**Subject: Julio Pochet – Module 5.1 Discussion – Software Weaknesses**

**CWE-434: Unrestricted File Upload**

For this discussion, I looked into **CWE-434: Unrestricted Upload of File with Dangerous Type**. This weakness was first added to the CWE list back on **July 19, 2006**, and it’s still a big issue in web applications today.

**📝 What It Means**

Basically, this happens when a website lets users upload files—like pictures or documents—but doesn’t properly check what’s being uploaded. If someone uploads a file that looks safe (like image.jpg) but is actually something dangerous (malicious.php), it can get executed on the server and cause a lot of problems.

**💥 How It Works**

Let’s say a site allows users to upload profile pictures but only checks the file extension (like .jpg) and not the actual content. An attacker could rename a PHP script to something like profile.php.jpg and upload it. If the server doesn’t double-check and stores it in a public folder, the attacker can run commands through a browser. That gives them remote access to the system.

**🔐 What It Violates**

* **Authorization**: Attackers might gain access to files or features they shouldn’t.
* **Availability**: A bad upload could crash the site or slow it down.
* **Integrity & Confidentiality**: Hackers could change files, steal data, or upload backdoors.

**🛠 How to Prevent It**

One solid fix is to **store uploaded files outside the public web folder** and only allow access through a controlled script. Also, rename uploaded files to something random and don’t trust the file extension alone—always check the real file type and use a whitelist of safe formats.

I picked this weakness because it’s super common in real-world websites and can be easy to overlook. If any of you have seen something like this in your own projects or work, I’d love to hear how it was handled!