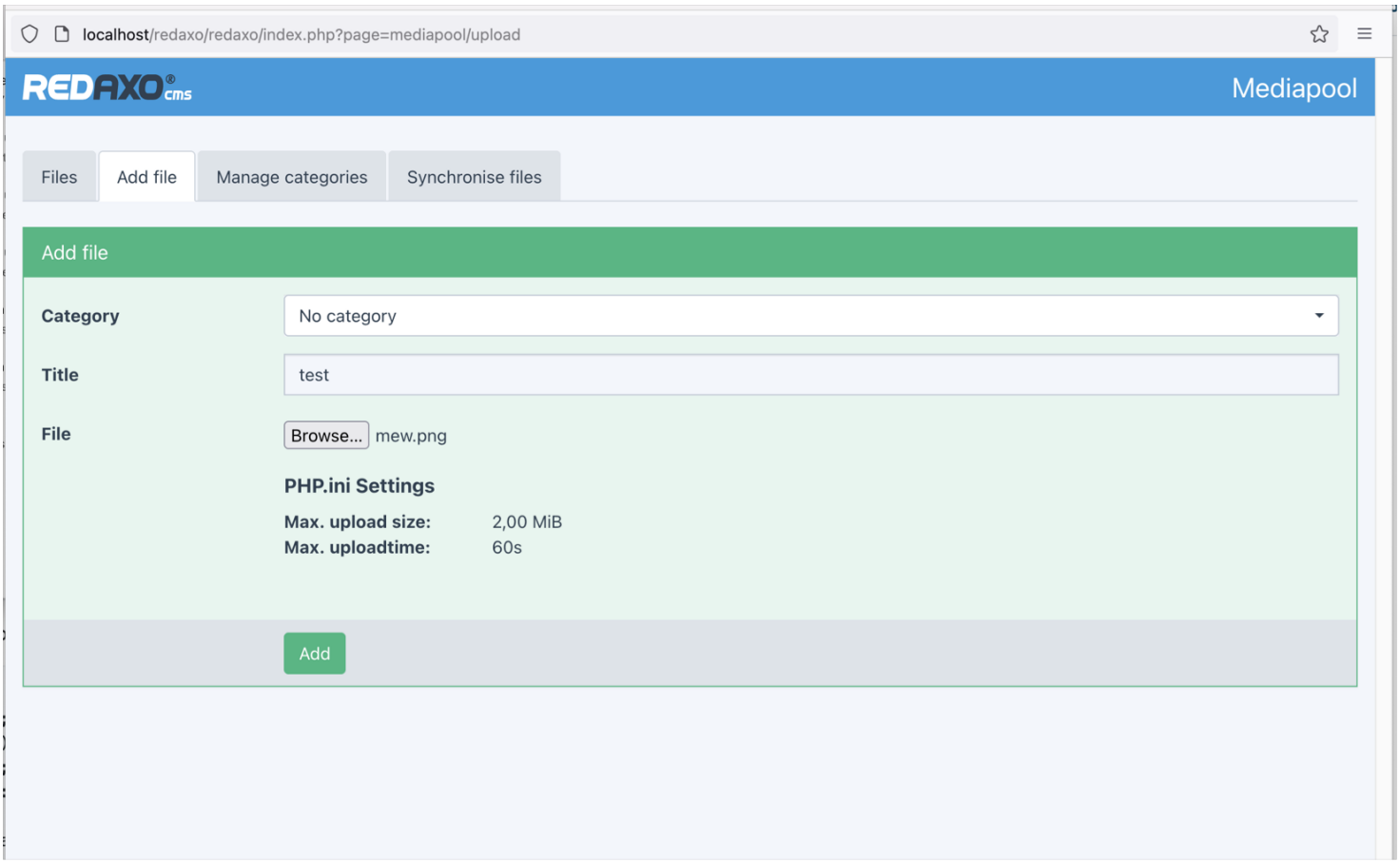
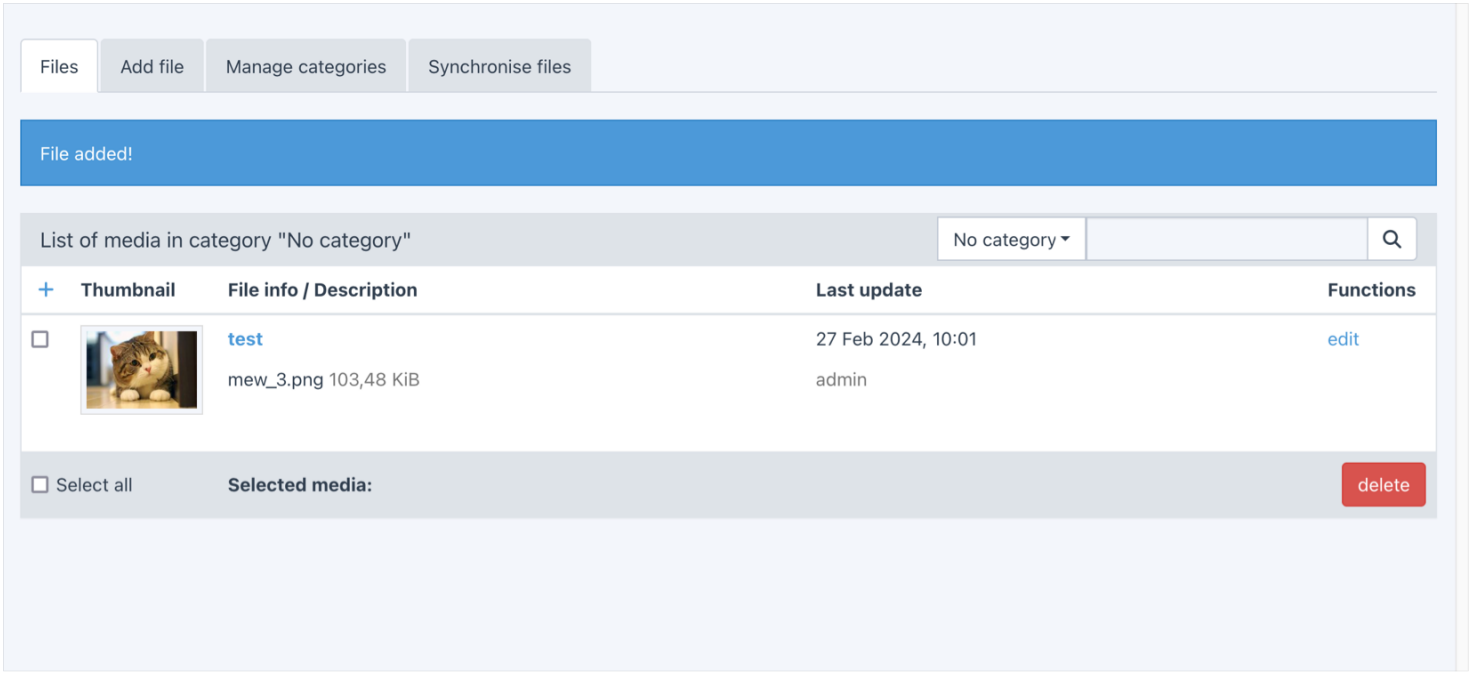
POC bug in REDAXO(cms) product:

During testing of your application, we identified a vulnerability in REDAXO that allows any file on the system to be deleted via the "delete media" feature by changing the file name "filename" via the "filename" function. function of "backup plugin".
The implementation process goes as follows:

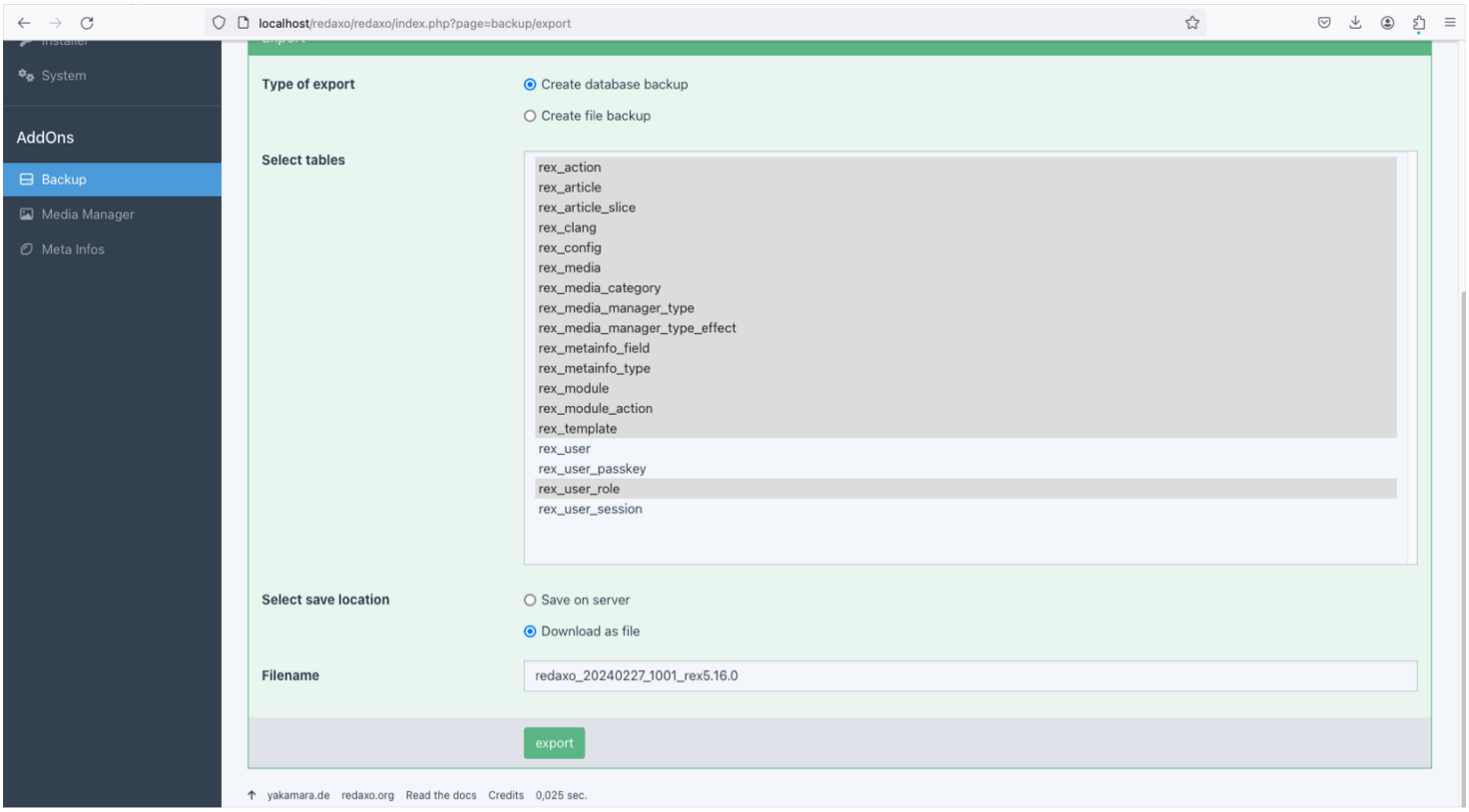
1. upload file mew.png with title="test"



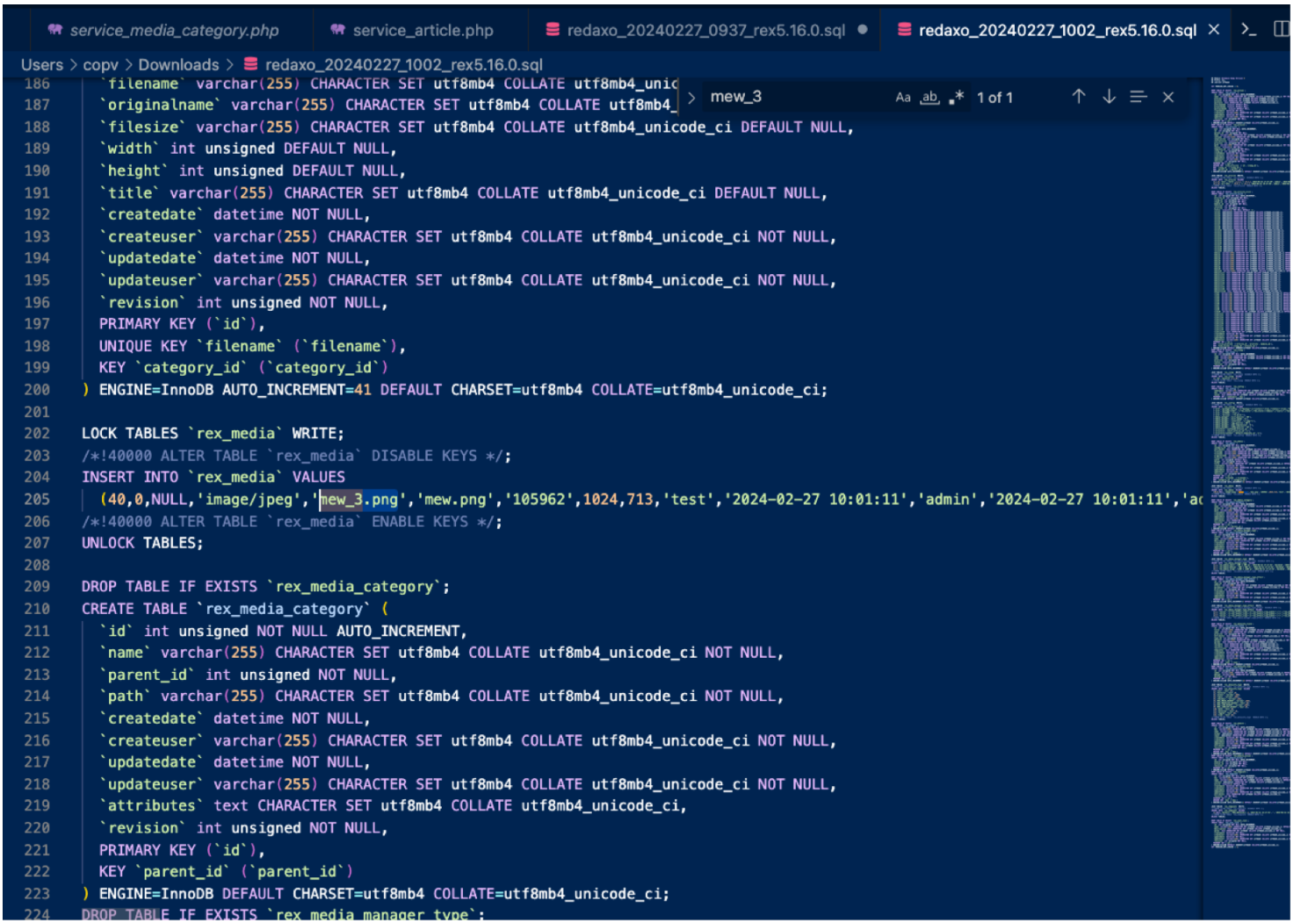
File *mew.png* was uploaded but renamed to *mew_3.png* because file *mew.png* already exists on my media folder.



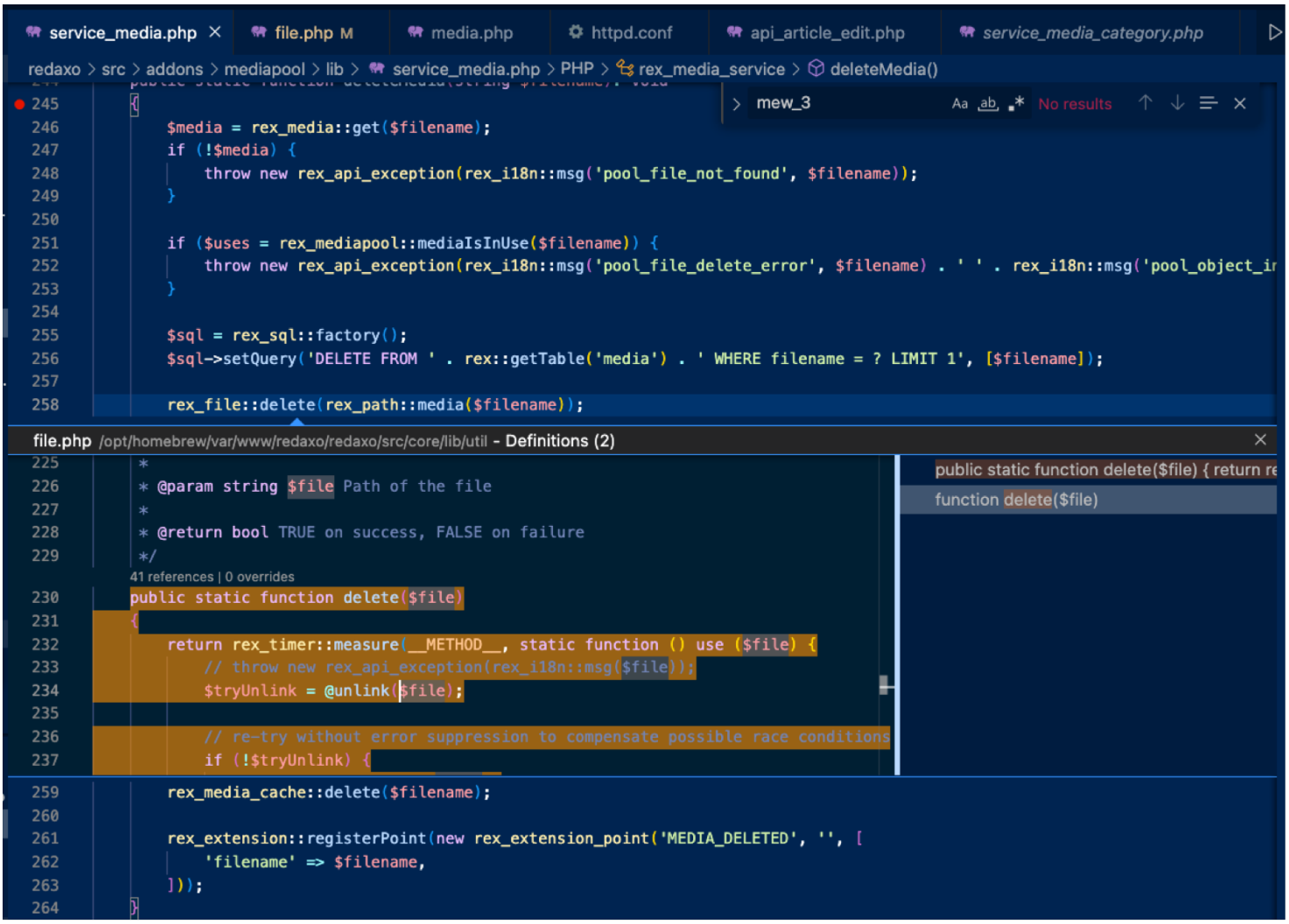
2. Perform data backup



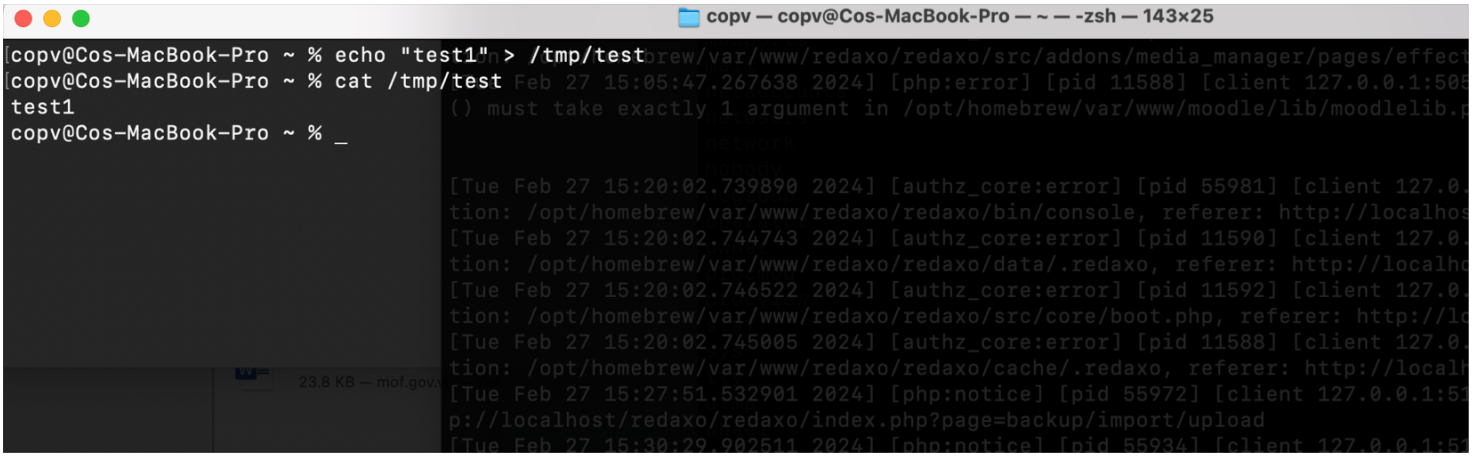
Reading the backup file I see mew_3.png



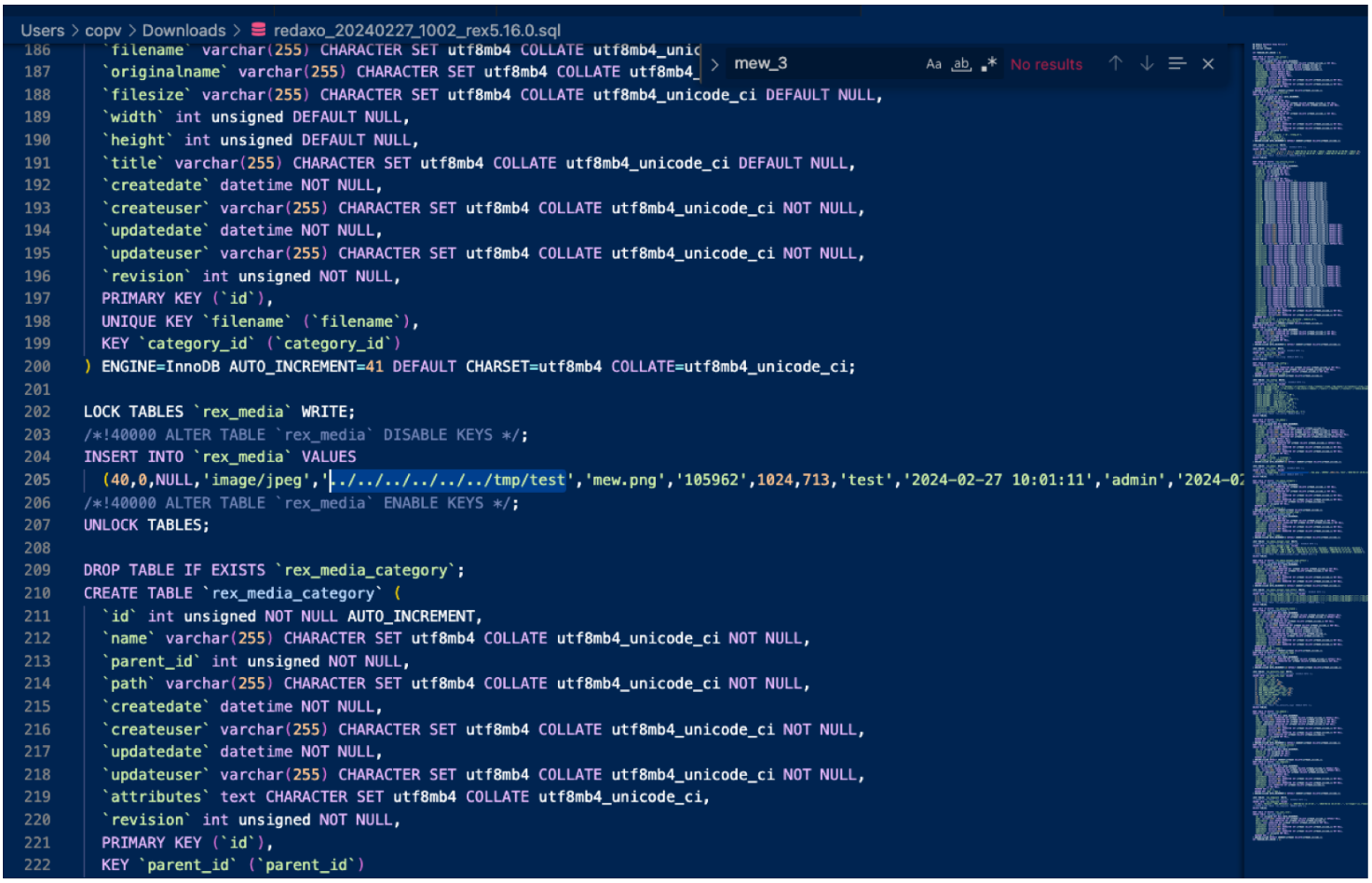
4. When I test the file deletion function, the unlink function deletes the file based on the $filename => when I rename the $filename, the path to delete the file will also change.



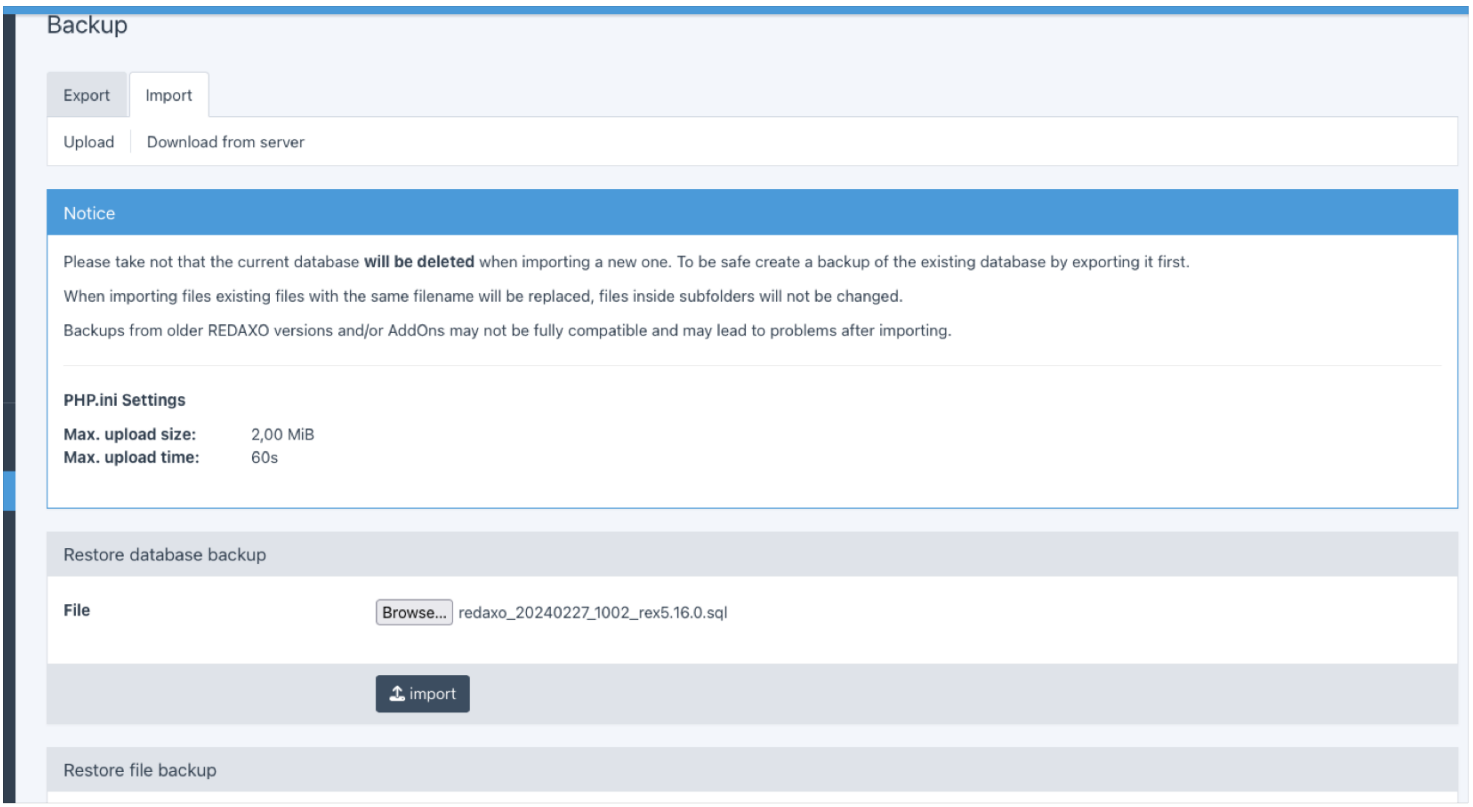
5. I created the file */tmp/test* with the information “test”



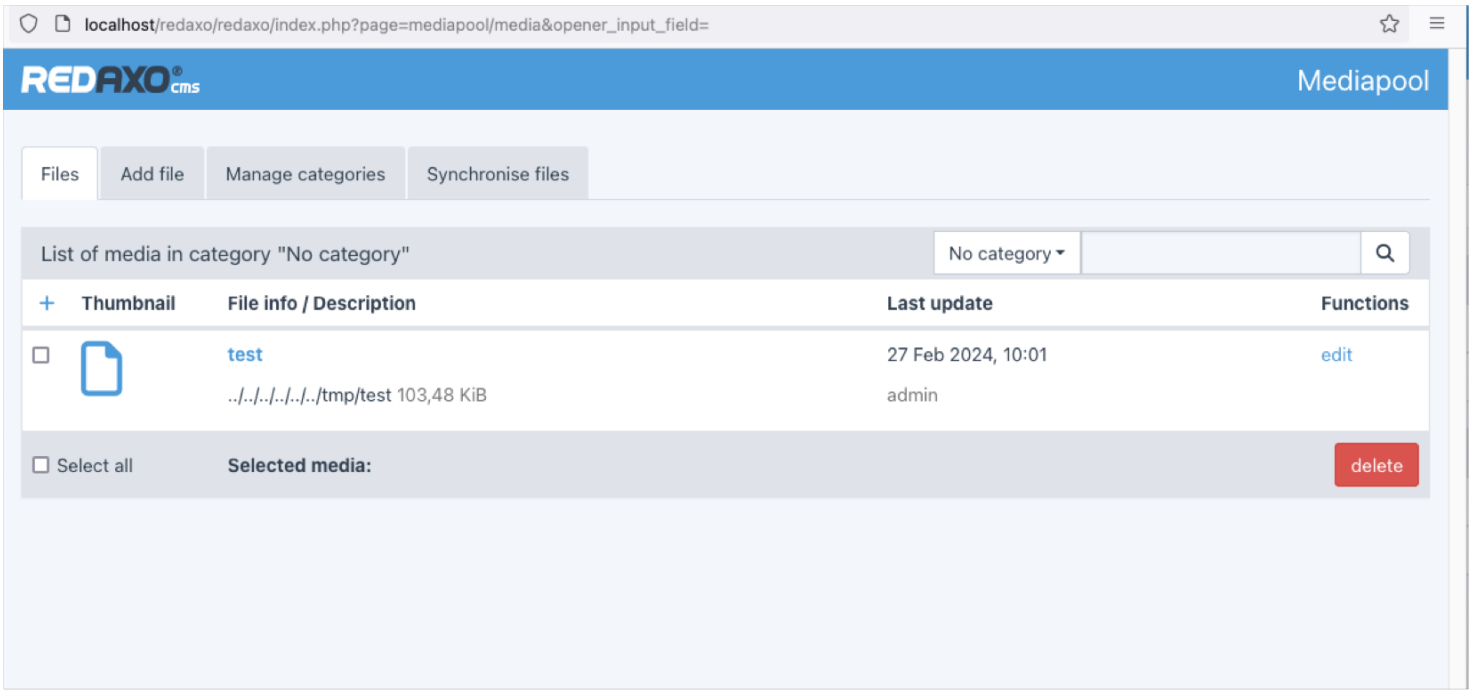
6. Change $filename in backup file from *mew_3.png* to *../../../../../../tmp/test*



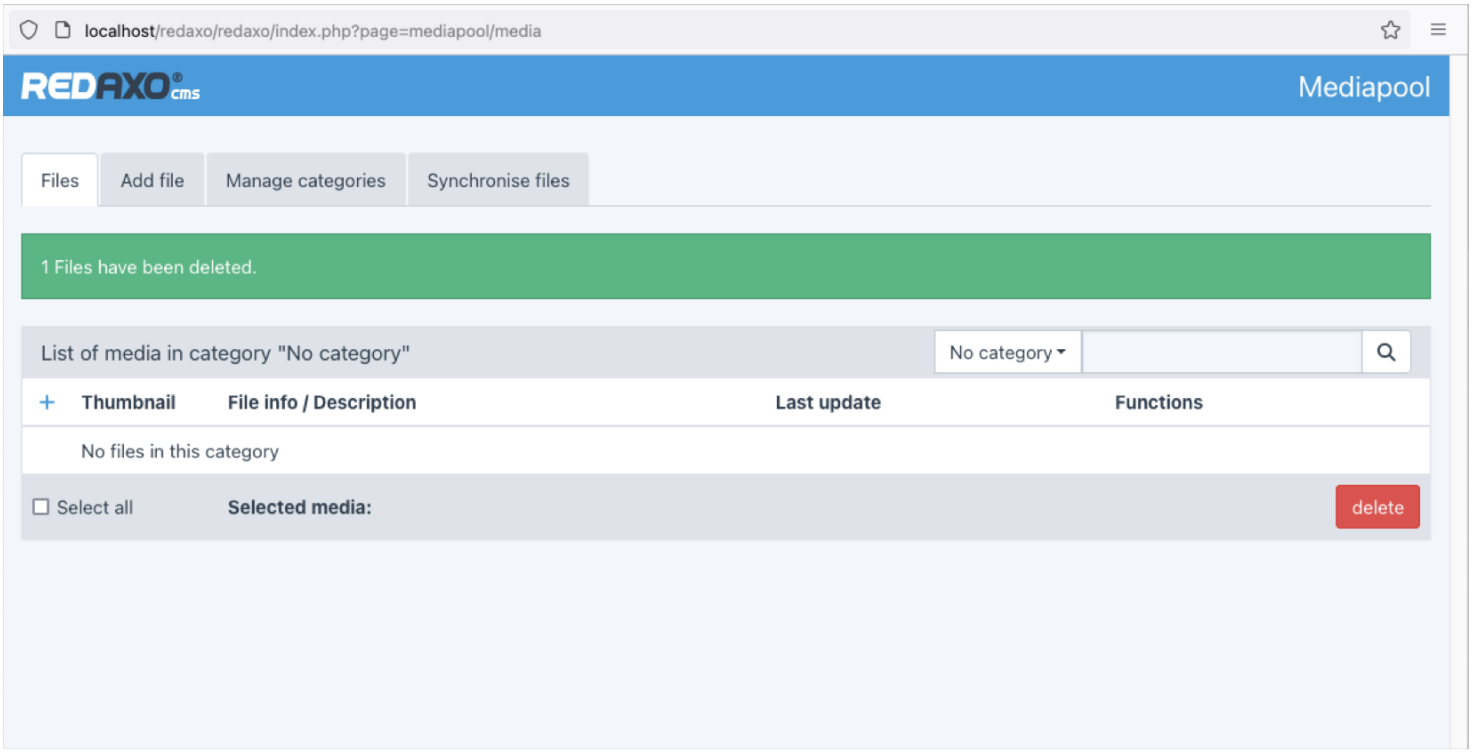
7. Back up data from the modified backup file.



8. Filename has been modified to *../../../../../../tmp/test*



9. Proceed to delete the file



10. My /tmp/test file has been deleted from the system.

Create by ***0xcopv***