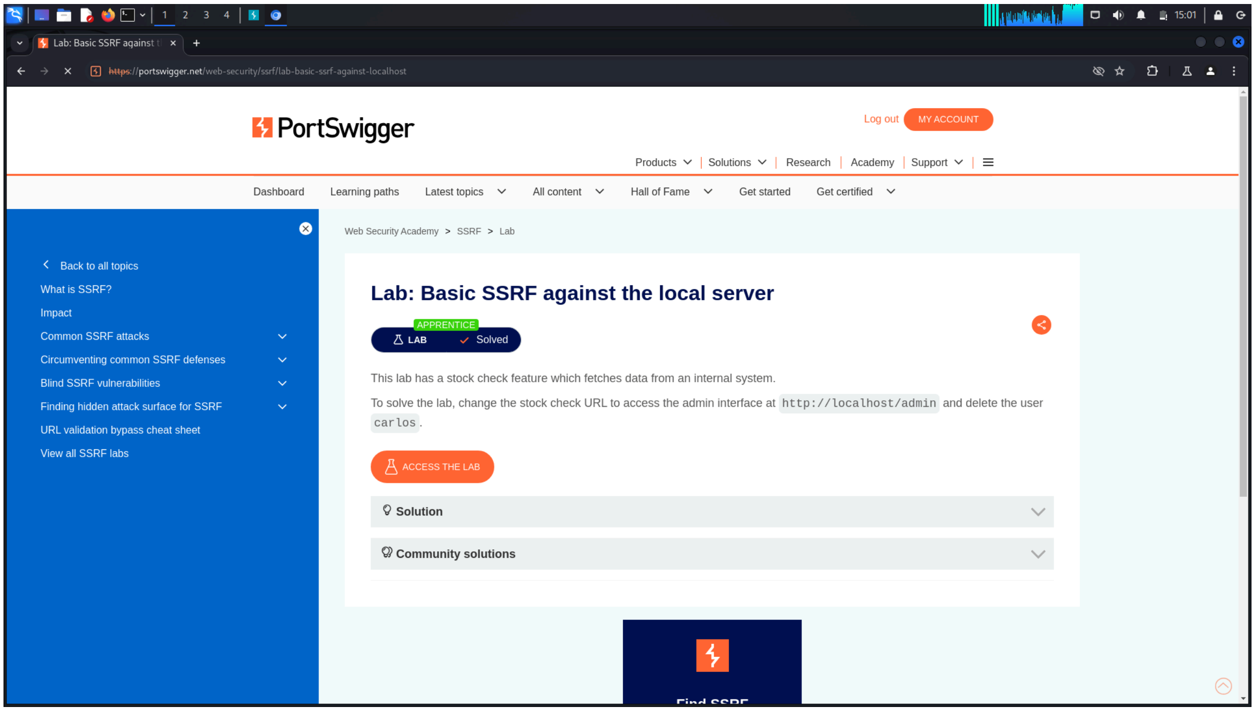
To solve the lab, review the ERB documentation to find out how to execute arbitrary code, then delete the `morale.txt` file from Carlos's home directory.

ACCESS THE LAB

Solution

Community solutions

Server-side request forgery(SSRF)

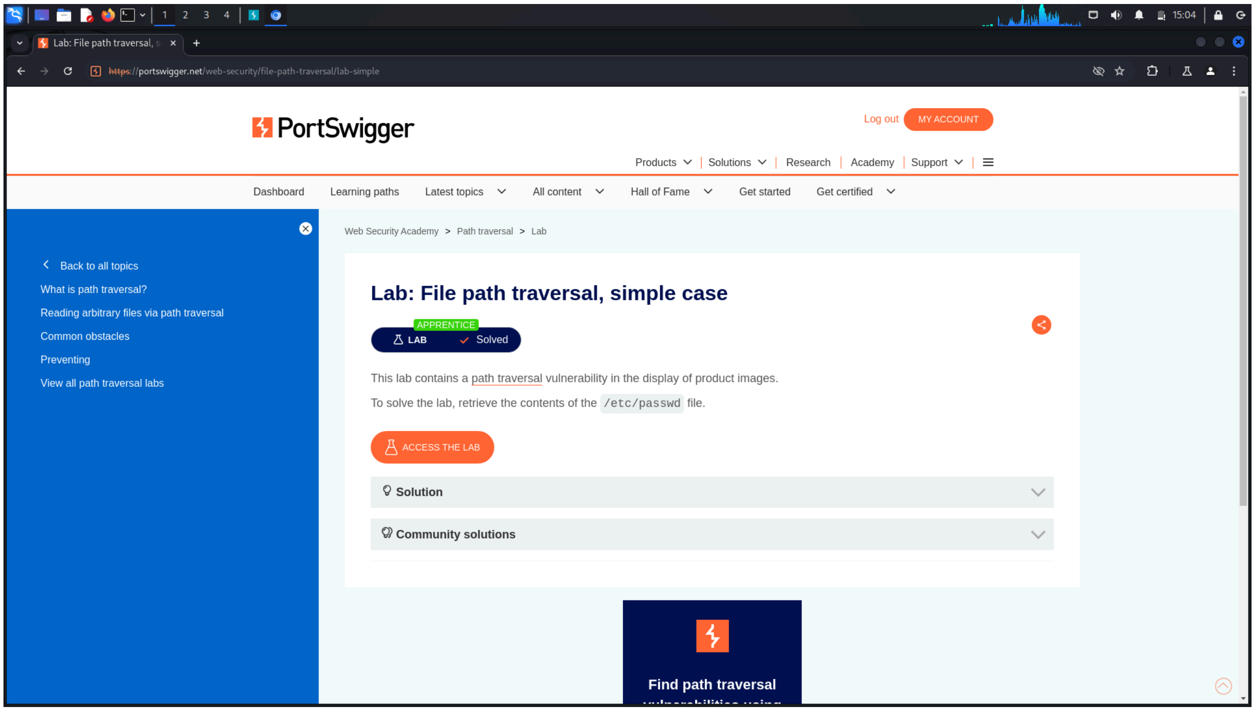


Lab: Basic SSRF against the local server

This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user `carlos`.

Path traversal



Lab: File path traversal, simple case

This lab contains a path traversal vulnerability in the display of product images.

To solve the lab, retrieve the contents of the `/etc/passwd` file.