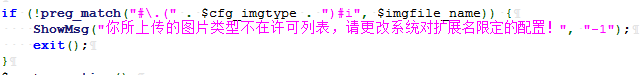
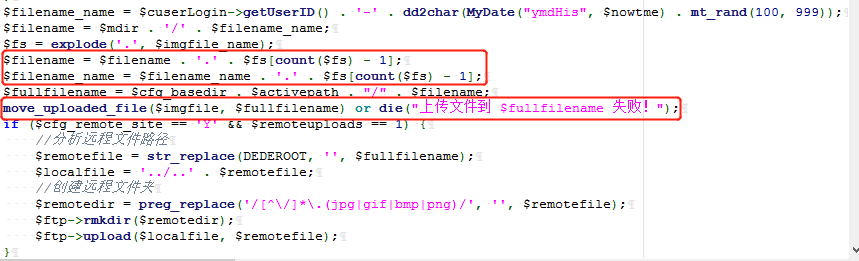
1、Code audit foundIn / Dede / dialog / select\_ images\_ post.php Replace the regular match in the file name with a blank



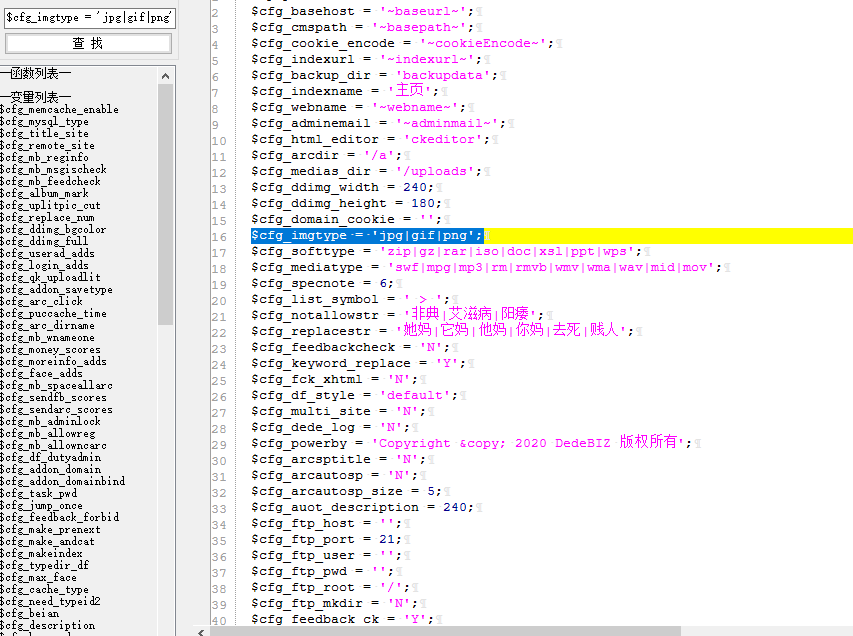
2、After that, whether there is a file format in the white list in the file name is retrieved. These two methods are not based on the suffix name of the file, so there is a problem of being bypassed



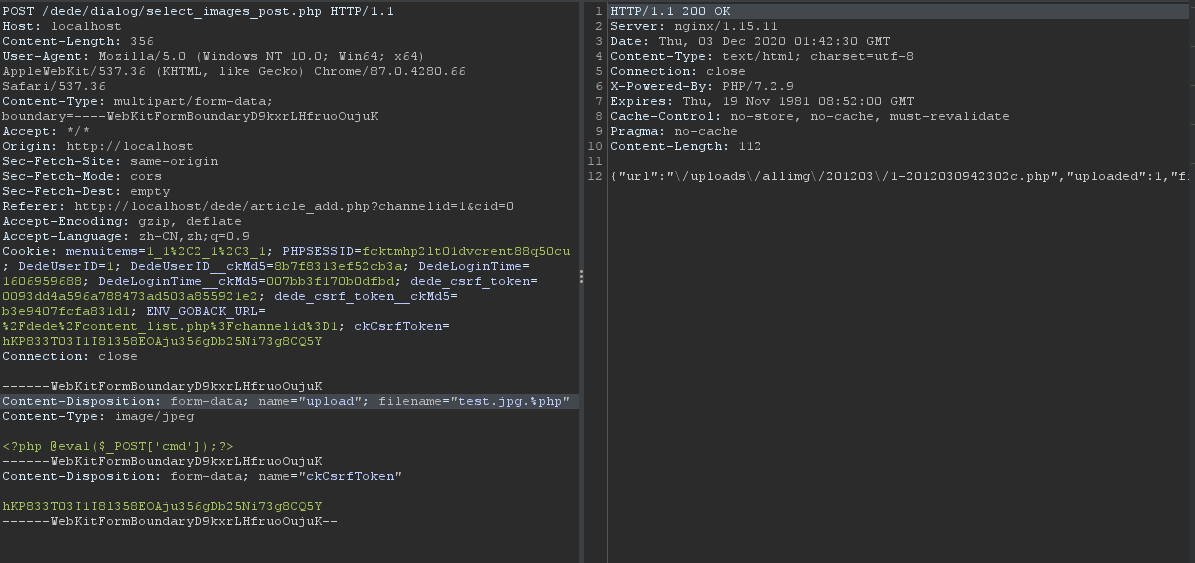
1. Take the suffix name of the file for splicing and uploading operations. There is a problem that the detection method is inconsistent with the upload file generation method, which leads to the bypass
2. We follow $CFG\_ Imgtype function



5、Follow $CFG\_ Imgtype comes to / install/ config.cache.inc . PHP, find the limitation of upload format



1. Finally, the uploaded file takes the suffix name of the file for splicing and uploading operations, so we can construct jpg.% PHP and other methods to bypass



**be careful**:The vulnerability is generated in the article editor. The test can be used in ordinary articles in the background. The member function needs to be opened in the foreground, and then the upload restriction can be bypassed in the editor of the member center