**SOLVED 6 LABS**

**SQL INJECTION, VAPT 2FA simple bypass,** **login bypass, SQL injection attack,path traversal(2)**

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

APPRENTICE

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:

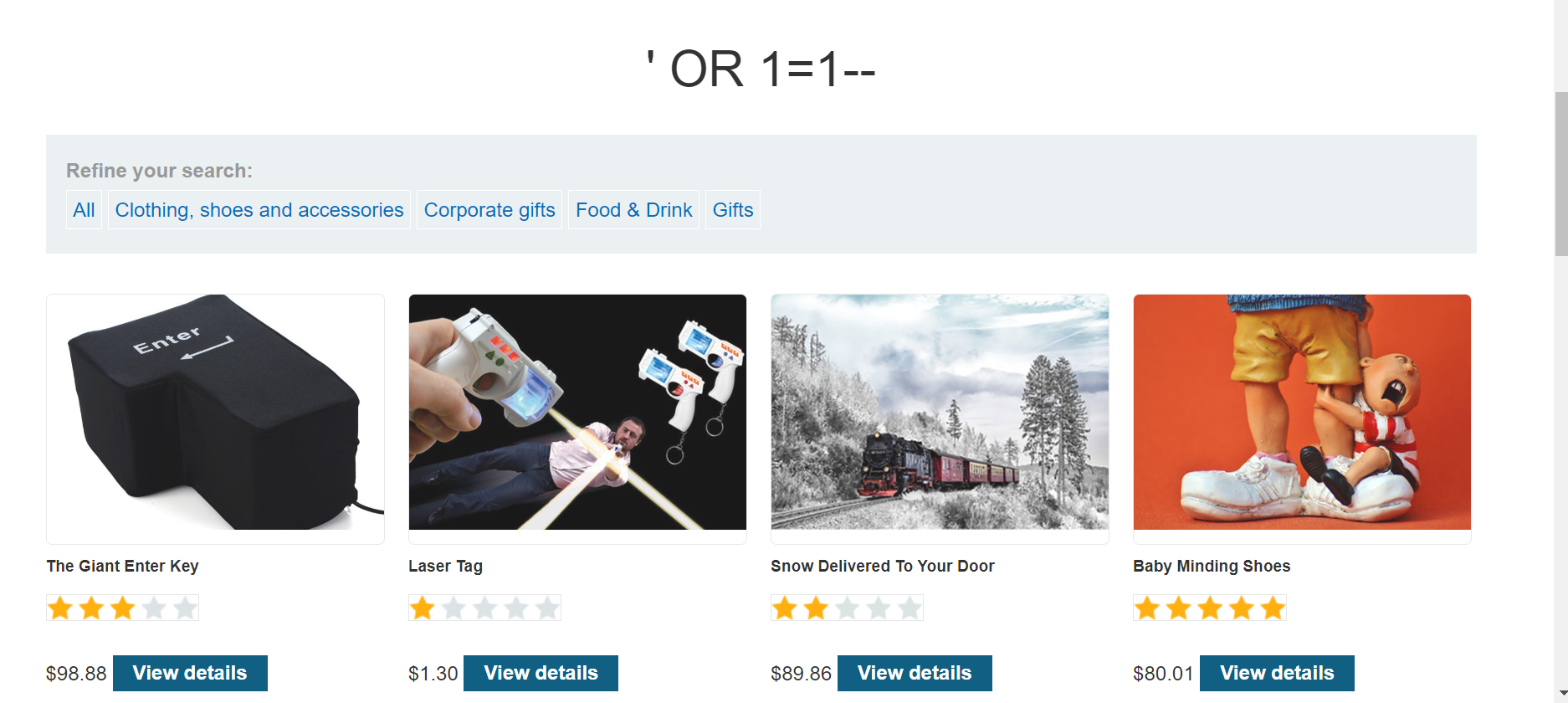
SELECT \* FROM products WHERE category = 'Gifts' AND released = 1

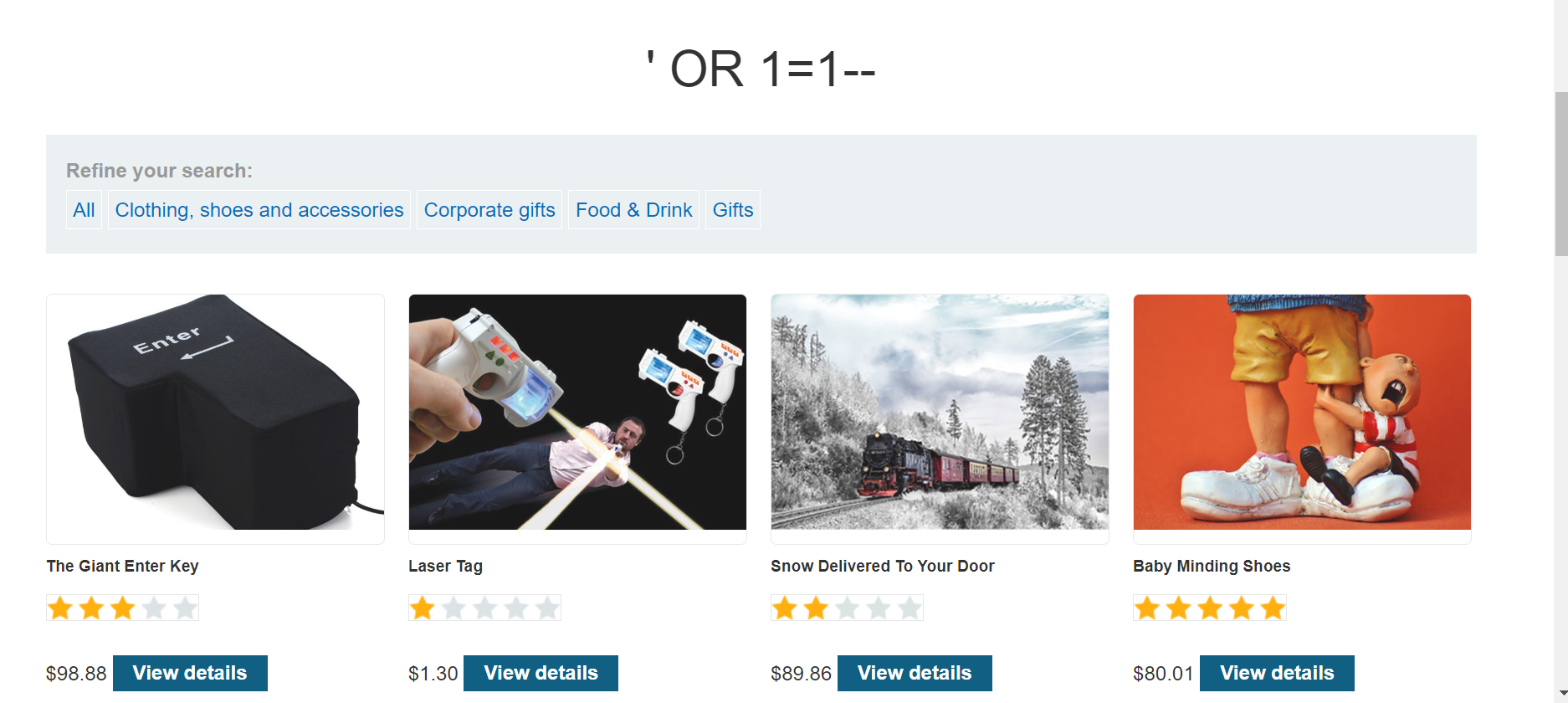
To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products.

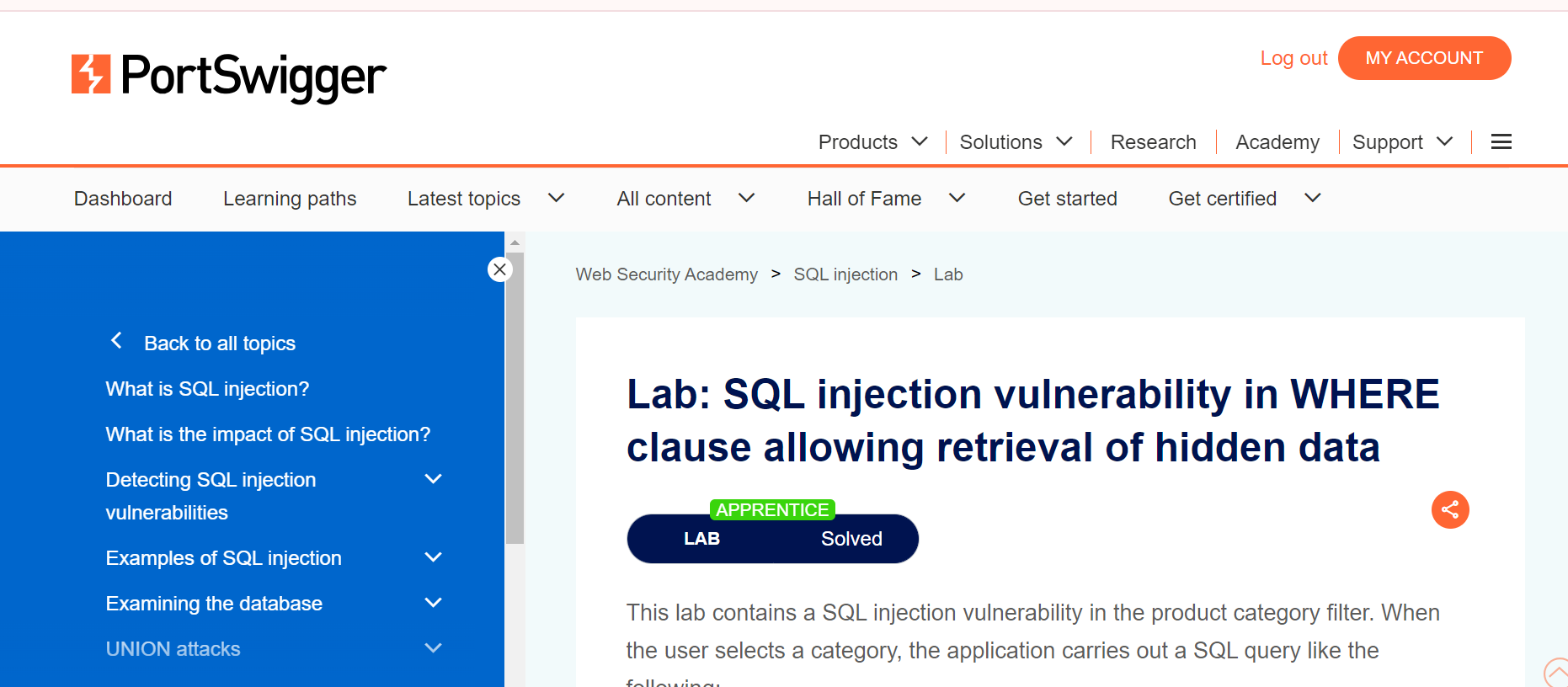
**Solution**

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Modify the category parameter, giving it the value '+OR+1=1--
3. Submit the request, and verify that the response now contains one or more unreleased products.
4. '+OR+1=1--

0aae00640330b6a882b5cf9b0074006c.web-security-academy.net/filter?category=%27+OR+1=1--





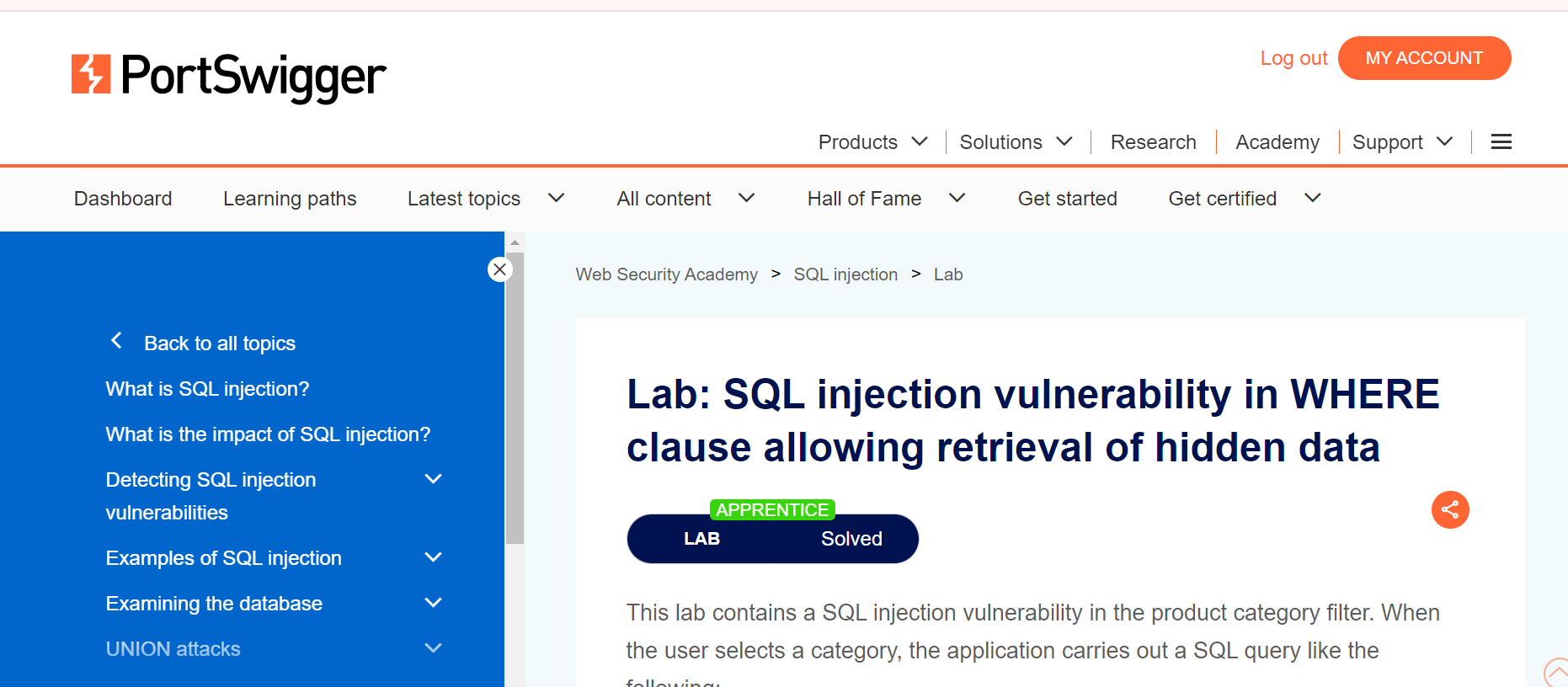


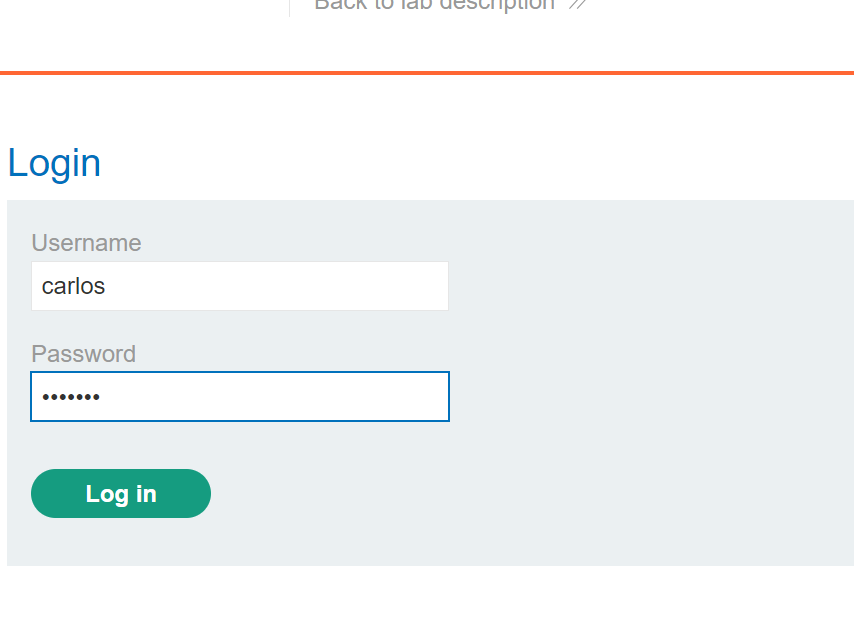
2) **Lab: 2FA simple bypass**

APPRENTICE

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



https://0a5900e804394d0084faaee9003b0018.web-security-academy.net/my-account

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a login box

Description automatically generated

3) **Lab: SQL injection vulnerability allowing login bypass**

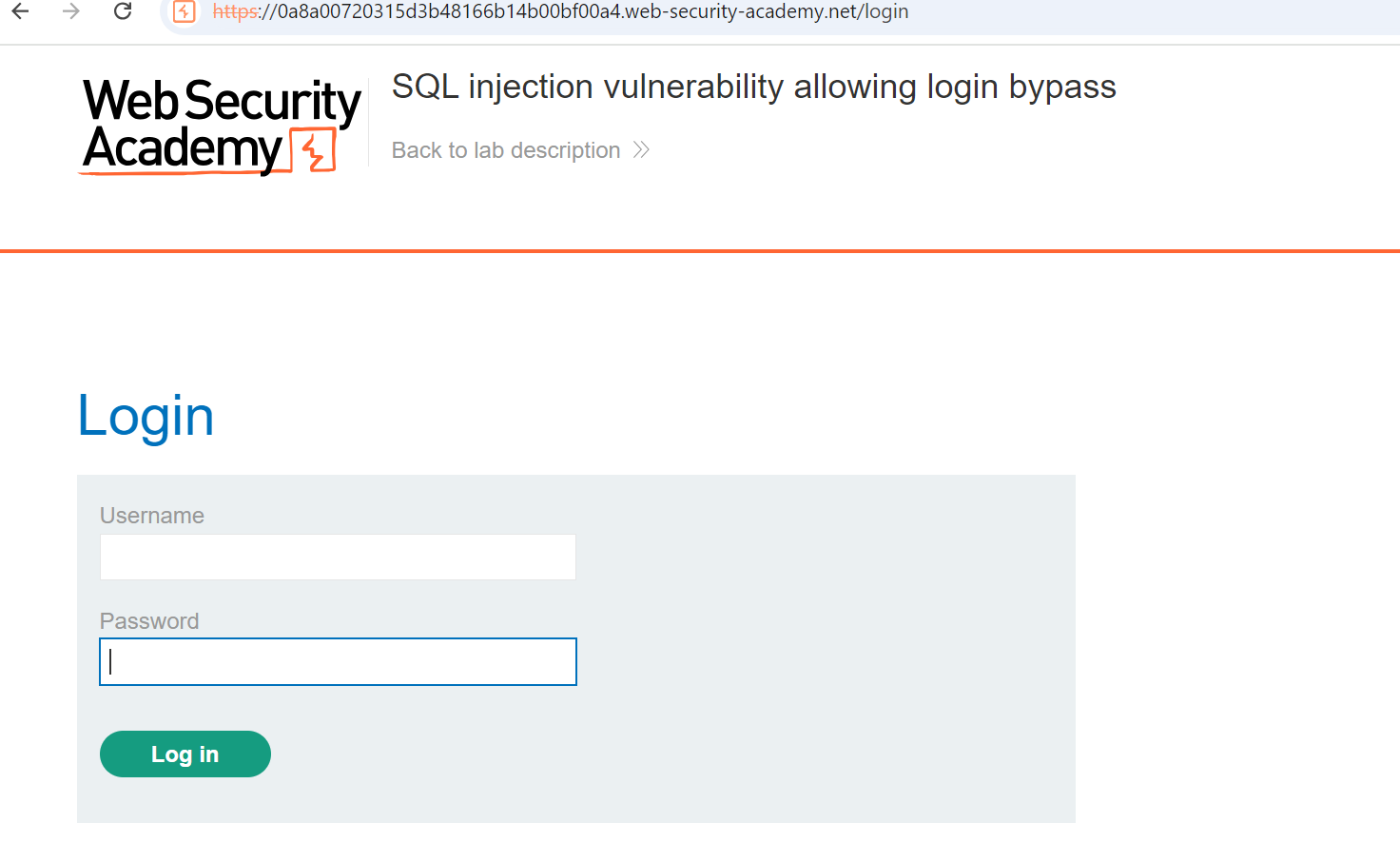
**APPRENTICE**

**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.**

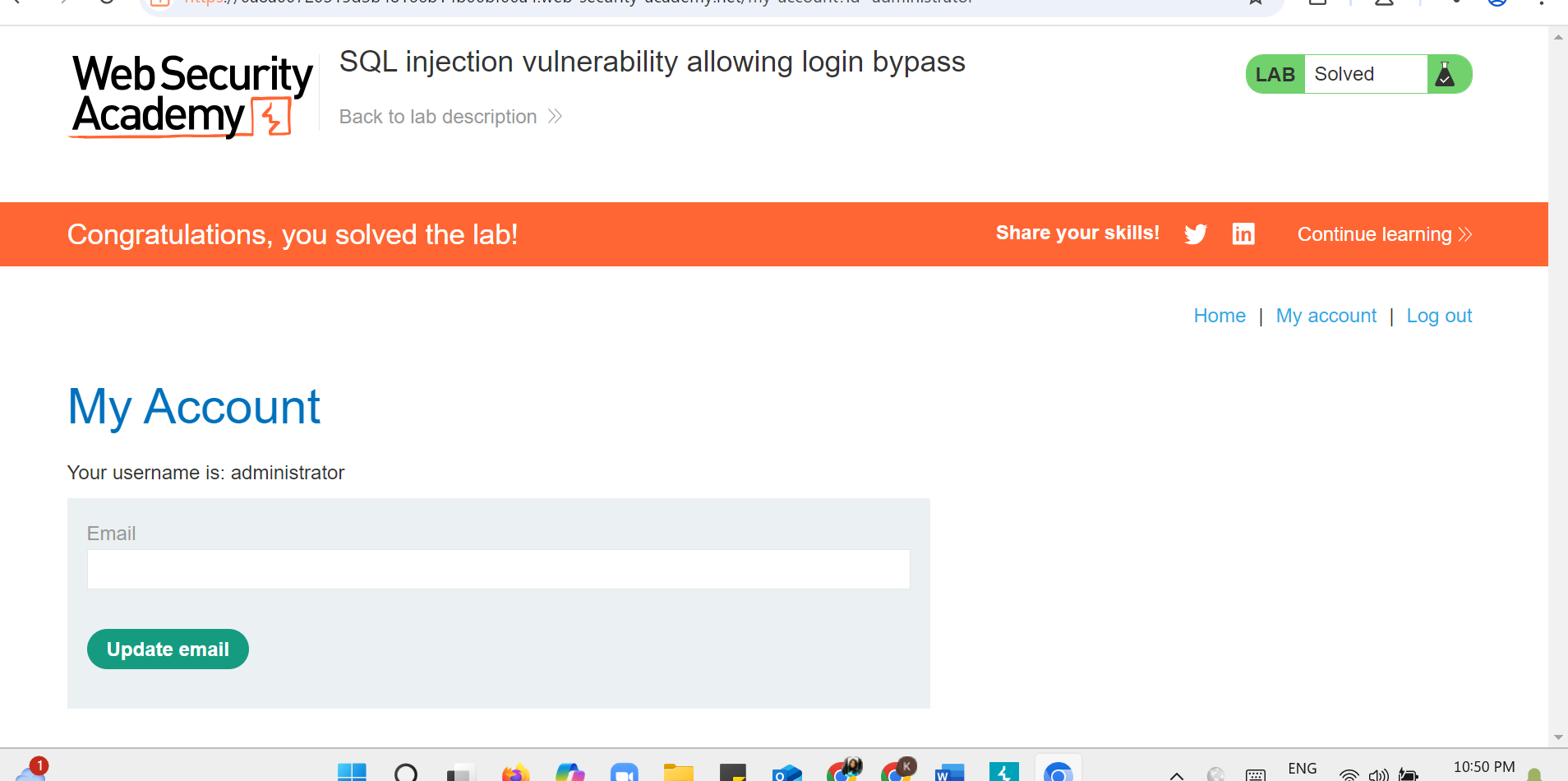
**Solution**

1. Use Burp Suite to intercept and modify the login request.
2. Modify the username parameter, giving it the value: administrator'—



A screenshot of a computer

Description automatically generated



4) **Lab: SQL injection attack, querying the database type and version on Oracle**

PRACTITIONER

This lab contains a SQL injection vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query.

To solve the lab, display the database version string.

**Solution**

1. Use Burp Suite to intercept and modify the request that sets the product category filter. 
2. Determine the [number of columns that are being returned by the query](https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns) and [which columns contain text data](https://portswigger.net/web-security/sql-injection/union-attacks/lab-find-column-containing-text). Verify that the query is returning two columns, both of which contain text, using a payload like the following in the category parameter:

'+UNION+SELECT+'abc','def'+FROM+dual—

A screenshot of a computer

Description automatically generated

1. Use the following payload to display the database version:

'+UNION+SELECT+BANNER,+NULL+FROM+v$version—

A screenshot of a web page

Description automatically generated

5) **Lab: Password reset broken logic**

APPRENTICE

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

**Solution**

1. With Burp running, click the **Forgot your password?** link and enter your own username.
2. Click the **Email client** button to view the password reset email that was sent. Click the link in the email and reset your password to whatever you want.
3. In Burp, go to **Proxy > HTTP history** and study the requests and responses for the password reset functionality. Observe that the reset token is provided as a URL query parameter in the reset email. Notice that when you submit your new password, the POST /forgot-password?temp-forgot-password-token request contains the username as hidden input. Send this request to Burp Repeater.
4. In Burp Repeater, observe that the password reset functionality still works even if you delete the value of the temp-forgot-password-token parameter in both the URL and request body. This confirms that the token is not being checked when you submit the new password.
5. In the browser, request a new password reset and change your password again. Send the POST /forgot-password?temp-forgot-password-token request to Burp Repeater again.
6. In Burp Repeater, delete the value of the temp-forgot-password-token parameter in both the URL and request body. Change the username parameter to carlos. Set the new password to whatever you want and send the request.
7. In the browser, log in to Carlos's account using the new password you just set. Click **My account** to solve the lab.

****

**Lab: File path traversal, simple case**

sThis lab contains a [path traversal](https://portswigger.net/web-security/file-path-traversal) vulnerability in the display of product images.

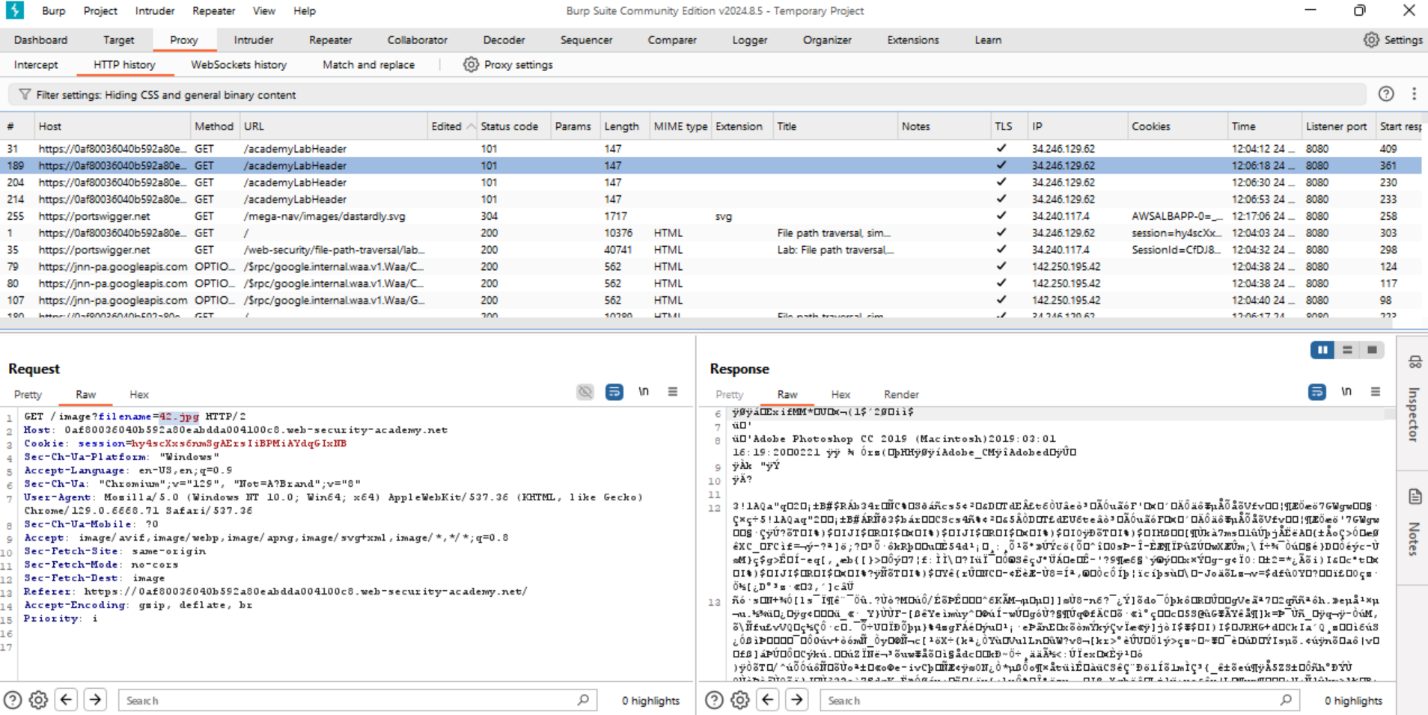
To solve the lab, retrieve the contents of the /etc/passwd file.

**Solution**

1. Use Burp Suite to intercept and modify a request that fetches a product image.
2. Modify the filename parameter, giving it the value:

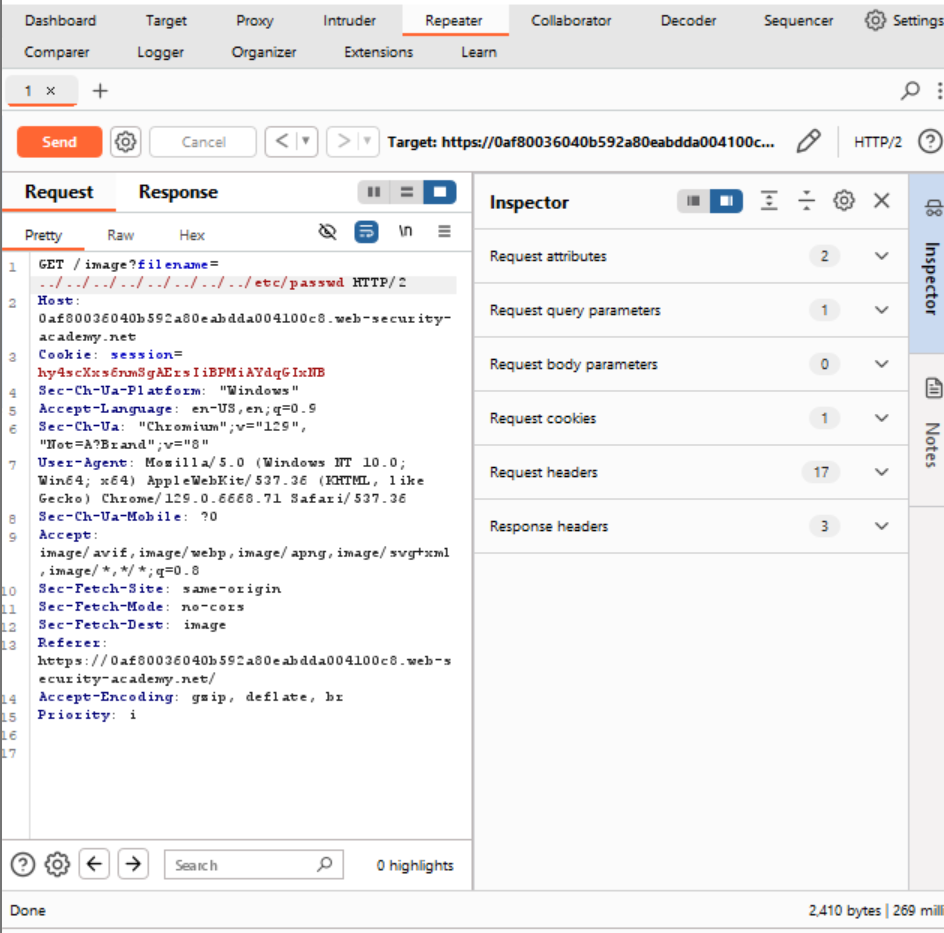
../../../etc/passwd

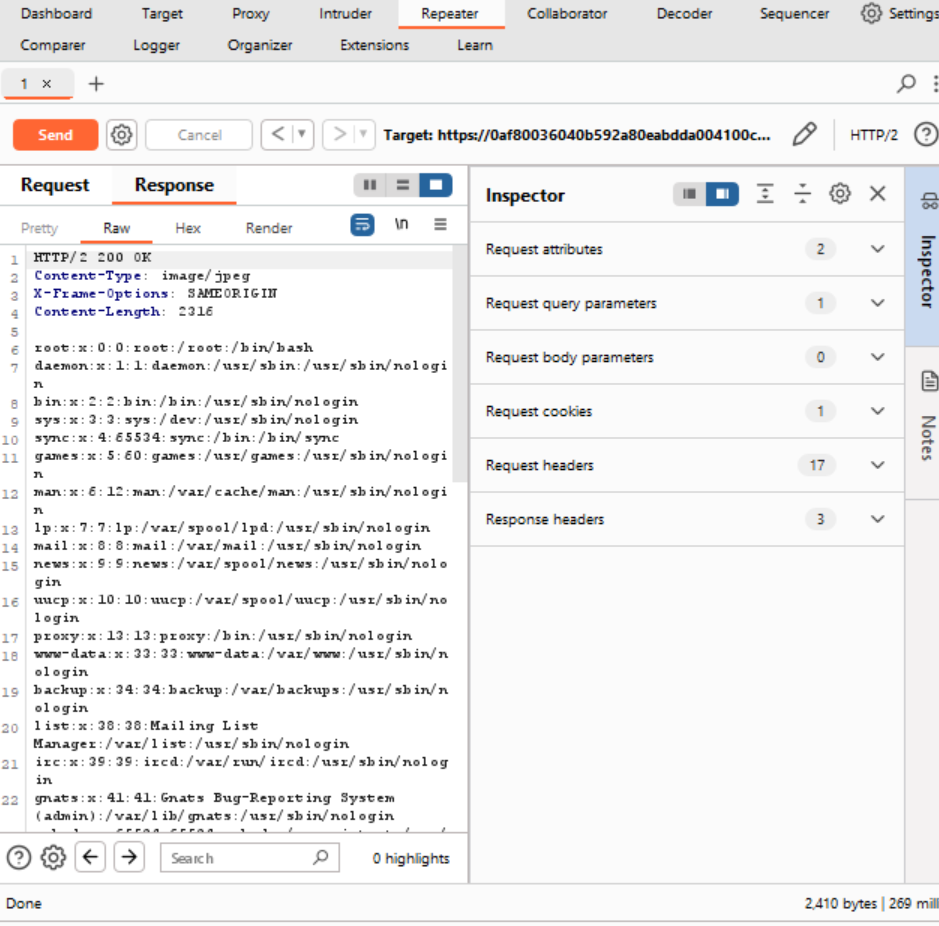
1. Observe that the response contains the contents of the /etc/passwd file.



A screenshot of a computer

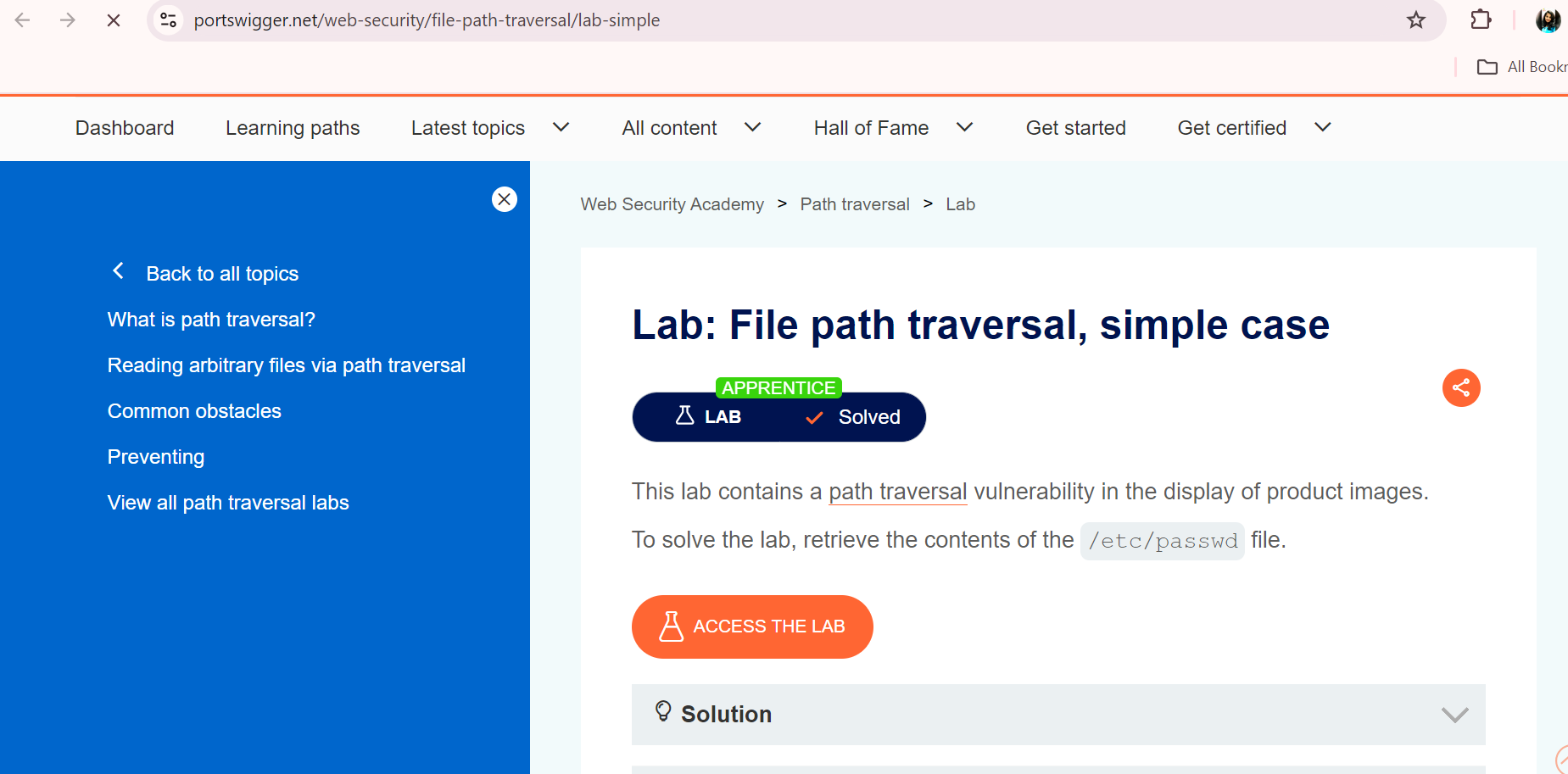
Description automatically generated





A screenshot of a computer

Description automatically generated





**Lab: File path traversal, validation of file extension with null byte bypass**

This lab contains a [path traversal](https://portswigger.net/web-security/file-path-traversal) vulnerability in the display of product images.

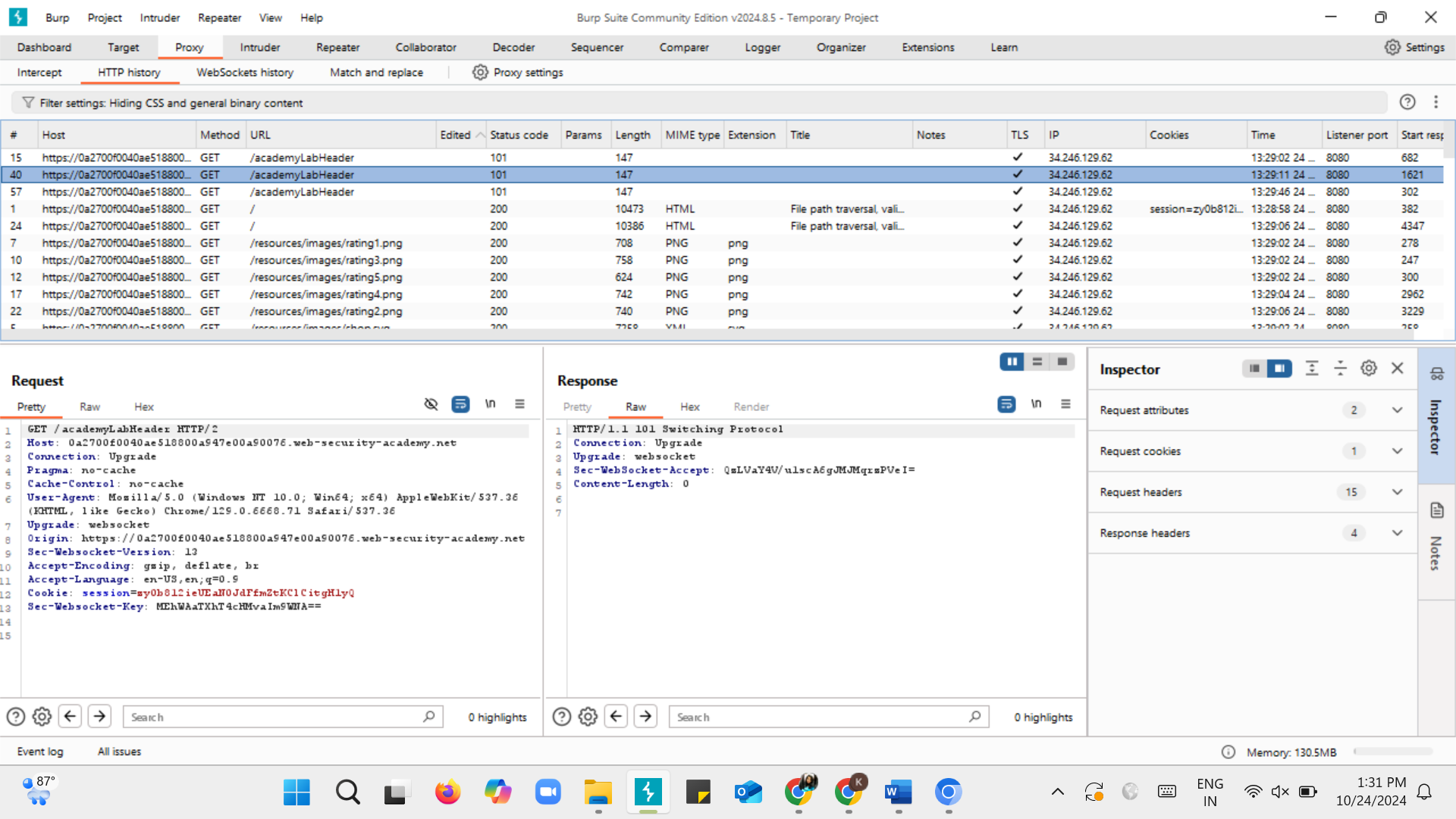
The application validates that the supplied filename ends with the expected file extension.

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

**Solution**

1. Use Burp Suite to intercept and modify a request that fetches a product image.
2. Modify the filename parameter, giving it the value:

../../../etc/passwd%00.png

1. A screenshot of a computer

   Description automatically generatedA screenshot of a computer

   Description automatically generatedA screenshot of a computer code

   Description automatically generated
2. Observe that the response contains the contents of the /etc/passwd file.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated