**SCENARIO**

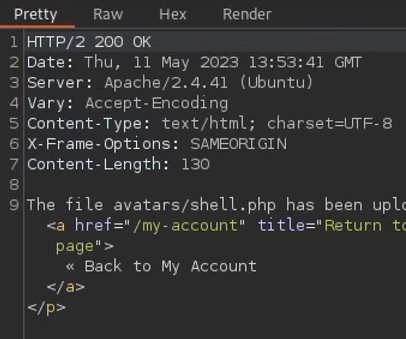
The lab's image upload mechanism has a blacklist for certain file extensions. Still, an old obfuscation technique using null bytes can bypass this.

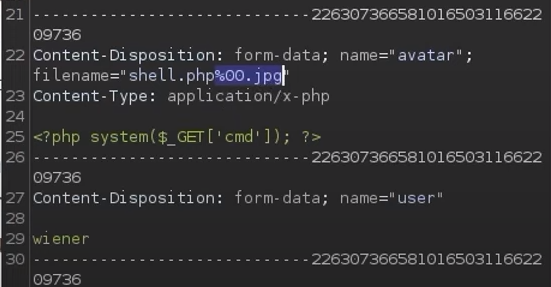
**PROCEDURE**

1. We tried to upload our exploit.php script but were restricted due to its extension.
2. Using Burp Repeater, we modified the upload request's filename to include a URL-encoded null byte followed by .jpg.
3. The server accepted this manipulated request, allowing our PHP script's execution and disclosure of Carlos's secret.

**PAYLOAD**

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

 **PROOF OF CONCEPT**



**REMEDIATION**

1. **Handle Null Bytes:** Modern servers and programming languages should handle null bytes properly; ensure they're updated.
2. **Content-based Validation:** Validate files based on their actual content rather than relying solely on filenames or extensions.
3. **Audit and Logging:** Keep detailed logs to monitor and detect any suspicious uploads.