Lab: Web shell upload via Content-Type restriction bypass
Date: 16.07.2025
Vulnerability type: Remote code execution (RCE)
Difficulty level: Medium
Purpose: This vulnerability takes advantage of insufficient Content-Type validation, allowing an attacker to upload a malicious file to the server. By using a web shell, the attacker can execute arbitrary commands remotely and gain unauthorized access to the system.

Vulnerability Description

The application implements insufficient validation of the Content-Type header during the file upload process. It relies solely on this header to determine the type of the uploaded file without verifying the actual file extension or content (magic bytes). As a result, an attacker can craft a malicious PHP web shell, modify the Content-Type to a permitted value (such as image/png), and upload it to the server. If the uploaded file is placed in a publicly accessible and executable directory, the attacker can access it directly via URL and execute arbitrary system commands.

This vulnerability may lead to full remote code execution (RCE) on the server, allowing the attacker to read, write, or delete files, and potentially escalate privileges depending on the web server's configuration.

Exploit Steps

1. The profile picture upload functionality was analyzed. It was observed that the server only accepted files with a Content-Type such as image/jpeg or image/png.
2. A PHP web shell file was created:
   <?php system($_GET['cmd']); ?>
3. A normal upload attempt via browser failed due to file type restrictions.
4. The request was intercepted using Burp Suite and manually modified:
   filename=shell.php
   Content-Type changed to image/jpeg
5. Upon sending the modified request, the file was successfully uploaded. The uploaded file was then accessed via: https://<site>/files/avatars/shell.php
6. The web shell was executed, and the contents of /home/carlos/secret were retrieved, completing the objective.

Payload & Tools

Type	Content
Payload	PHP script: <?php system($_GET[‘cmd’]); ?>
Tools	Burp Suite

Risks and Recommended Security Measures

Risk	Recommended Security Measure
An attacker may upload a malicious web shell and execute remote commands on the server (RCE).	Validate file MIME type, extension, and content (magic bytes) on the server side before accepting the file.
The application relies solely on the Content-Type header for file type validation.	Never trust client-provided headers; enforce MIME type checks on the server side.
Uploaded files might be stored in an executable directory.	Store uploaded files in a directory with no script execution permissions (e.g., disable PHP execution).

Notes

This vulnerability can lead to severe security risks, especially Remote Code Execution (RCE), if uploaded files are processed without proper server-side validation. Such a weakness can potentially allow attackers to gain full control over the system.

Relying solely on content-type validation is insufficient. Additional layers like MIME type checks and file signature analysis should be implemented on the server side.

It is recommended to review the application at both the source code and configuration levels. Furthermore, regular security testing should be conducted to ensure long-term protection.
