**SCENARIO**

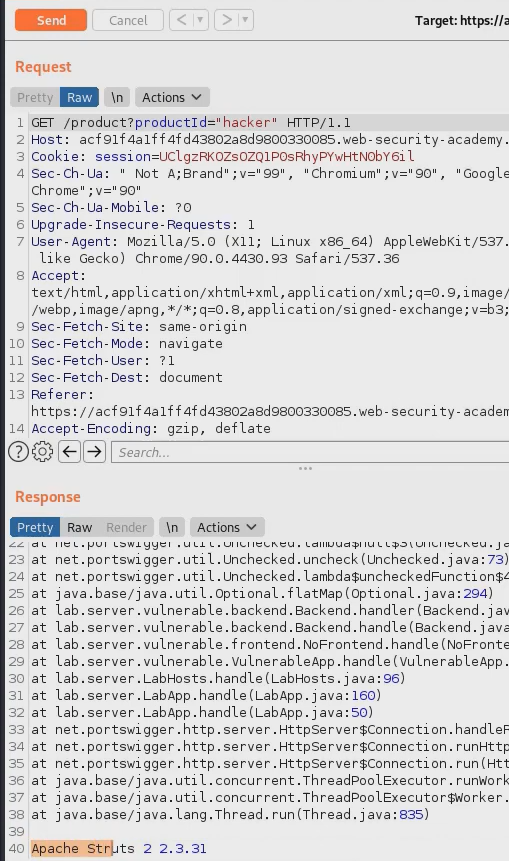
The application's error-handling exposes comprehensive stack traces, which leak critical version information about an incorporated third-party framework.

**PROCEDURE**

1. Initiate Burp and access a product page.
2. In Burp, under "Proxy" > "HTTP history", observe that product page GET requests carry a productID parameter.
3. Manipulate this parameter's value in Burp Repeater, replacing it with a string.
4. This change induces an error, revealing that the application uses Apache Struts 2 version 2.3.31.

**PAYLOAD**

Manipulated request: GET /product?productId="test"

**PROOF OF CONCEPT  
  
  
  
REMEDIATION**

1. **Mute Error Details:** Configure the application to only expose generic error messages, preventing detailed stack traces.
2. **Update Frameworks Regularly:** Ensure third-party frameworks are consistently updated to avoid known vulnerabilities.
3. **Security Audits:** Regularly audit and test the application for information leakage vulnerabilities.