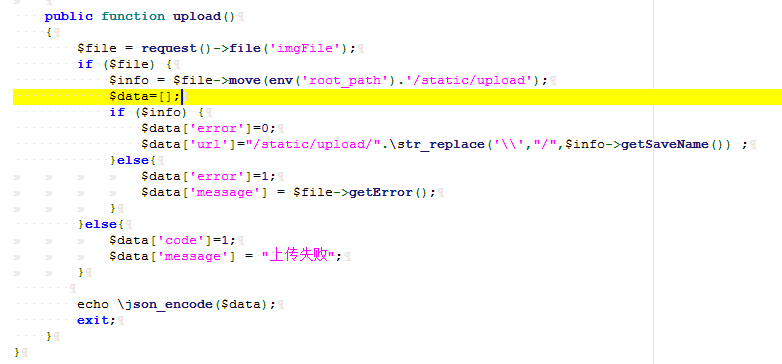
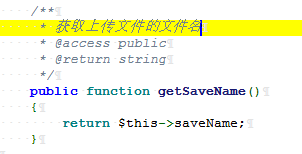
In / application / admin / controller/ Index.php The upload() function is used to move and judge the uploaded files. First, receive the request as imgfile (image upload), and then move the file to the directory of the website / static / upload /, and then use the getsavename function.



Check the move function and find that it is located in / ThinkPHP / library / think/ File.php The move function in is used to move files



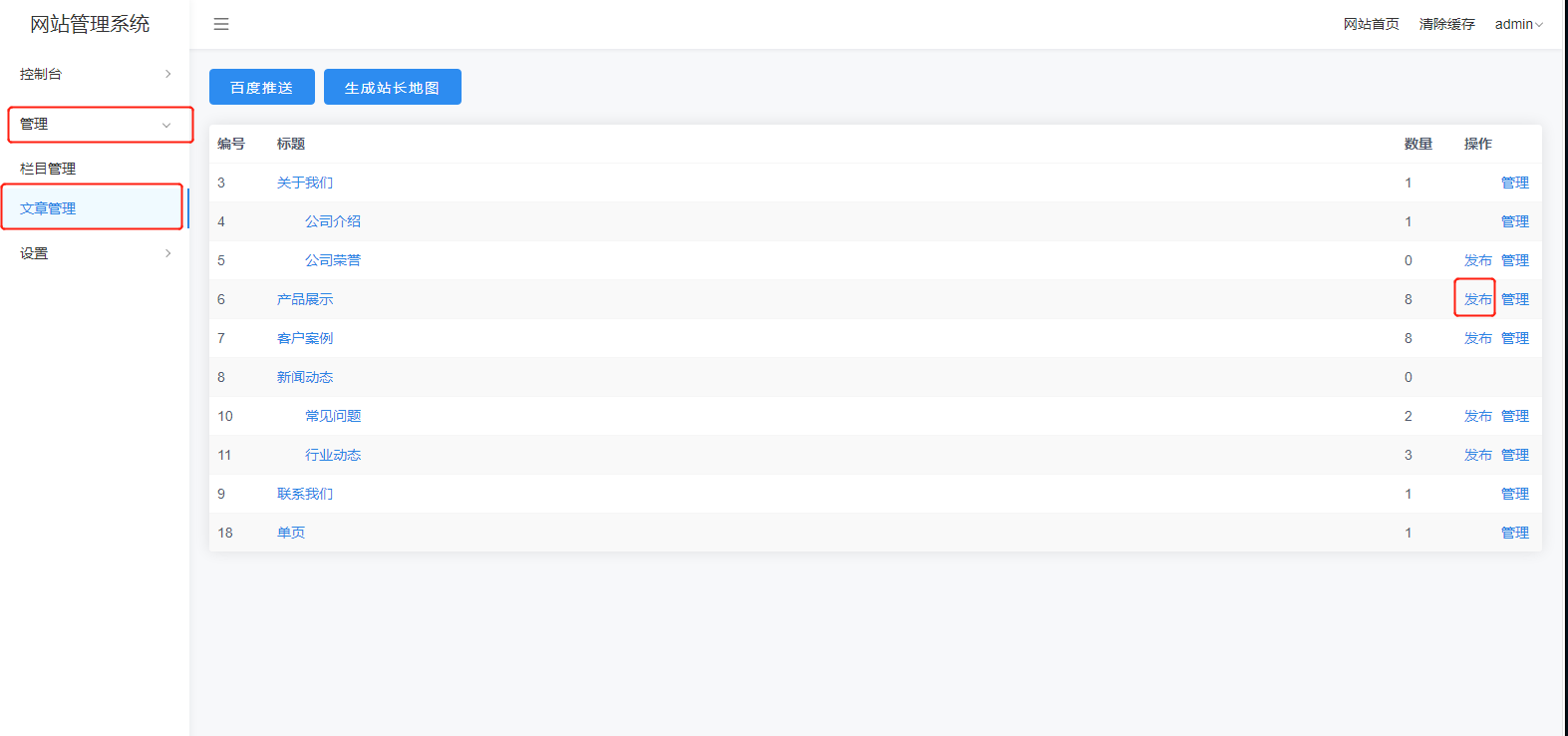
The getsavename function returns the file path directly.



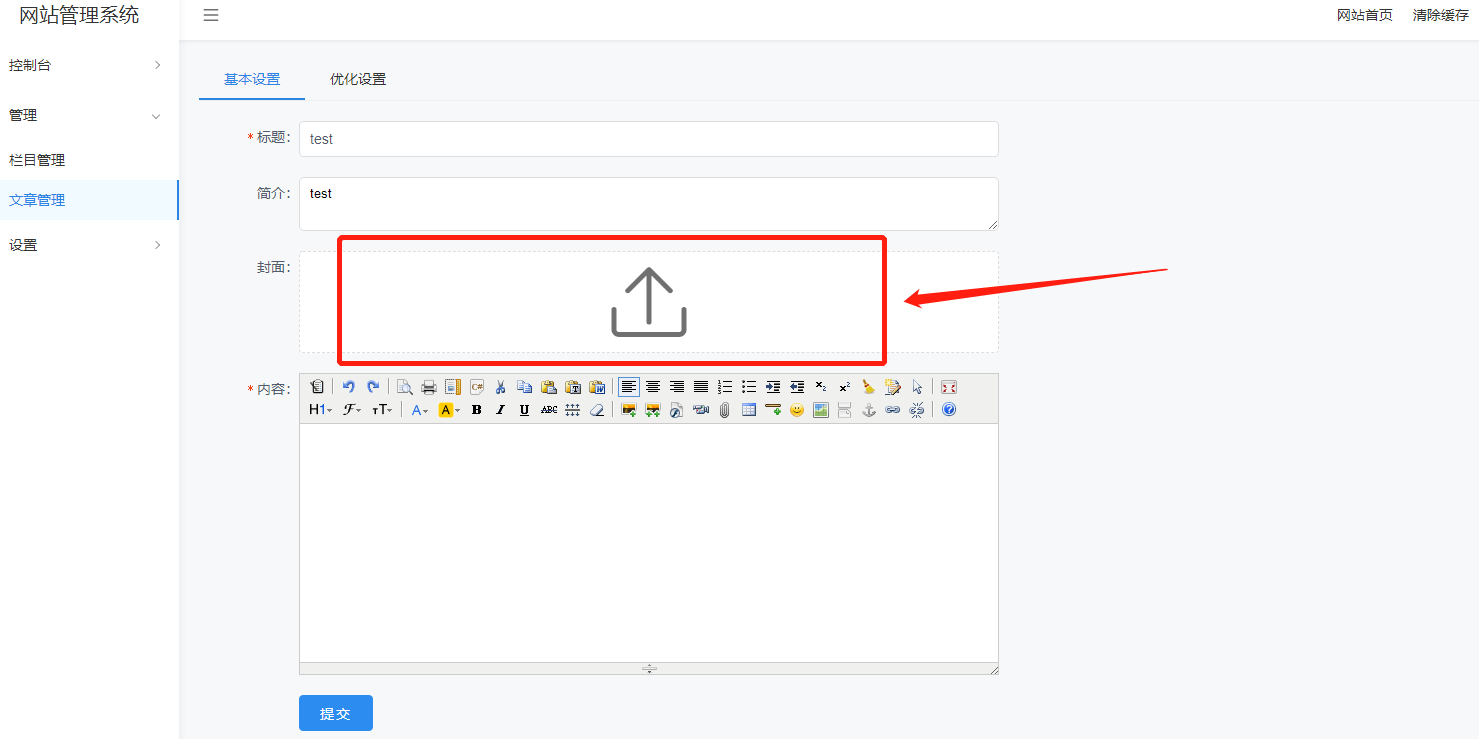
Conclusion:In the process of moving the file after uploading, the application does not judge the uploaded file, resulting in arbitrary file upload.

Test:

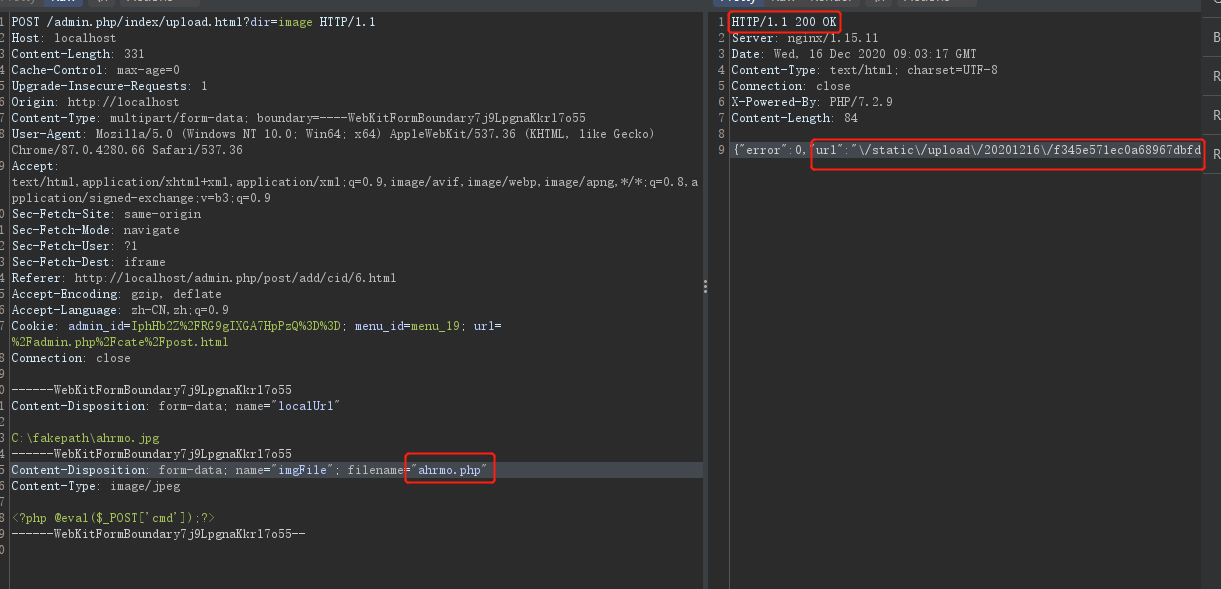
In the background > Management > Article Management > Publishing



Upload location



After uploading the. JPG suffix file, the packet is intercepted.



Although the prompt fails, the file exists. If you use the ant sword to connect, the connection is successful.

