**SCENARIO**

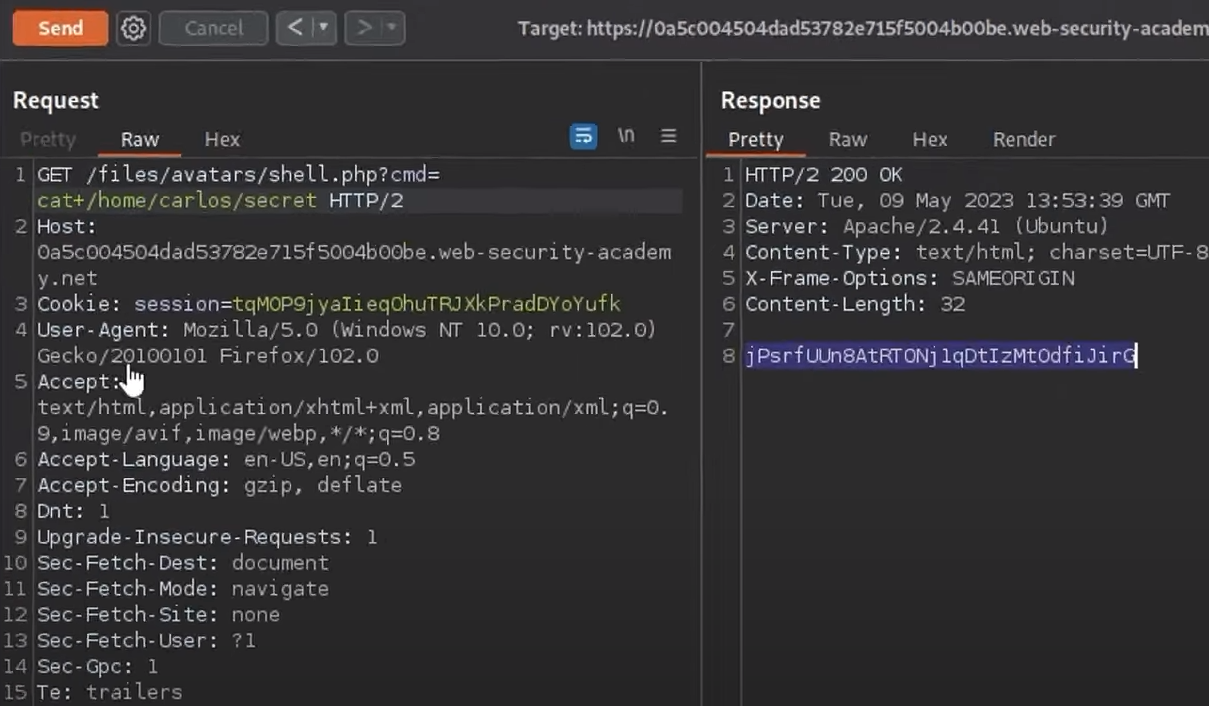
The lab showcases an image upload function that attempts to restrict uploads based on the MIME type. However, the validation is based on user-controlled input, allowing us to bypass it.

**PROCEDURE**

1. After logging in, we uploaded an image avatar and reviewed the path in Burp's HTTP history.
2. We prepared an exploit.php script aiming to reveal Carlos's secret.
3. Our initial attempt to upload the script was blocked due to MIME type restrictions.
4. Using Burp Repeater, we manipulated the POST request's Content-Type to image/jpeg, tricking the server into accepting our malicious PHP file.
5. Adjusting the GET request's path in Burp Repeater allowed us to execute the script and uncover Carlos's secret

**PAYLOAD**

<?php echo file\_get\_contents('/home/carlos/secret'); ?>

**  
PROOF OF CONCEPT**

**REMEDIATION**

1. **Server-side MIME Type Detection:** Rely on server-side MIME type detection rather than user-provided values.
2. **Disallow Direct Script Execution:** Ensure that the directory where files are uploaded cannot directly execute scripts.
3. **Content Inspection:** Implement a solution that inspects the actual content of uploaded files to determine their legitimacy.