**SCENARIO**

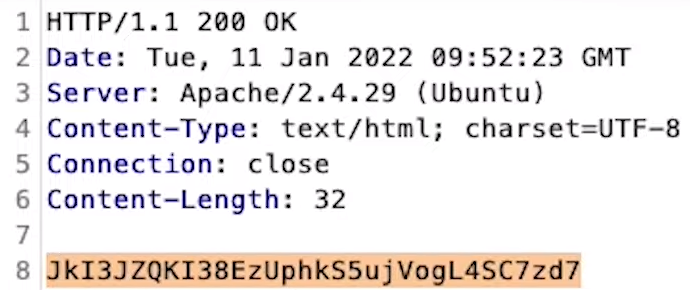
The lab's image upload system uses a blacklist to prevent certain file extensions. Nevertheless, a flaw in its setup can be exploited.

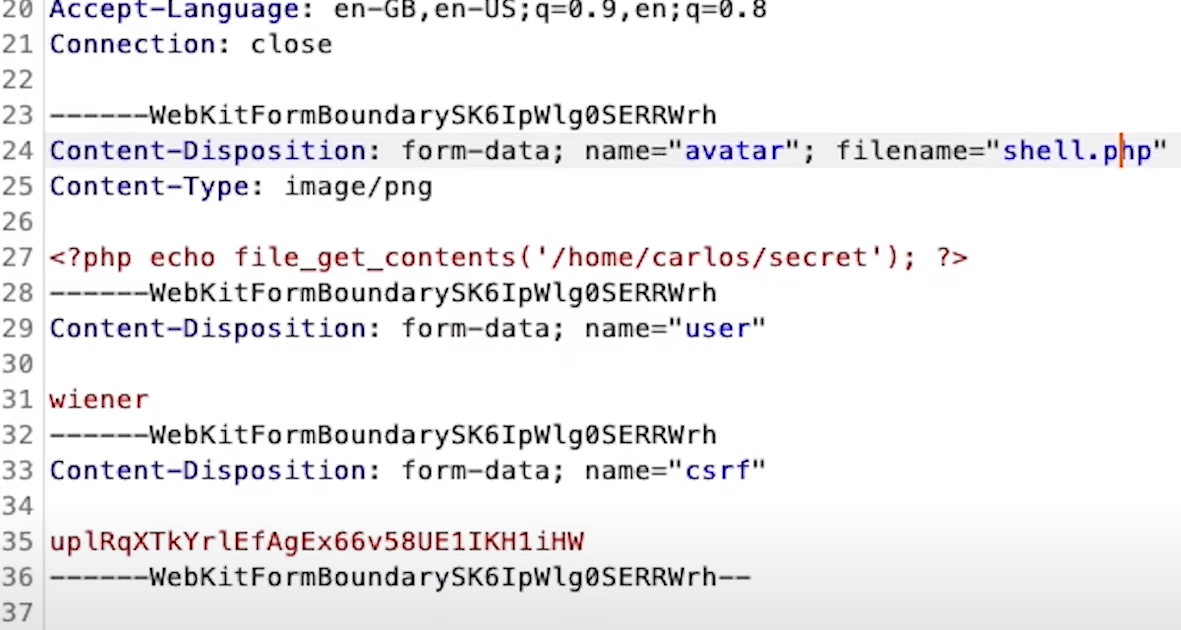
**PROCEDURE**

1. We attempted to upload our exploit.php script as an avatar but faced restrictions due to its .php extension.
2. In Burp, the server's headers indicated an Apache server.
3. Using the .htaccess file, we mapped the .l33t extension to be treated as PHP, bypassing the extension restriction.
4. By uploading our malicious PHP with the .l33t extension, we successfully executed it, revealing Carlos's secret.

**PAYLOAD**

1. AddType application/x-httpd-php .l33t
2. <?php echo file\_get\_contents('/home/carlos/secret'); ?>

**  
PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Disable .htaccess Overwrite:** Disable or limit the capabilities of .htaccess files.
2. **File Content Validation:** Inspect the actual content of uploaded files to determine if they contain code.
3. **Maintain a Strict Whitelist:** Allow only specific file extensions.