File path traversal, traversal sequences stripped with superfluous URL-decode –

Lab Report

Submitted By:

Name: Arsalan Khan
Position/Role: Internee
Date: July 25, 2025

Platform:

PortSwigger

Objective:

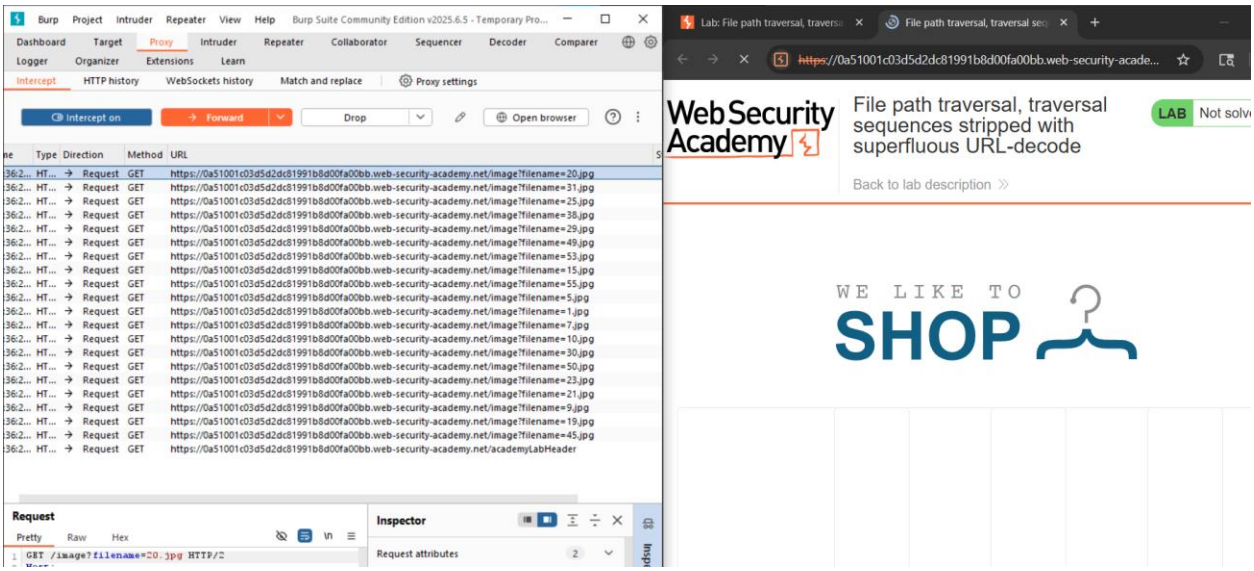
Bypass path traversal protections that apply filtering before URL-decoding, and retrieve the contents of the /etc/passwd file.

Tools Used:

- Burp Suite Community

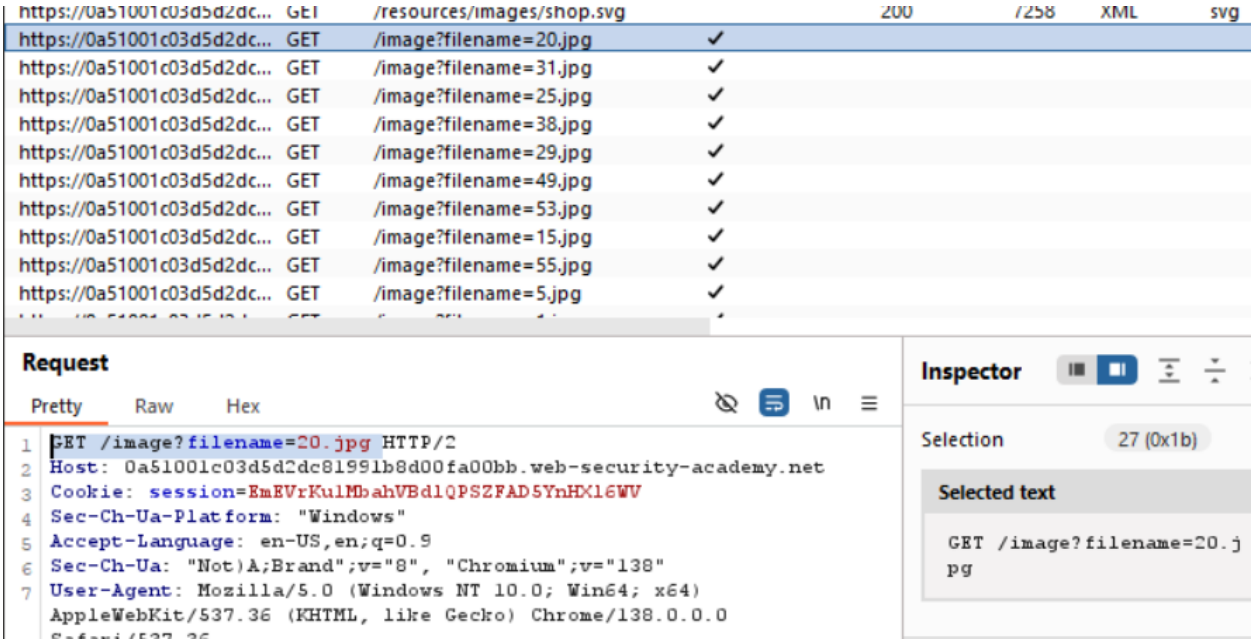
1. Access the Lab

- Observed the presence of product images loaded from the server.



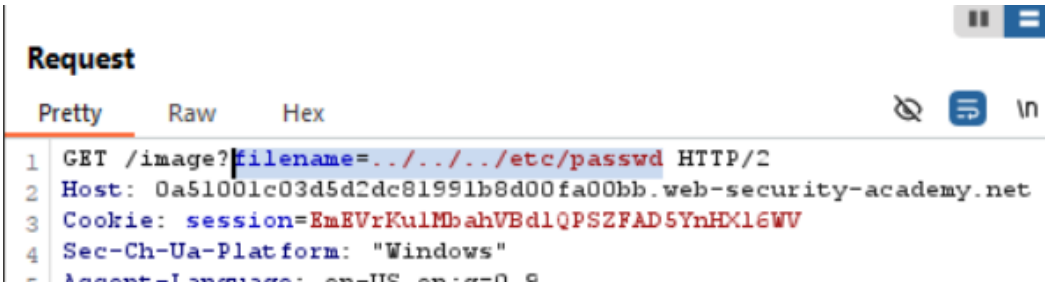
2. Intercept an Image Request

- Used Burp Suite to intercept an image request triggered by clicking or loading a product.



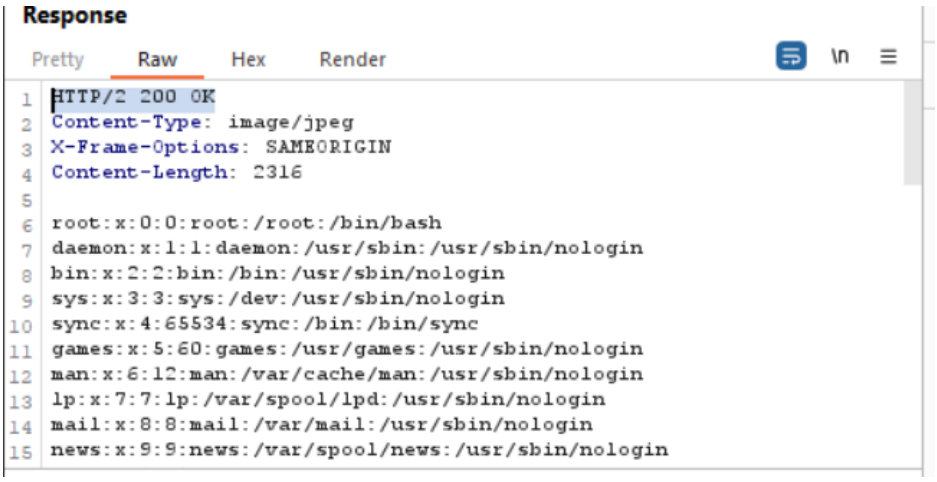
3. Modify the Request with Double Encoding

- Sent the request to Burp Repeater**.**
- Replaced the filename parameter with the following double-encoded traversal payload**:**

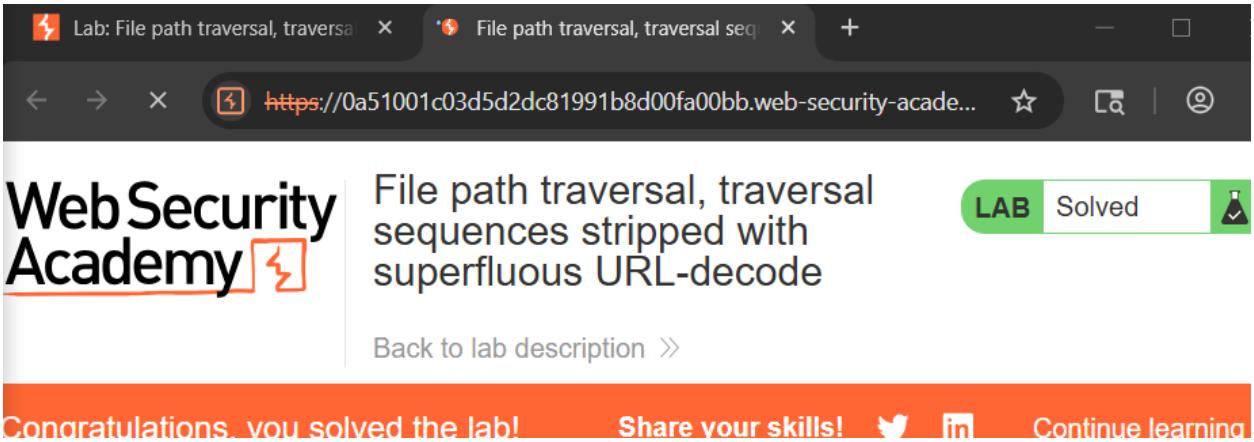


4. Observe the Response

- Received a response containing the content of /etc/passwd, confirming that the traversal was successful.



5. Submit the Lab



Vulnerability Analysis:

- **Vulnerability:** The application filters user input before decoding, allowing double-encoded traversal sequences to bypass restrictions.
- **Impact:** Allows unauthorized access to server-side files (in this case, `/etc/passwd`).
- **Severity:** High

Mitigation Recommendations:

- Decode input before validating it.
- Use strict allow-lists for file access (e.g., match only against known safe filenames).
- Sanitize and normalize file paths using secure libraries.
- Never trust URL-encoded input without full decoding and validation.
- Run applications with least privilege to limit file access risk.

Conclusion:

The lab illustrates how superfluous or misordered URL-decoding can be exploited. By using a double-encoded path traversal payload, we accessed sensitive server files and solved the lab.

End…