hansmach1ne Update README.md ... on Aug 9 History

..

README.md	4 months ago
poc.py	11 months ago

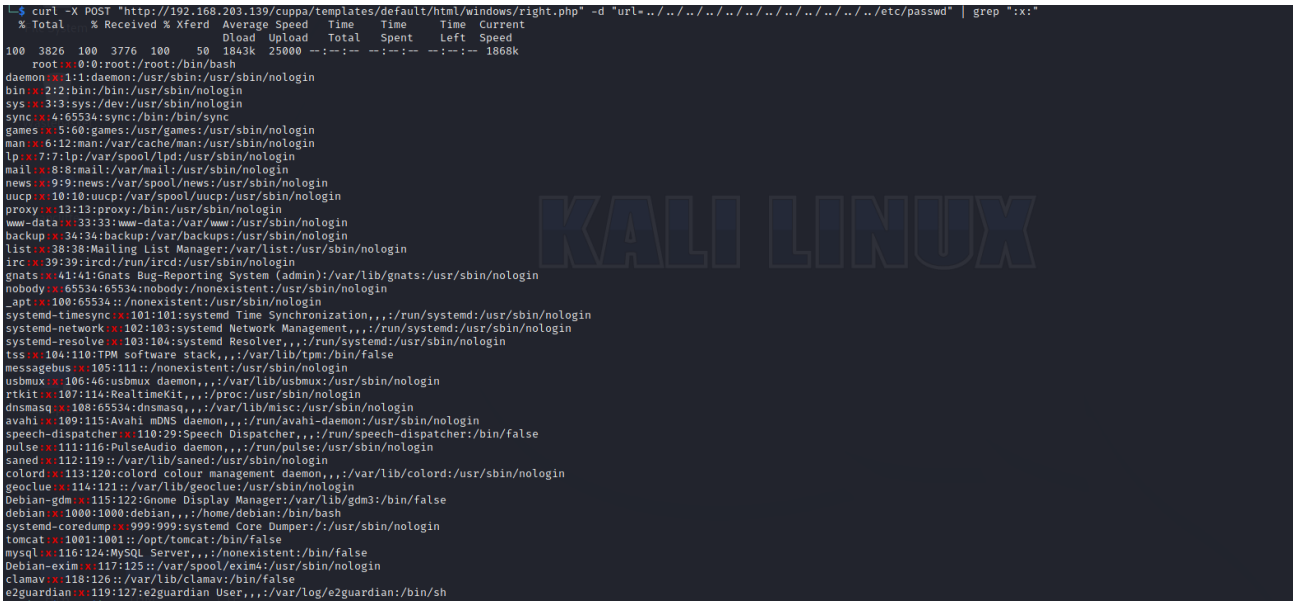
README.md

Local File Inclusion vulnerabilities in CuppaCMS templates

Vulnerability disclosed:

- CuppaCMS's latest github commit https://github.com/CuppaCMS/CuppaCMS/commit/4c9b742b23b924cf4c1f943f48b278e06a17e297 (dated Nov 12, 2019) and before (no version numbers) suffers from Local File Inclusion vulnerability, allowing access to system files. Script '/templates/default/html/windows/right.php' has parameter $_POST['url'] that is not sanitised properly. This allows access to arbitrary files on the server.

PoC:



Author: Mateo Hanžek

Reference: CuppaCMS/CuppaCMS#18
CVE-2022-34121