Google Dork Used:
"Header for logs at time" ext:log

Link to Exposed File:
https://www.investsrilanka.com/wp-content/uploads/smush-1c90fe93ab42be223762.log

Description & Potential Impact:
The URL points to a .log file located in the /wp-content/uploads/ directory. This structure confirms that investsrilanka.com is built on the WordPress platform. The filename identifies the source of the log as the Smush plugin, a popular tool for image optimization.

An examination of the log file's contents reveals:

Timestamps of plugin operations.

A list of image filenames and their directory paths.

Server environment details (PHP version, memory settings).

Error messages and plugin-specific operational data.

This information provides a clear footprint of the technologies used by the website.

Potential Impact:

Reconnaissance: An attacker can confirm the specific CMS (WordPress) and plugins in use. This allows them to search for known vulnerabilities associated with that software.

Information Leakage: The log exposes internal file paths and server configuration details, which can help an attacker build a more accurate map of the target system.