Information disclosure on debug page – Lab Report

Submitted By:

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

Platform:

PortSwigger

Objective:

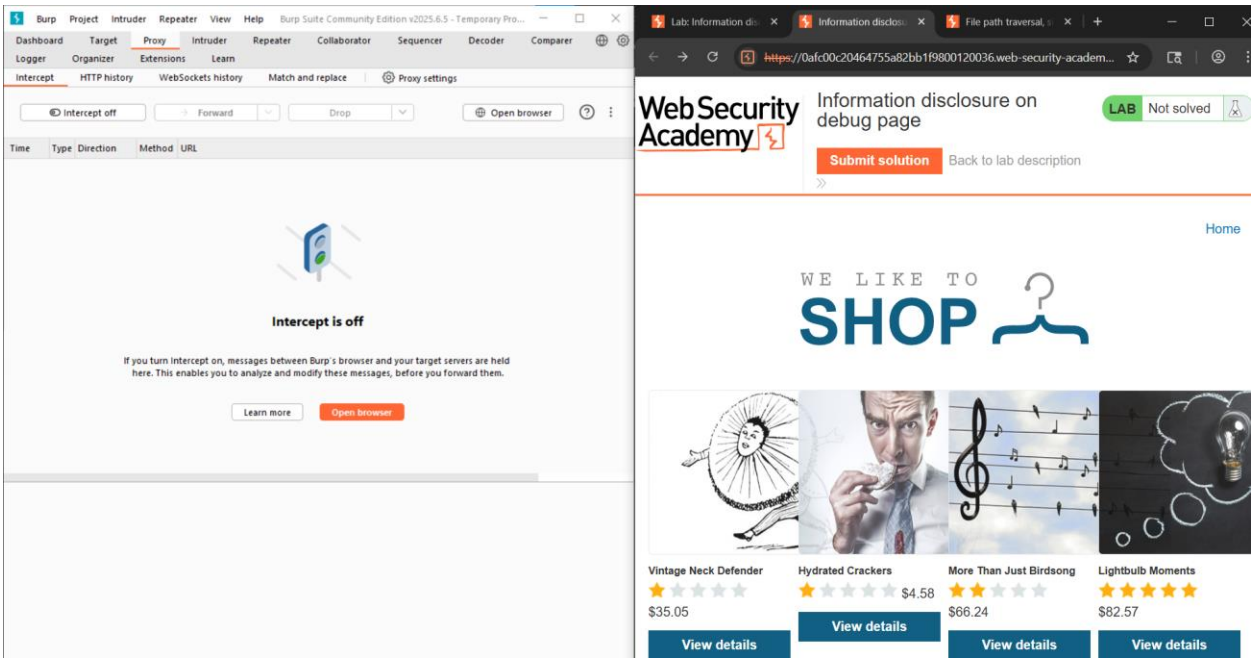
Identify and extract sensitive information disclosed on a debug page. Specifically, retrieve the value of the SECRET_KEY environment variable and submit it to solve the lab.

Tools Used:

- Burp Suite Community

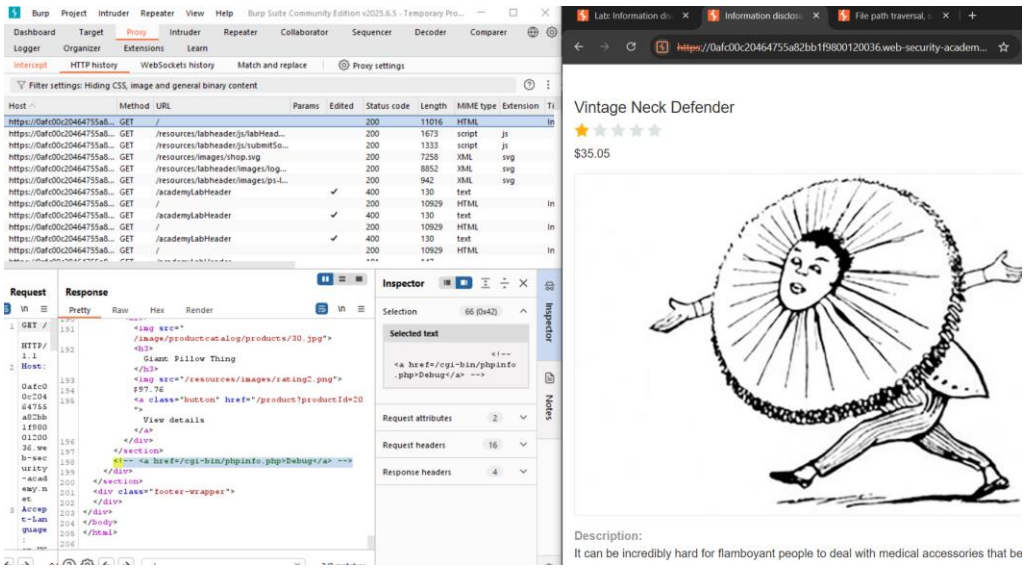
1. Access the Lab

- Opened the home page to start the analysis.



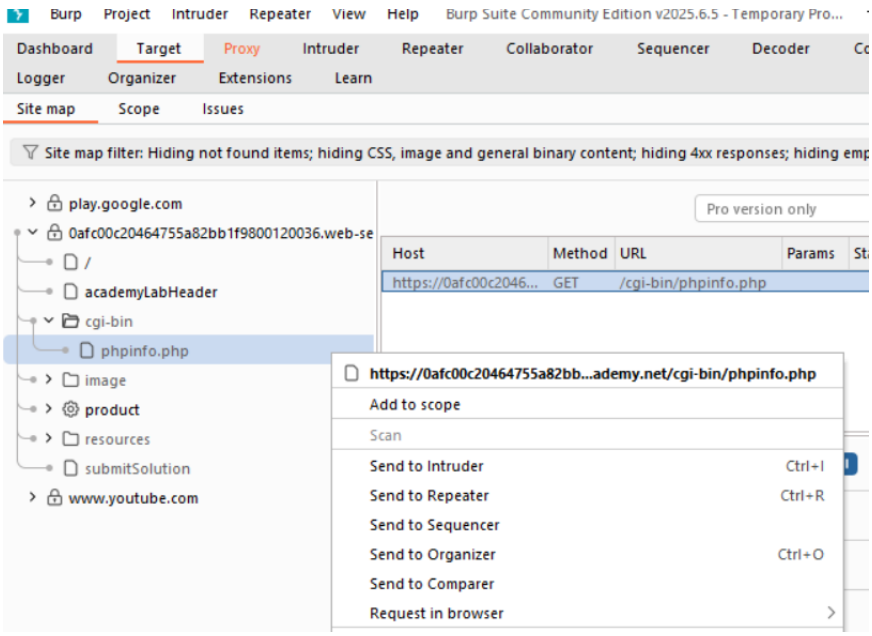
2. Inspect HTML for Comments

- Searched manually through the code for any HTML comments**.**
- Found the following hidden comment:



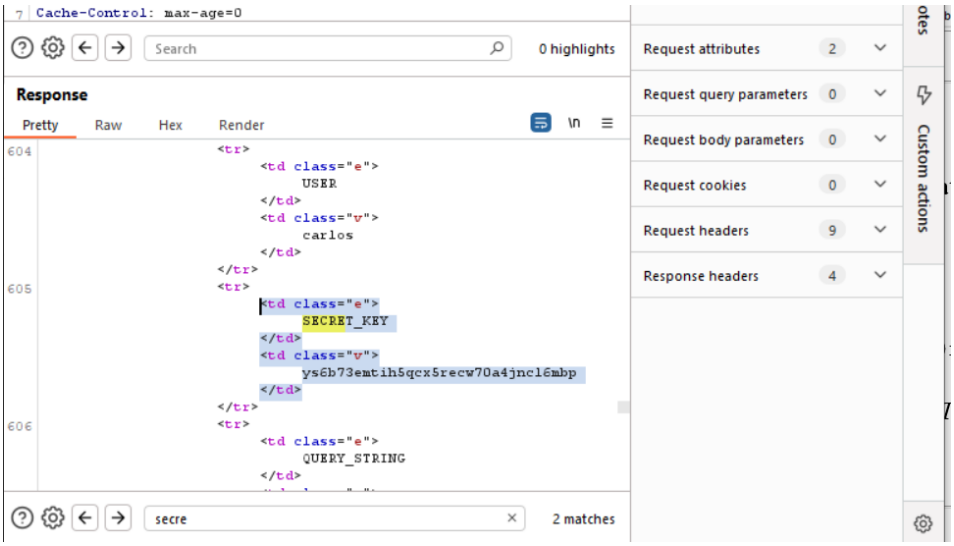
3. Access the Debug Page

- In the Site Map, right-clicked on /cgi-bin/phpinfo.php
- Selected "Send to Repeater"

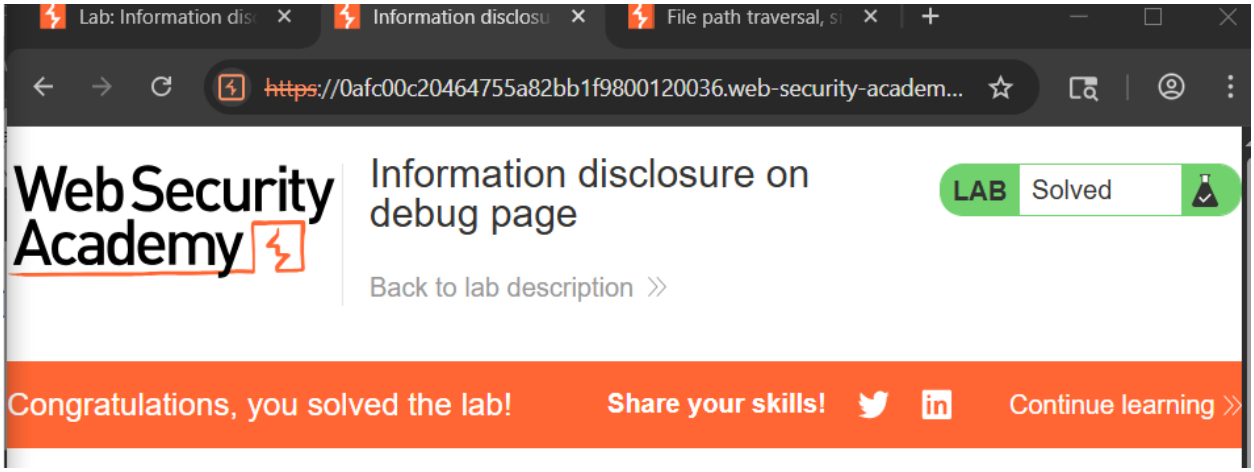


4. Extract the SECRET_KEY

- The debug page displayed PHP configuration info, including environment variables.
- Searched the response for SECRET_KEY.
- Found a line similar to:



5. Submit the SECRET_KEY



Vulnerability Analysis:

- **Issue:** A debug page (/cgi-bin/phpinfo.php) is publicly accessible and reveals sensitive server configuration data.
- **Sensitive Data Found:** SECRET_KEY (used in sessions, encryption, or app logic).
- **Cause:** Exposing internal diagnostic pages in production.
- **Impact:** Attackers can use leaked keys to forge session tokens or decrypt sensitive data.

Mitigation Recommendations:

- Remove or restrict access to all debug/diagnostic pages in production.
- Use authentication and IP-based access controls for admin/debug tools.
- Regularly audit application comments and metadata for sensitive references.
- Store sensitive environment variables securely and avoid exposing them in outputs.

Conclusion:

The lab demonstrates the risks of exposing debug tools in production. By analyzing the site's HTML and hidden paths, we were able to access phpinfo.php and extract the SECRET_KEY, successfully solving the lab.

End...