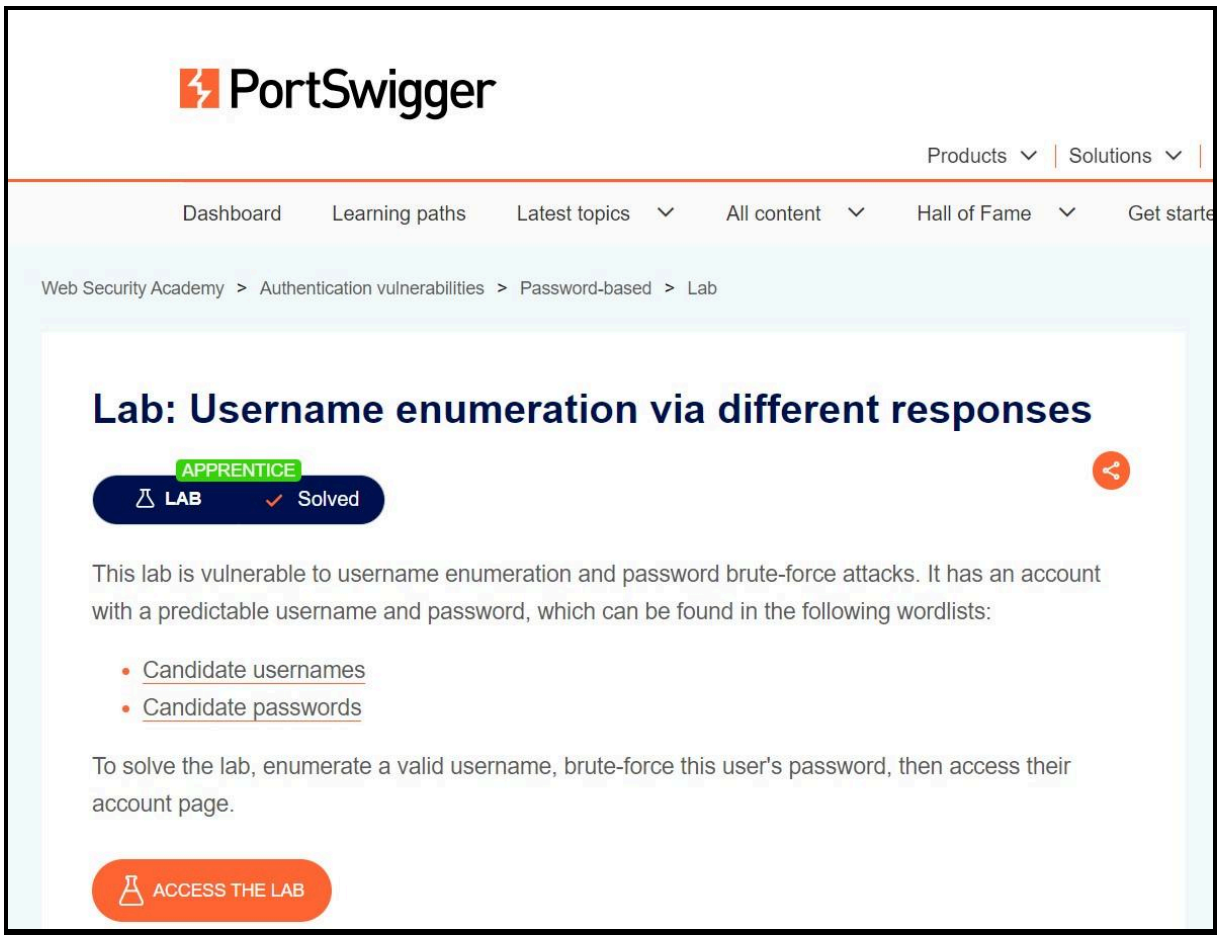
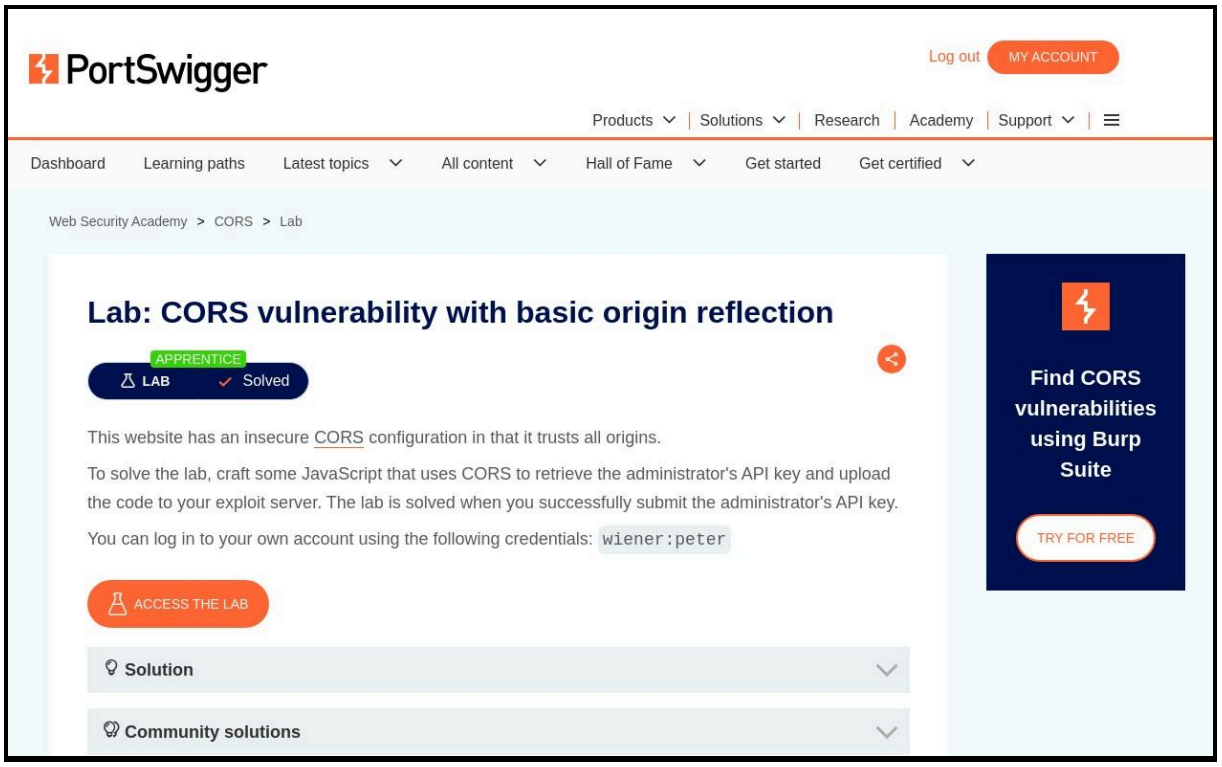
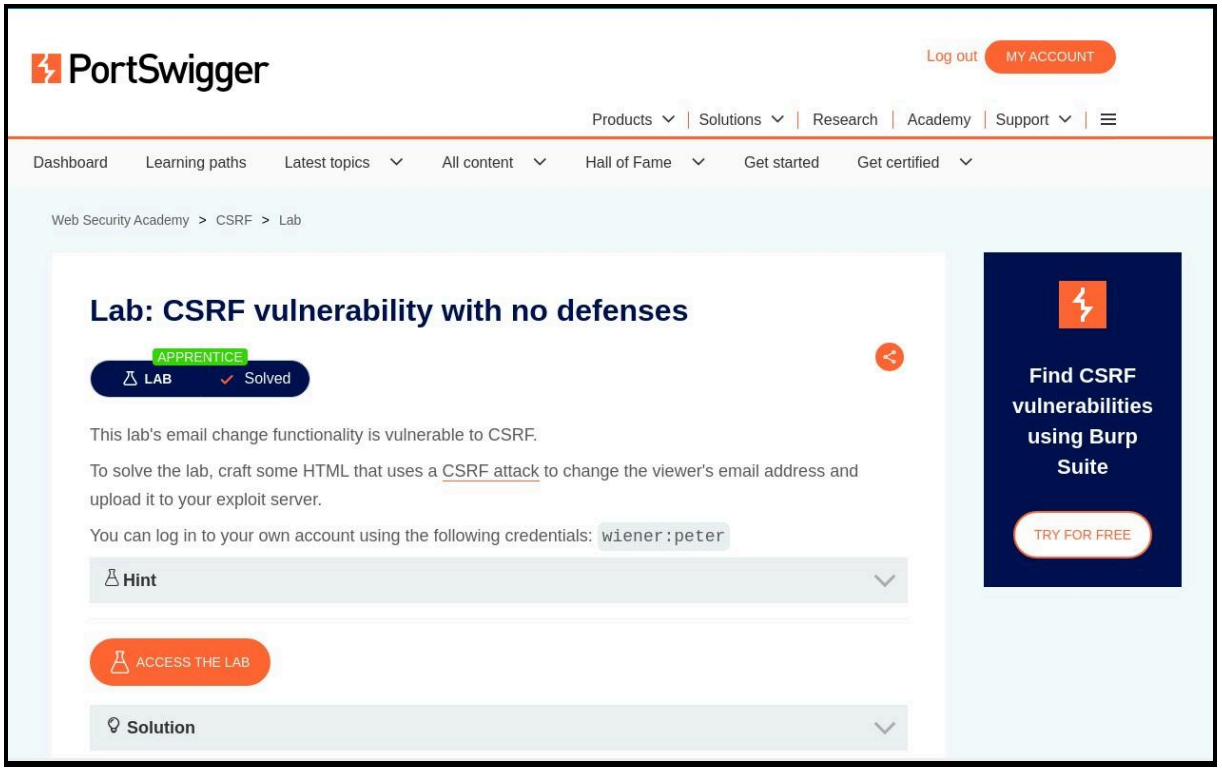
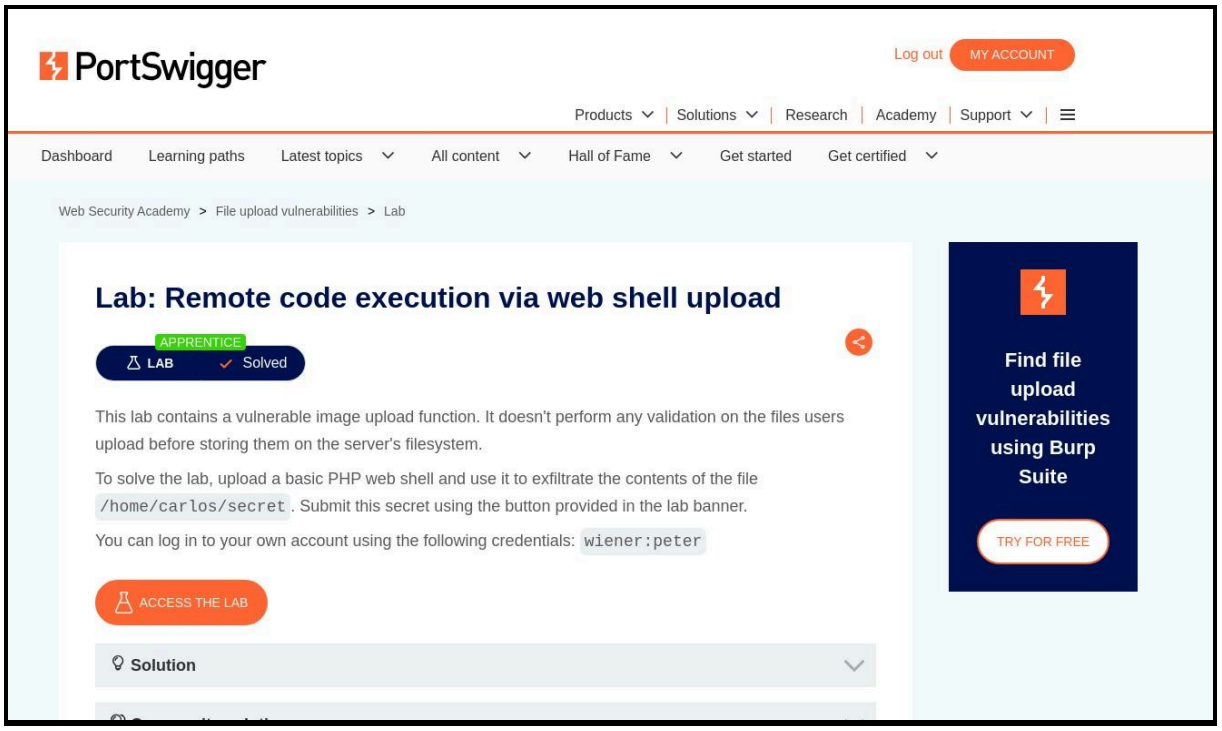
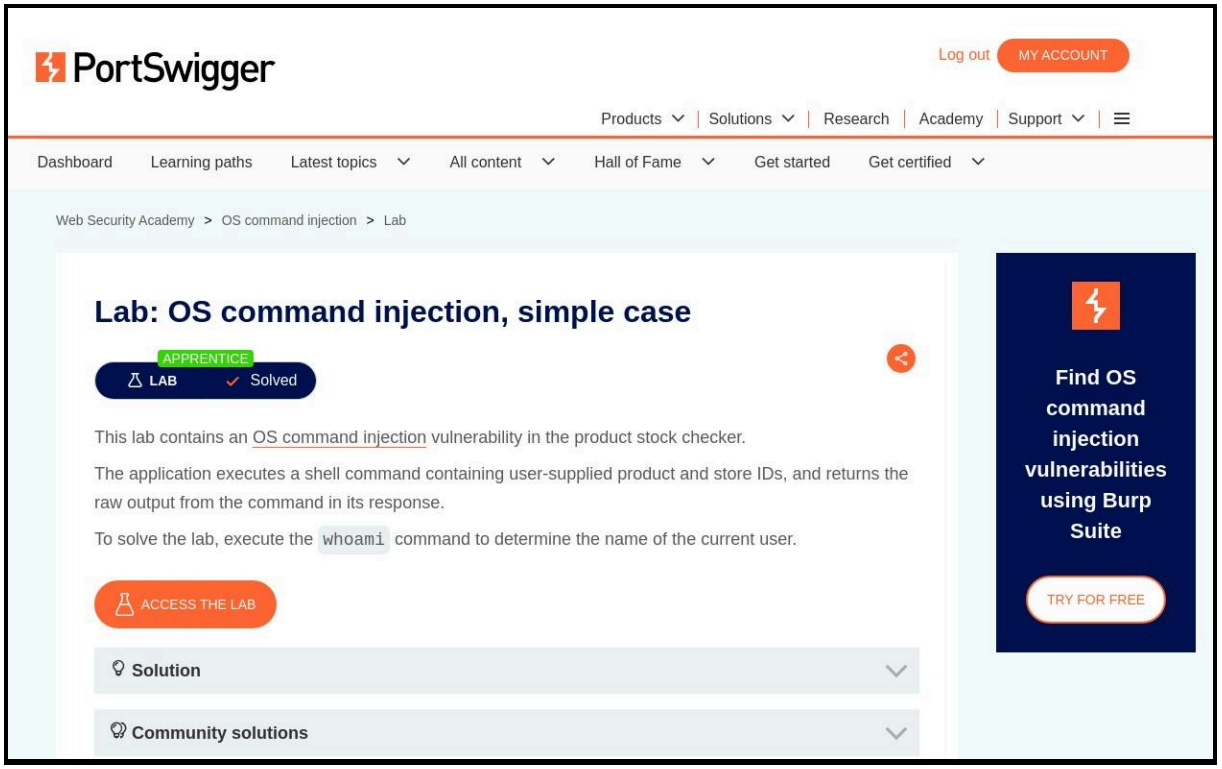
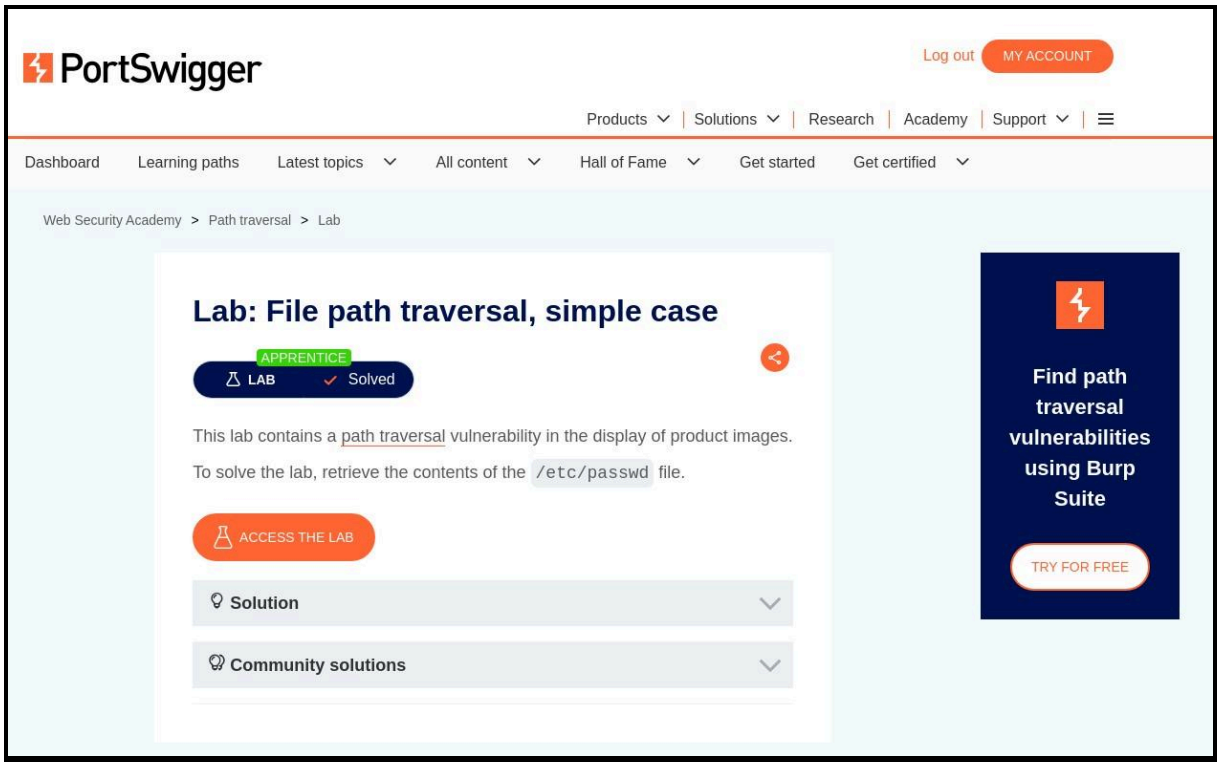

PortSwigger
Products
Solutions
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get starte
Web Security Academy > Authentication vulnerabilities > Password-based > Lab
Lab: Username enumeration via different responses
APPRENTICE
LAB
Solved
This lab is vulnerable to username enumeration 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.
ACCESS THE LAB

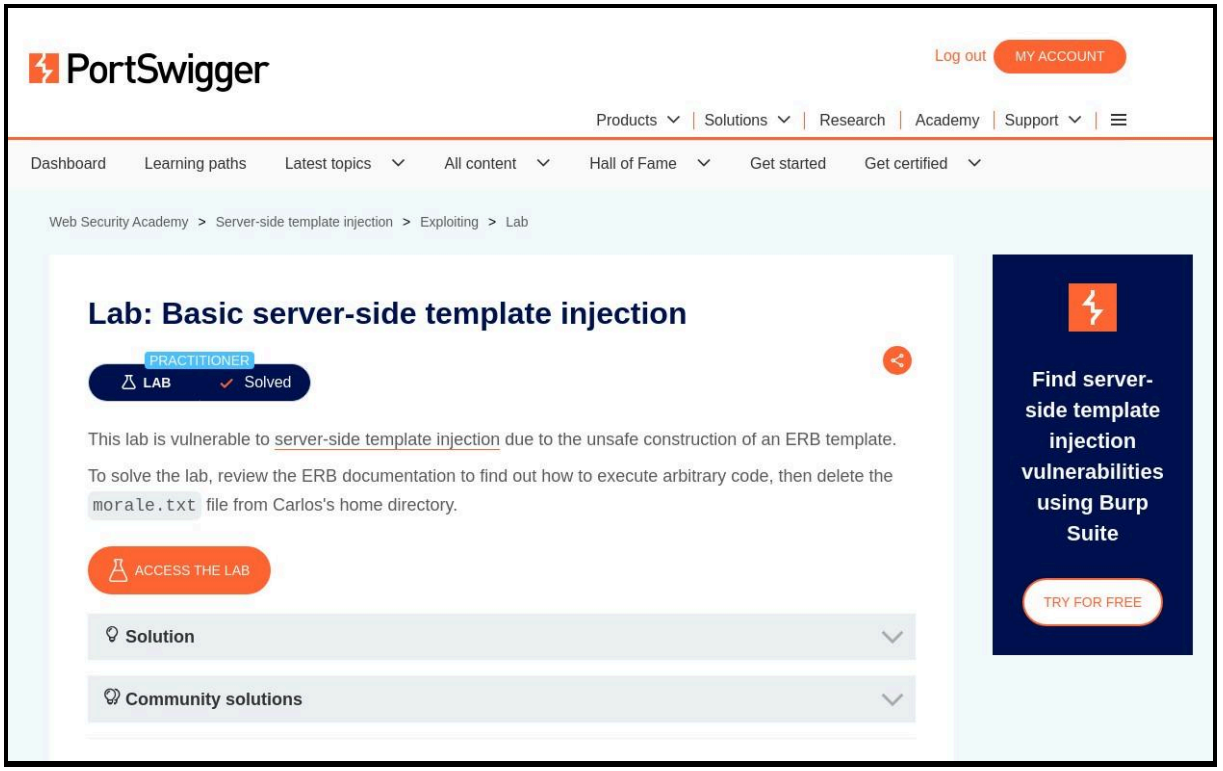

PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Web Security Academy > CORS > Lab
Lab: CORS vulnerability with basic origin reflection
APPRENTICE
LAB
Solved
This website has an insecure 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
ACCESS THE LAB
Solution
Community solutions
Find CORS vulnerabilities using Burp Suite
TRY FOR FREE

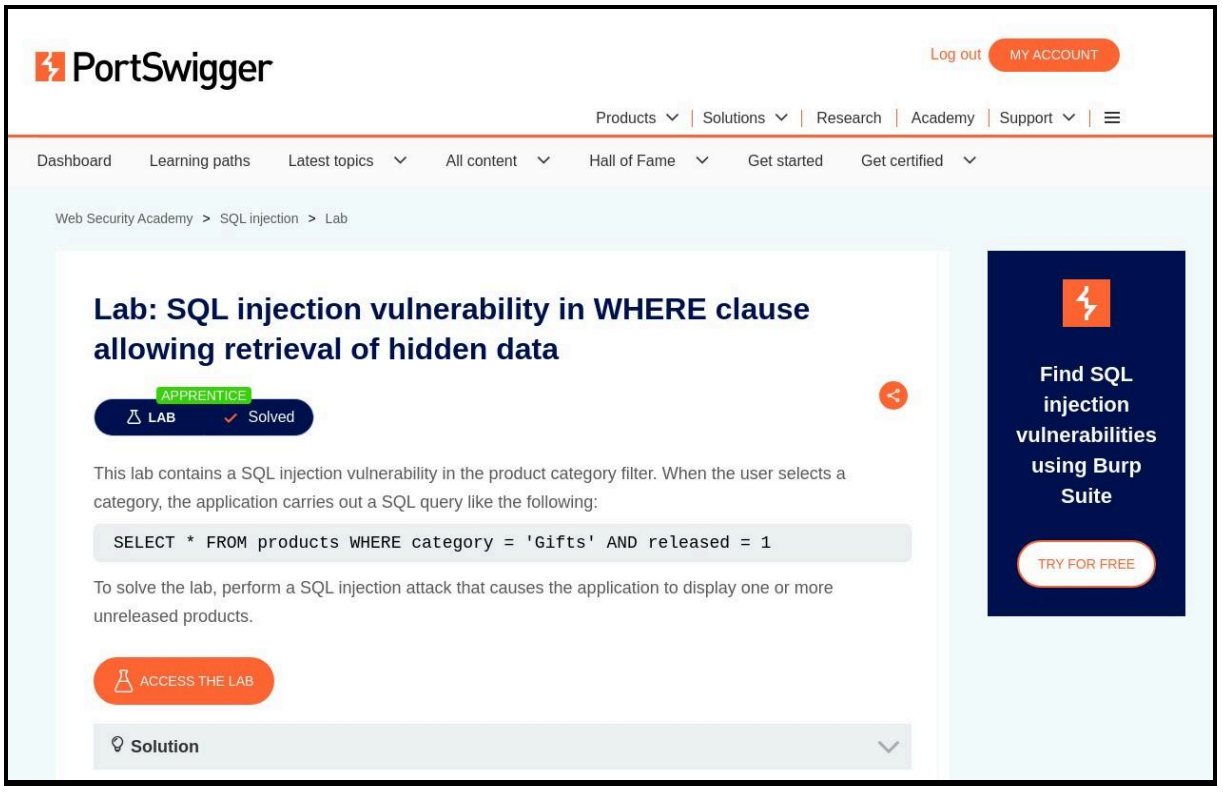

PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Web Security Academy > CSRF > Lab
Lab: CSRF vulnerability with no defenses
APPRENTICE
LAB
Solved
This lab's email change functionality is vulnerable to CSRF.
To solve the lab, craft some HTML that uses a CSRF attack to change the viewer's email address and upload it to your exploit server.
You can log in to your own account using the following credentials: wiener:peter
Hint
ACCESS THE LAB
Solution
Find CSRF vulnerabilities using Burp Suite
TRY FOR FREE

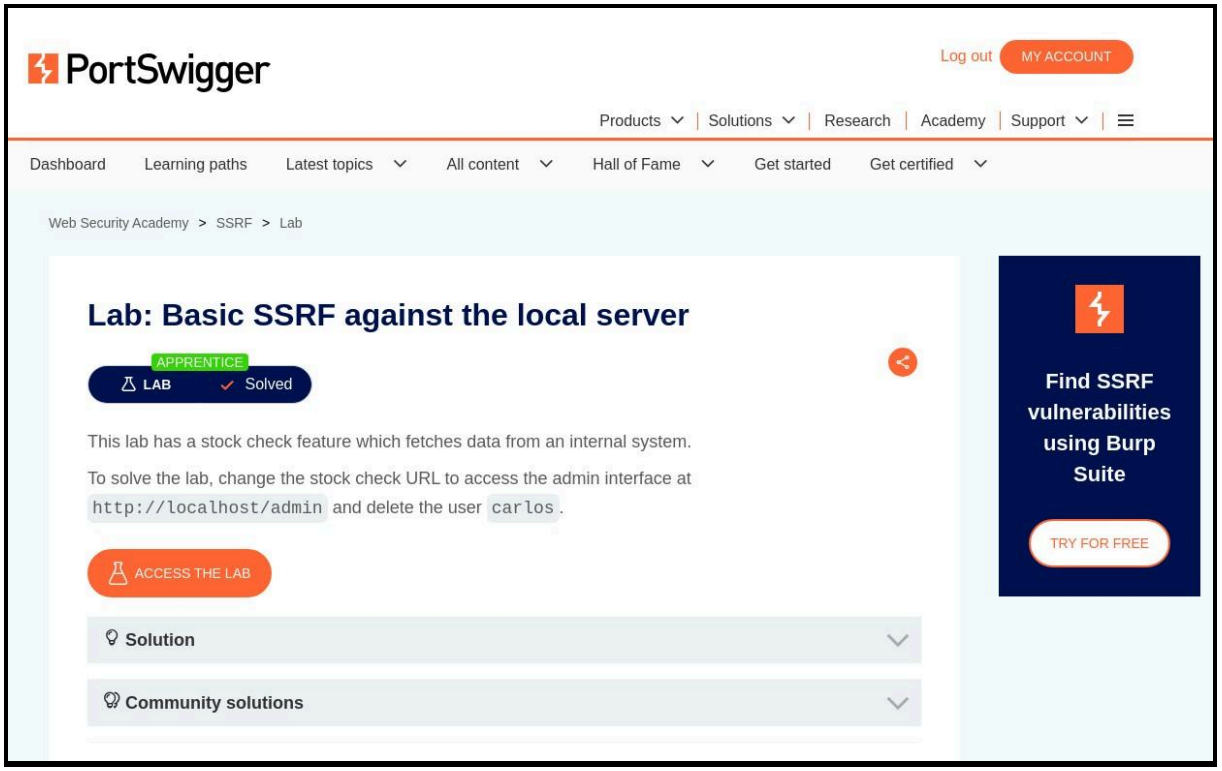

PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Web Security Academy > File upload vulnerabilities > Lab
Lab: Remote code execution via web shell upload
APPRENTICE
LAB
Solved
This lab 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
ACCESS THE LAB
Solution
Find file upload vulnerabilities using Burp Suite
TRY FOR FREE

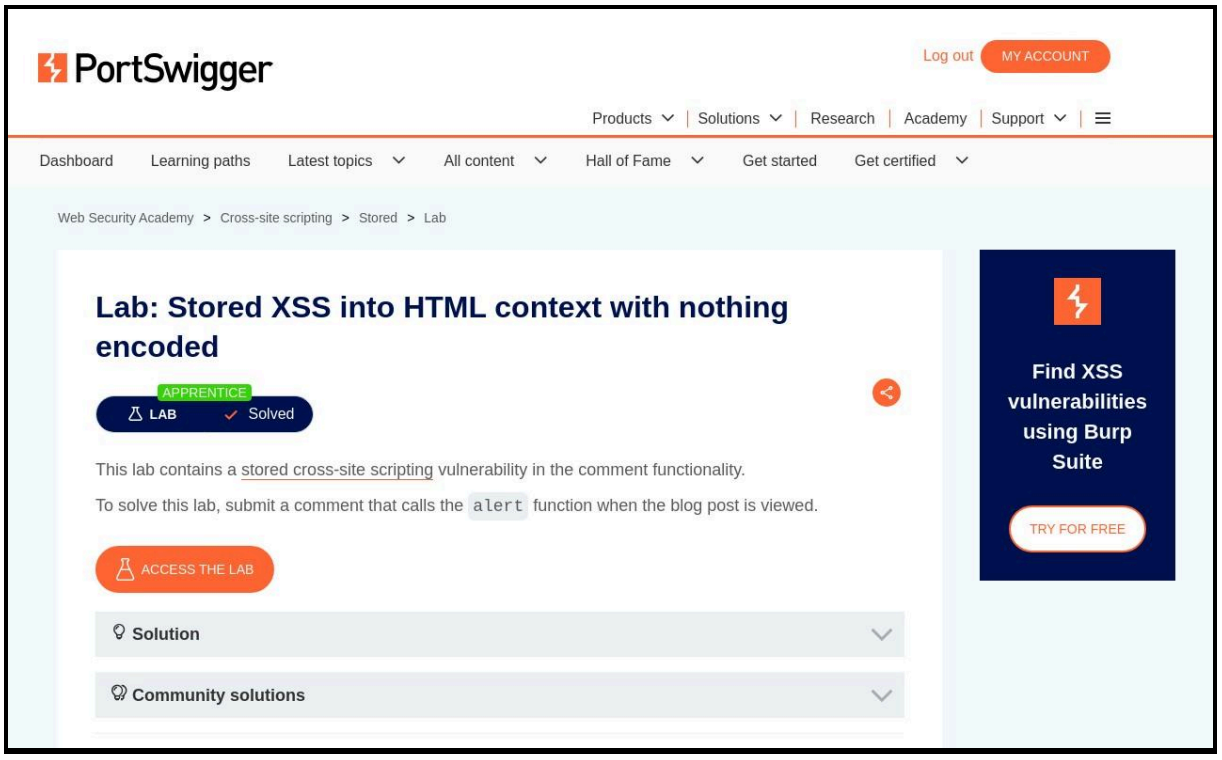

PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Support
Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Web Security Academy > OS command injection > Lab
Lab: OS command injection, simple case
APPRENTICE
LAB
Solved
This lab contains an OS command 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
Find OS command injection vulnerabilities using Burp Suite
TRY FOR FREE


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 > Path traversal > Lab
Lab: File path traversal, simple case
APPRENTICE
LAB
Solved
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.
ACCESS THE LAB
Solution
Community solutions
Find path traversal vulnerabilities using Burp Suite
TRY FOR FREE


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 > 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
Find server-side template injection vulnerabilities using Burp Suite
TRY FOR FREE


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 > SQL injection > Lab
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
Find SQL injection vulnerabilities using Burp Suite
TRY FOR FREE


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 > SSRF > Lab
Lab: Basic SSRF against the local server
APPRENTICE
LAB
Solved
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.
ACCESS THE LAB
Solution
Community solutions
Find SSRF vulnerabilities using Burp Suite
TRY FOR FREE


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 > Stored > Lab
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
Find XSS vulnerabilities using Burp Suite
TRY FOR FREE