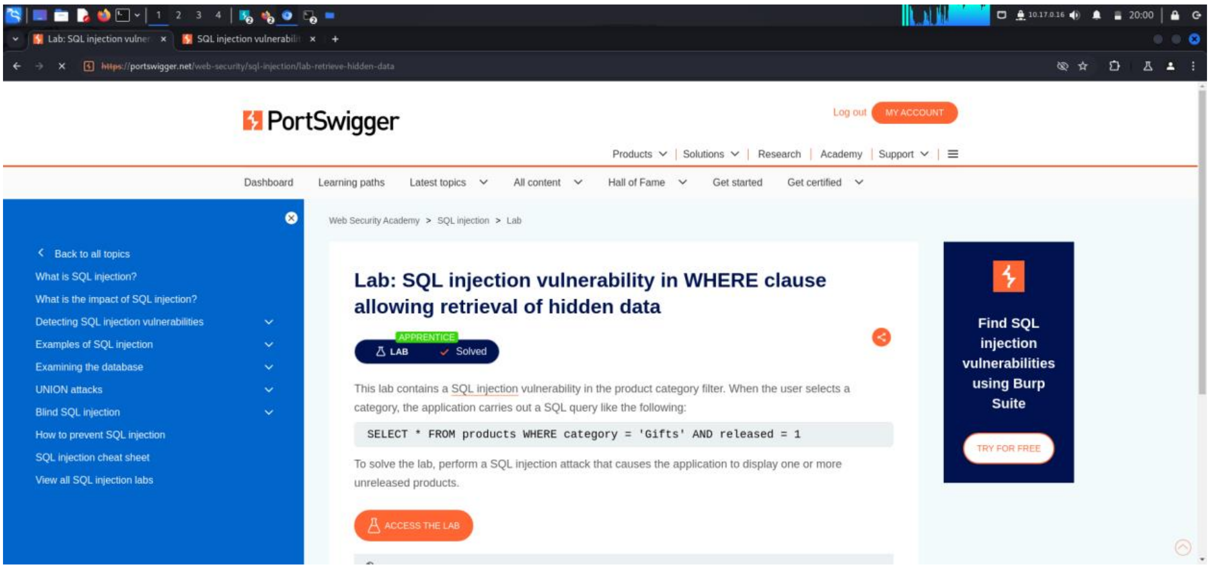
PORTSWIGGER LABS

SQL injection

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data


Lab: SQL injection vulner
SQL injection vulnerabili
https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data
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 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
Web Security Academy > SQL injection > Lab
APPRENTICE
LAB
Solved
ACCESS THE LAB
Find SQL injection vulnerabilities using Burp Suite
TRY FOR FREE

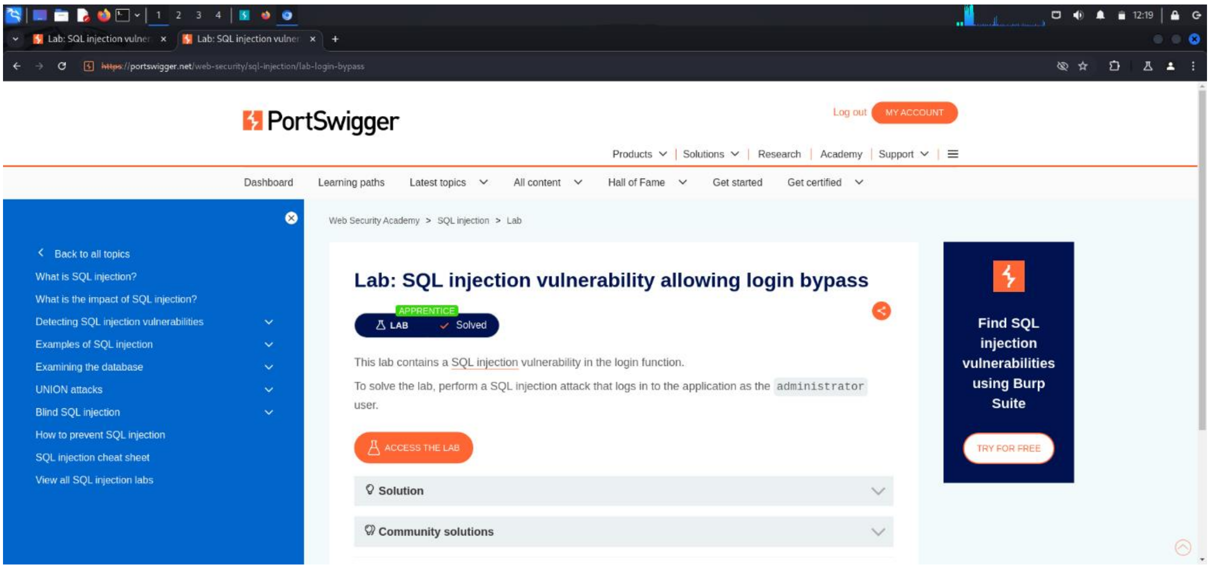
Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

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.

SQL injection vulnerability allowing login bypass


Lab: SQL injection vulner
Lab: SQL injection vulner
https://portswigger.net/web-security/sql-injection/lab-login-bypass
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 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
Web Security Academy > SQL injection > Lab
APPRENTICE
LAB
Solved
ACCESS THE LAB
Solution
Community solutions
Find SQL injection vulnerabilities using Burp Suite
TRY FOR FREE

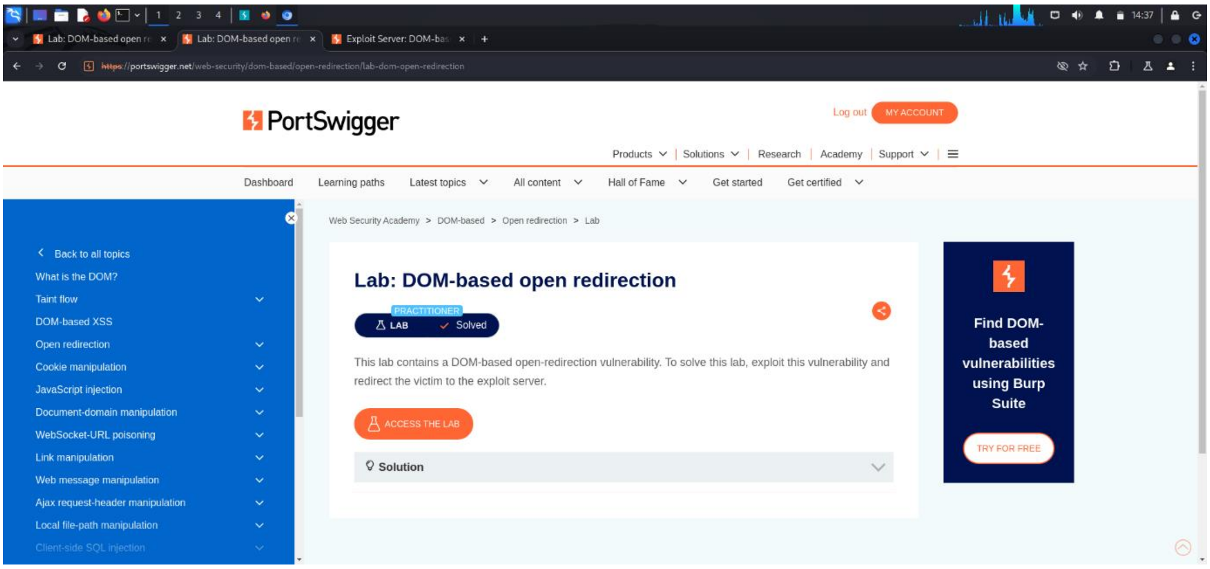
Lab: SQL injection vulnerability allowing login bypass

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.

DOM-based vulnerabilities

DOM-based open redirection

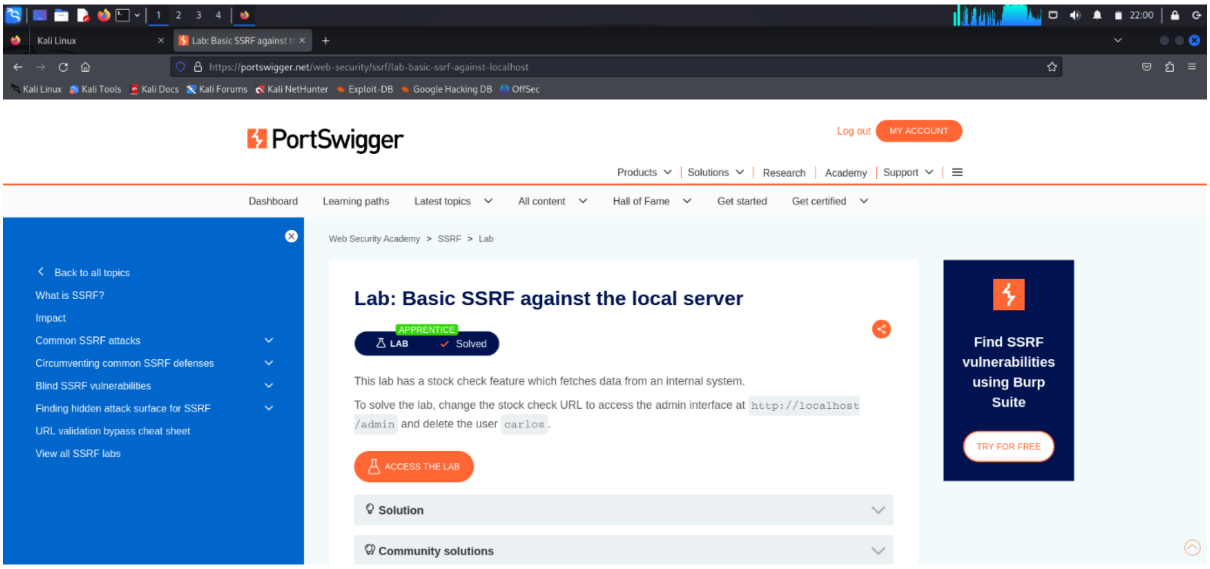


Lab: DOM-based open redirection

This lab contains a DOM-based open-redirection vulnerability. To solve this lab, exploit this vulnerability and redirect the victim to the exploit server.

Server-side request forgery (SSRF)

Basic SSRF against the local server



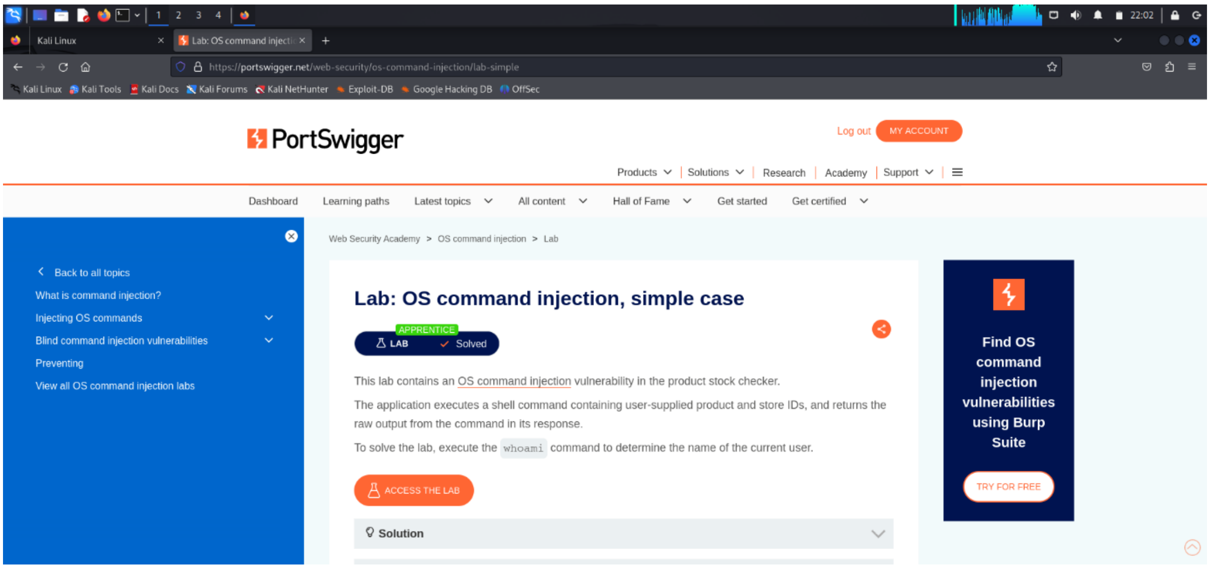
Lab: Basic SSRF against the local server

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`.

OS command injection

OS command injection, simple case



Lab: OS command injection, simple case

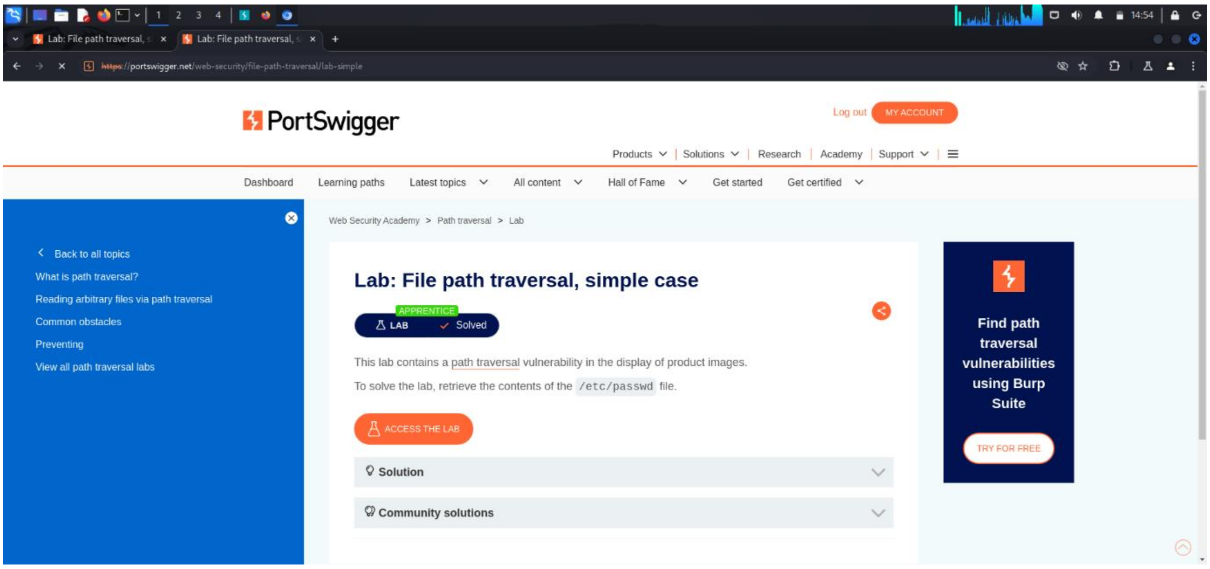
This lab contains an OS command injection vulnerability in the product stock checker.

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.

Path traversal

File path traversal, simple case



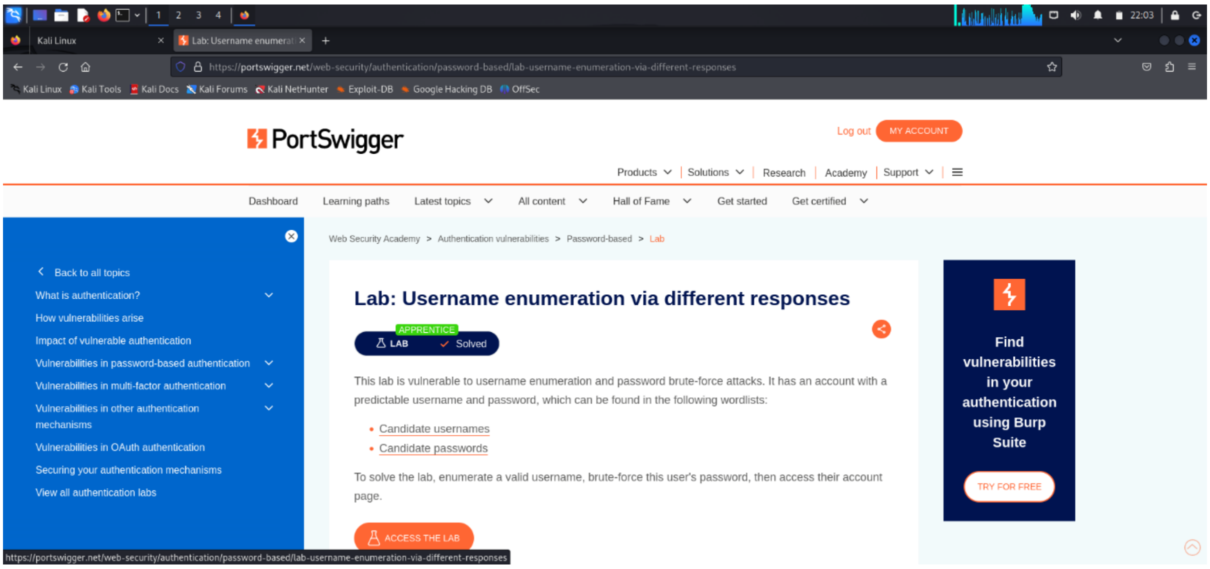
Lab: File path traversal, simple case

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.

Authentication

Username enumeration via different responses


Kali Linux
Lab: Username enumerat
https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
Find vulnerabilities in your authentication using Burp Suite
TRY FOR FREE
22:03

Lab: Username enumeration via different responses

APPRENTICE LAB Solved

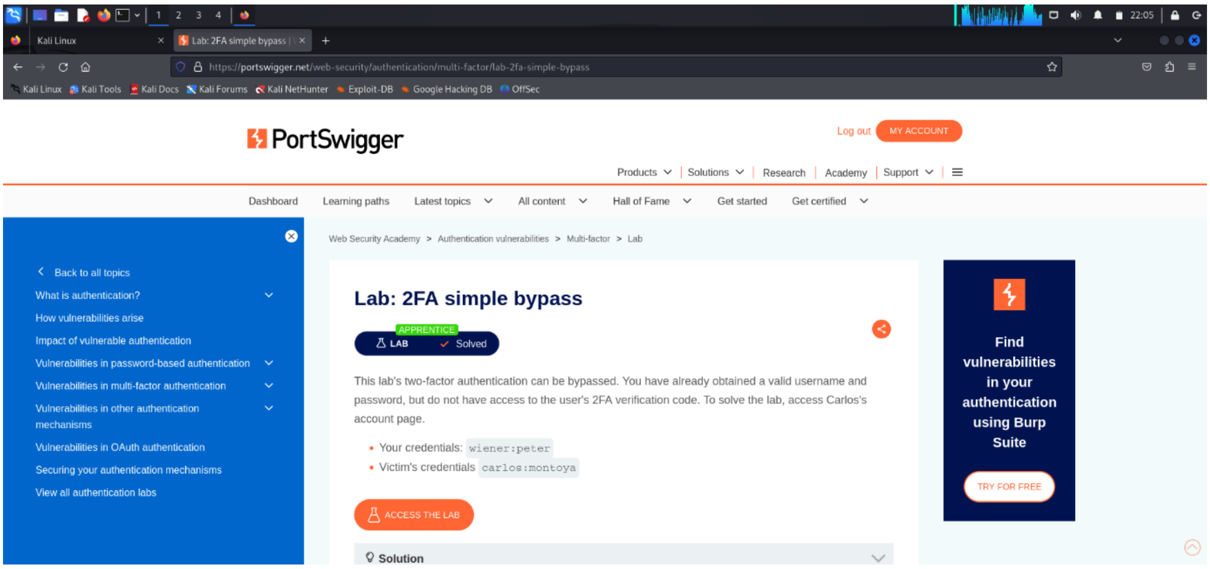
This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- 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

2FA simple bypass


Kali Linux
Lab: 2FA simple bypass
https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-simple-bypass
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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 > Multi-factor > Lab
Find vulnerabilities in your authentication using Burp Suite
TRY FOR FREE
22:05

Lab: 2FA simple bypass

APPRENTICE LAB Solved

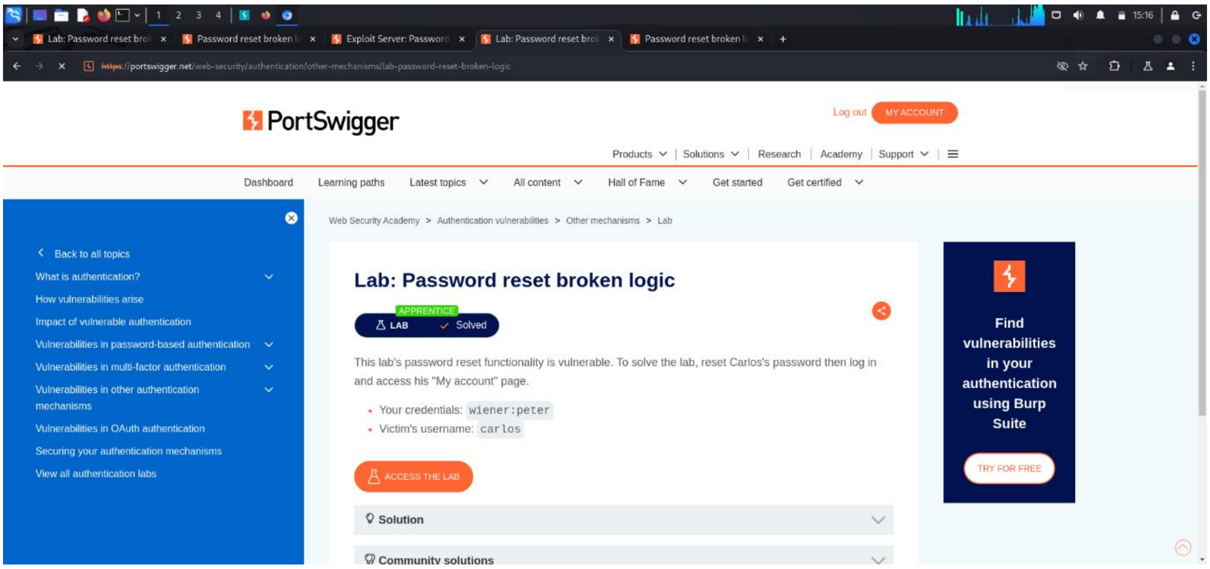
This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

- Your credentials: `wiener:peter`
- Victim's credentials `carlos:montoya`

ACCESS THE LAB

Solution

Password reset broken logic



Lab: Password reset brok
Password reset broken l
Exploit Server: Password
Lab: Password reset brok
Password reset broken l
https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-broken-logic
15:16
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 > Other mechanisms > Lab
APPRENTICE
LAB
Solved
ACCESS THE LAB
Solution
Community solutions
Find vulnerabilities in your authentication using Burp Suite
TRY FOR FREE

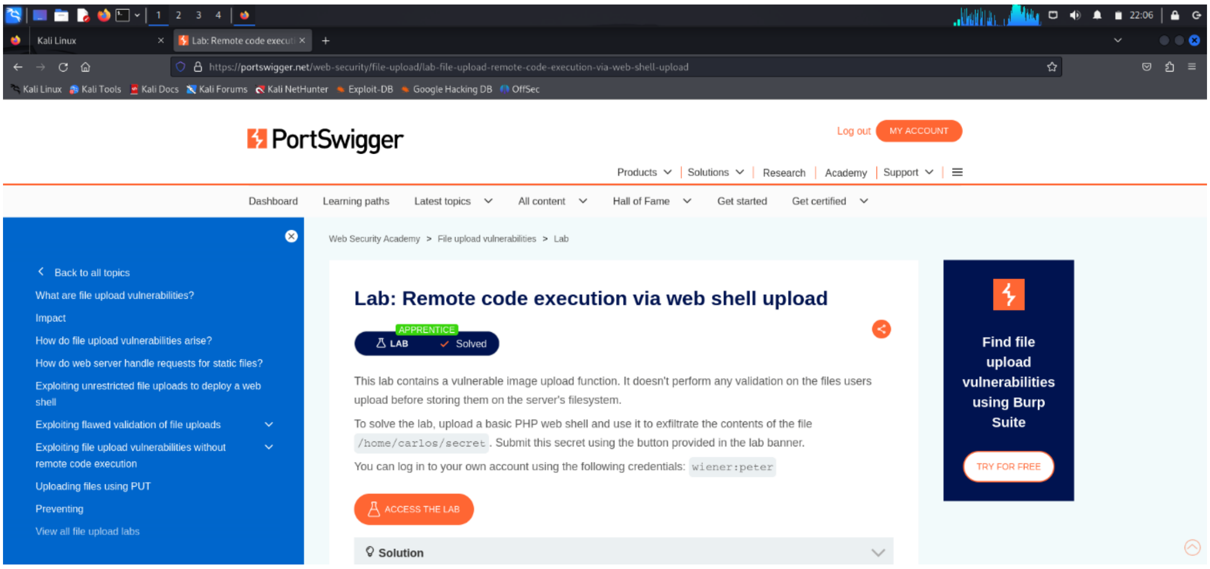
Lab: Password reset broken logic

This lab's password reset functionality is vulnerable. To solve the lab, reset Carlos's password then log in and access his "My account" page.

- Your credentials: `wiener:peter`
- Victim's username: `carlos`

File upload vulnerabilities

Remote code execution via web shell upload



Kali Linux
Lab: Remote code executi
https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
22:06
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
Find file upload vulnerabilities using Burp Suite
TRY FOR FREE

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`