README for WordPress File Upload Vulnerability Scanner

Prerequisites

Before using this script, ensure that you have the following:

- Python 3.x installed on your machine.
- The `requests` library installed. You can install it using pip:

  ```
  pip install requests
  ```

Input Files

The script expects the following input files:

1. **targets.txt**: This file should contain a list of target URLs to check, one per line. The URLs can be domain names (e.g., example.com) or complete URLs (e.g., http://example.com). The script will check each target for a specific plugin version.

Output Files

The script generates an output file named **results.txt**. This file will contain the results of the version checks for each URL from the `targets.txt` file. The results will include the status of the plugin (if found) and whether it is the vulnerable version "2.7.6". Any issues or status codes such as 403, 404, or errors will also be recorded in the output file.

What This Script Does

The WordPress File Upload Vulnerability Scanner is a Python script that checks a list of target websites for a specific version of the WP File Upload plugin. It searches for the plugin version "2.7.6" and records the findings. If the plugin version is found, it will check if it matches "2.7.6" and report it. If the plugin is found but the version doesn't match, it will log that information. The script also logs other HTTP statuses like 403 (Forbidden) and 404 (Not Found) for each plugin path.

Some of the Key Features

- **Plugin Version Check**: The script checks multiple plugin paths to see if the plugin is installed and if it's the vulnerable version "2.7.6".
- **Multiple Status Logging**: The script handles various HTTP status codes like 200 (OK), 403 (Forbidden), and 404 (Not Found), logging them with appropriate messages.
- **Error Handling**: logs any error messages.
- **Input and Output Files**: The script reads from `targets.txt` for the list of targets and writes the results to `results.txt`.
- **Easy to Use**: Simply prepare the input file and run the script. It will handle the rest, printing progress to the terminal and saving results in an output file.

How to Run

1. Prepare a `targets.txt` file with one target URL per line.
2. Make sure the Python script WordPress_File_Upload_Vuln_Scanner.py is in the same directory as `targets.txt` or adjust the file paths accordingly.
3. Run the script from your terminal or command line:
   `python WordPress_File_Upload_Vuln_Scanner.py`

4. After the script completes, check the `results.txt` file for the output, which will contain the URLs and their corresponding results.

Notes

- The script checks specific paths related to the WP File Upload plugin. These paths are hardcoded and include paths like `wp-content/plugins/wp-file-upload/readme.txt` and other URI's.
- The version to check for is 2.7.6. If another version is found, it will still log the URL but with a note that it's not the vulnerable version.
- The script assumes that the target websites are using HTTP. If your target URLs use HTTPS, make sure to adjust the URLs in the `targets.txt` file accordingly.