File Upload Vulnerability

Prof. Anthoniraj Amlanathan

What is File Uploading?

- A file is a computer resource for recording data on a storage device.
- File uploading is essentially a website or web app feature that allows users to upload images, audios, videos, and documents.
- For instance, social media apps allow users to upload videos and image files.
- VTOP allows students to upload Digital Assignments in PDF Format or Word Format.

File Types (MIME)

- The abbreviation MIME stands for **Multi-purpose Internet Mail Extensions**.
- MIME types form a standard way of classifying file types on the internet.
- Common MIME types
  - multipart/form-data - HTML with <input type = “file”>
  - text/plain – Plain Text Files
  - application/pdf – PDF Documents
  - application/msword – Microsoft Word (Older Versions)
  - application/vnd.openxmlformats-officedocument.wordprocessingml.document (New Office Versions E.g. 365)

Vulnerabilities in File Upload

- Attackers can harm your web app in different ways
  - They can upload malicious files containing viruses.
  - Attackers can upload a very heavy file that can cause the server to malfunction.
  - Cyber attackers can use suspicious file names that can cause issues in the server.
- Generally, Attacks can happen with file name, type, and size.

Prevention Techniques

- File Content Validation
- File Name Validation
- File Size Limitations