🕵️‍♂️🆆🅲 Wordpress: Manual Enumeration 💪(additional Information)

if it turns out that we find that the /uploads/ section is accessible, this file could exposes sensitive information such as:

🗒️ 1. Confidential or accidentally leaked files

Sometimes administrators mistakenly upload:

- Backups (.zip, .sql, .bak)
- Internal documents (.docx, .pdf, .xlsx)
- Configuration or code files (.env, .php, .conf)

🖼️ 2. Images with metadata EXIF that reveal:

- Author's username
- Editing tools
- Geolocation (if not removed)

🐚 3. Backdoors or Web Shells

If the site allows file uploads without properly validating extensions, an attacker could:

- Upload a disguised **web shell** (e.g., image.php.jpg)
- Access it directly from **/wp-content/uploads/evil.php**

📅 4. Dates and folder structure

This allows an attacker to infer:

- When the content was created
- Recent site activity
- Useful information for fingerprinting

🧠 5. Enumerating file names

- Files with **names** like **invoice_john_doe.pdf** or **admin_notes.docx** may reveal **usernames**, **email addresses**, or **sensitive information**.
- You may also find company names, product names, or internal versions.

🔁 6. Filename Reuse

You can test if the site renames duplicate files (e.g., file.jpg, file-1.jpg, etc.), and then:

- Infer that a file with that name already exists.
- Use brute force or dictionaries to find valid names.

And much more