New issue

Jump to bottom

Code injection caused by arbitrary file editing vulnerability in taocms3.0.2 #28

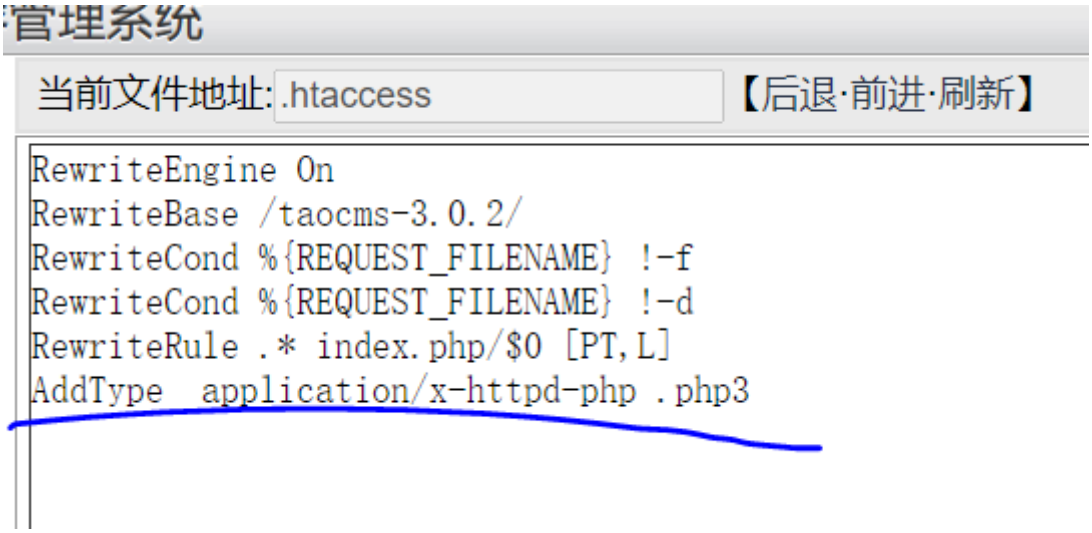
Open **debug601** opened this issue on Feb 18 · 0 comments

debug601 commented on Feb 18

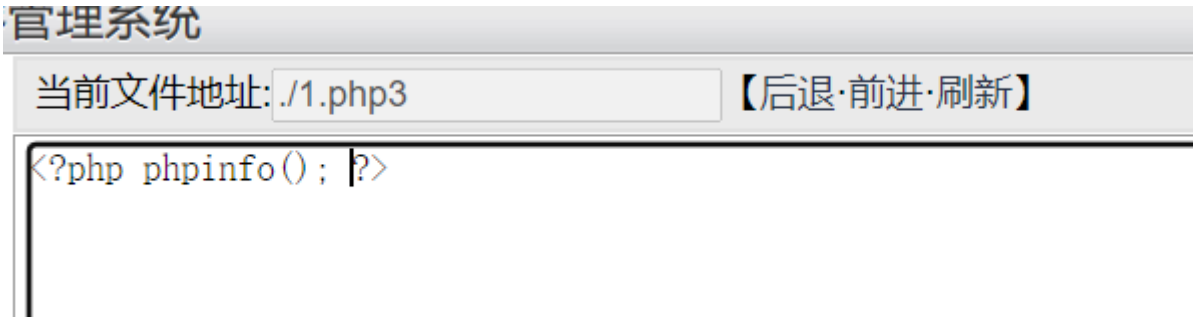
We click on file management to go to the management location of the website and directory.

Click to edit the .htaccess file and add a line at the end, 'AddType application/x-httpd-php.php3', click Save.

The function of the statement 'AddType application/x-httpd-php .php3' is to execute all files with the .php3 suffix as .php files.



We create a 1.php3 file and write''to 1.php3.



Visit the 1.php3 file in the directory of the website and find that it has been executed successfully. It's really great.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant