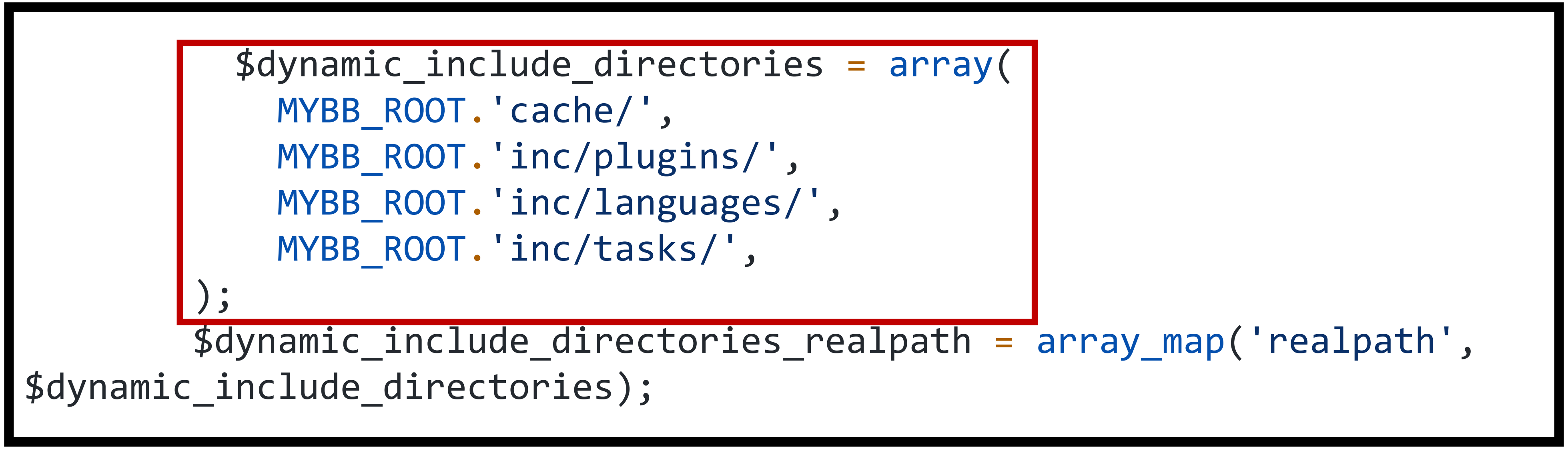
Mybb RCE in admin Panel

Contents

- LFI to RCE

1. BlackList Based Dir Check

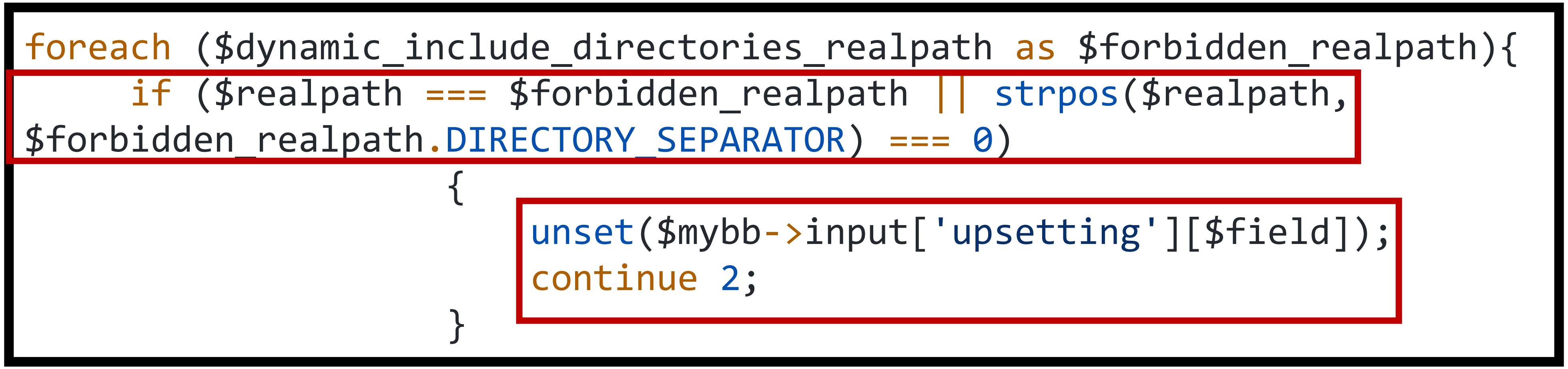


```
          $dynamic_include_directories = array(
            MYBB_ROOT.'cache/',
            MYBB_ROOT.'inc/plugins/',
            MYBB_ROOT.'inc/languages/',
            MYBB_ROOT.'inc/tasks/',
        );
        $dynamic_include_directories_realpath = array_map('realpath',
$dynamic_include_directories);
```

/Upload/admin/modules/config/settings.php 1172 ~ 1178 line

First, We can setting control upload directory in Mybb but there is a mitigation to prevent exploit
If you look at the code, there is a blacklist directory for each because if we can arbitrary file write
in this blacklist directory, very easy to remote code execution

2. Mitigation Analysis

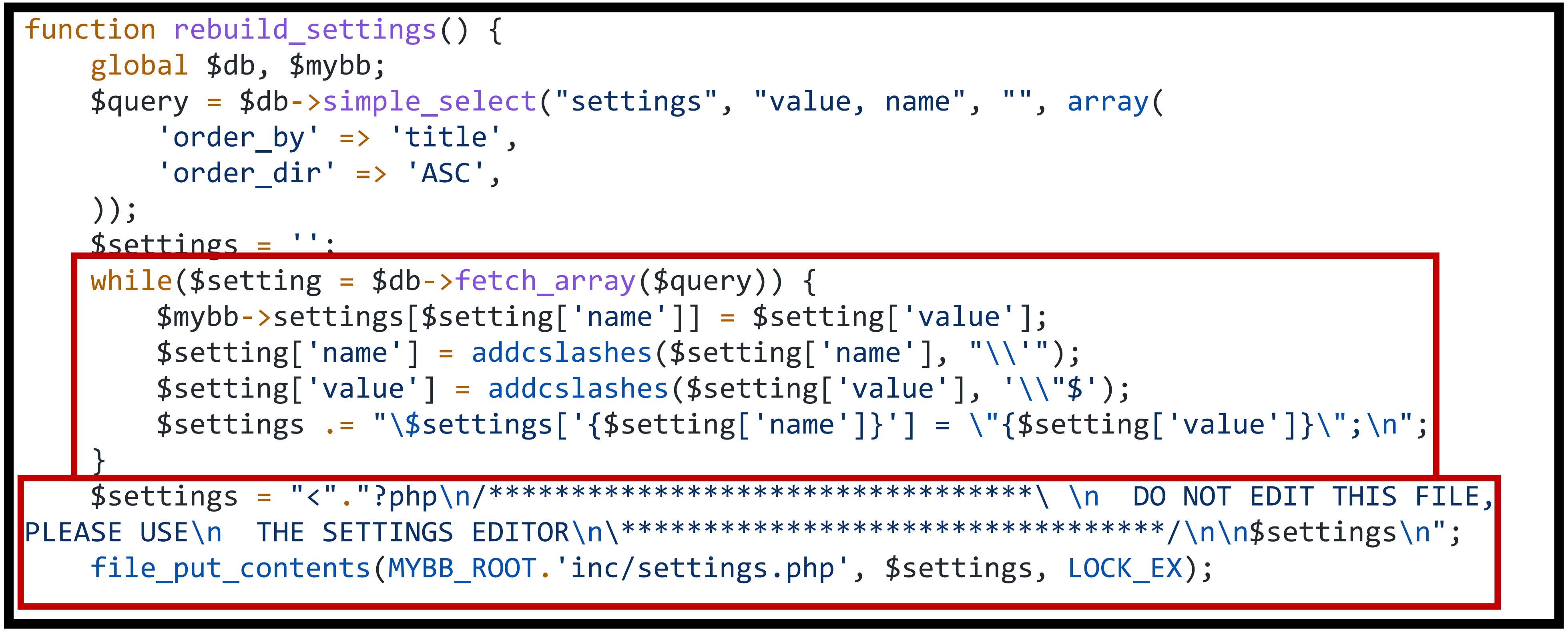


```
foreach ($dynamic_include_directories_realpath as $forbidden_realpath){
     if ($realpath === $forbidden_realpath || strpos($realpath,
$forbidden_realpath.DIRECTORY_SEPARATOR) === 0)
                    {
                         unset($mybb->input['upsetting'][$field]);
                         continue 2;
                    }
```

/Upload/admin/modules/config/settings.php 1200 ~ 1206 line

If you look at the code Compare the values of the previously created dynamic_include_directories_realpath array variable with the user input and unset them if they are the same This mitigation makes it difficult to change those settings to the previously described blacklist directory. However, paths other than the blacklist can be set

3. Rebuild settings function

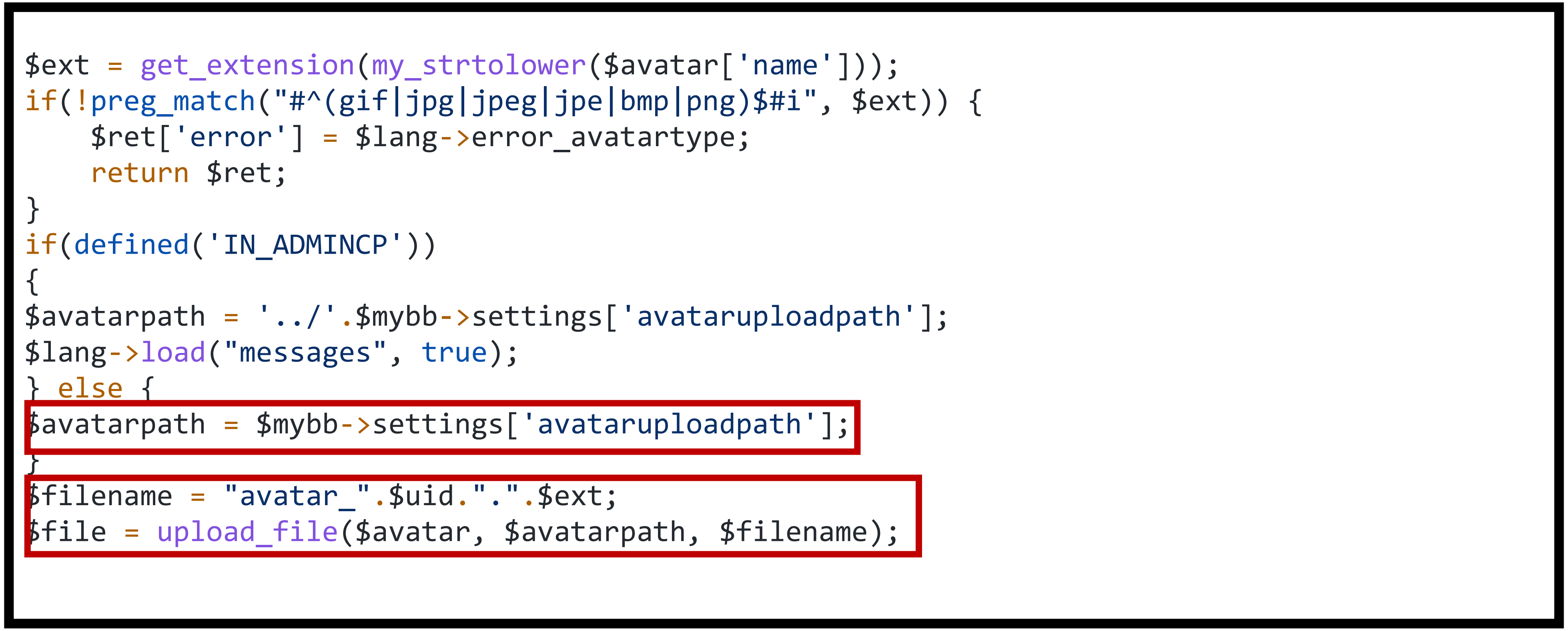


```php
function rebuild_settings() {
    global $db, $mybb;
    $query = $db->simple_select("settings", "value, name", "", array(
        'order_by' => 'title',
        'order_dir' => 'ASC',
    ));
    $settings = '';
    while($setting = $db->fetch_array($query)) {
        $mybb->settings[$setting['name']] = $setting['value'];
        $setting['name'] = addcslashes($setting['name'], "\\'");
        $setting['value'] = addcslashes($setting['value'], '\\"$');
        $settings .= "\$settings['{$setting['name']}'] = \"{$setting['value']}\";\n";
    }
    $settings = "<"."?php\n/*********************************\ \n  DO NOT EDIT THIS FILE,
PLEASE USE\n  THE SETTINGS EDITOR\n\*********************************/\n\n$settings\n";
    file_put_contents(MYBB_ROOT.'inc/settings.php', $settings, LOCK_EX);
```

/Upload/inc/functions.php 6967 ~ 6991 line

If the mitigation pass, the settings are saved in the database and the rebuild_settings function is called. The function searches the row in the database and is written in inc/settings.php.

4. Avatar Upload

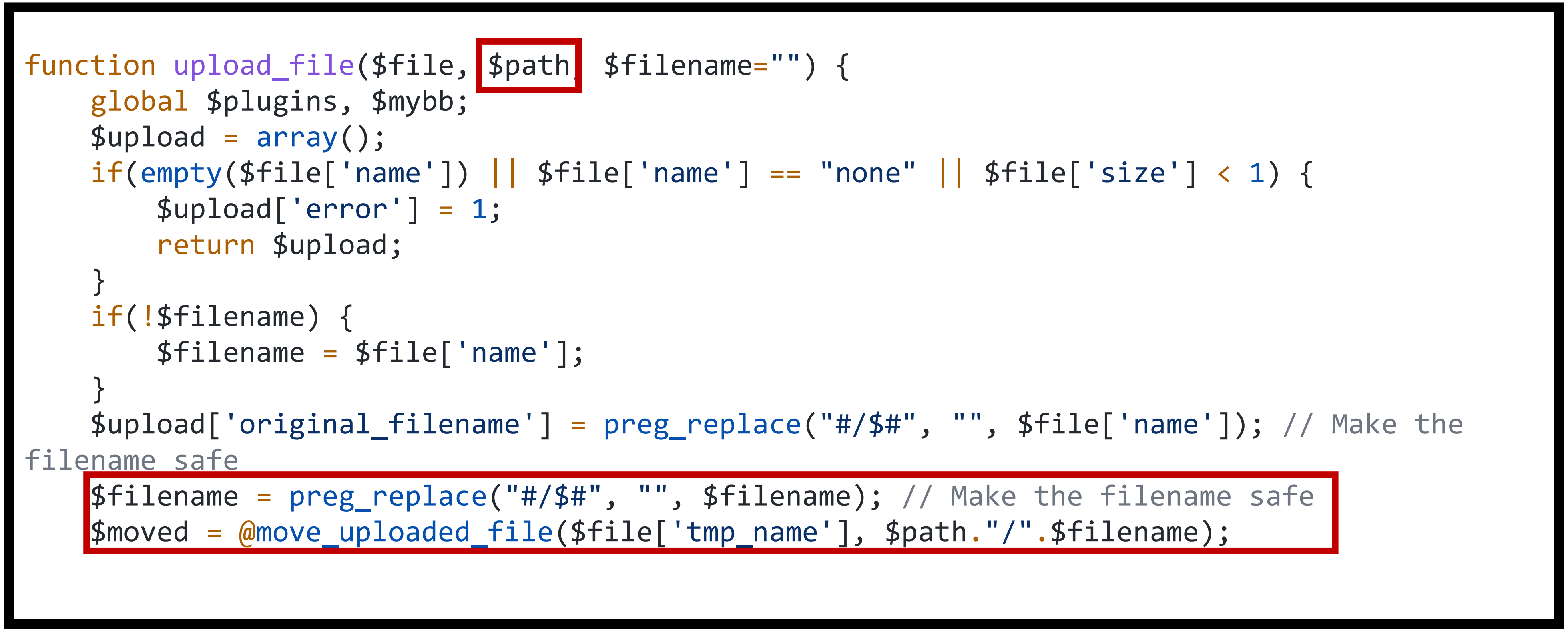


```
$ext = get_extension(my_strtolower($avatar['name']));
if(!preg_match("#^(gif|jpg|jpeg|jpe|bmp|png)$#i", $ext)) {
    $ret['error'] = $lang->error_avatartype;
    return $ret;
}
if(defined('IN_ADMINCP'))
{
$avatarpath = '../'.$mybb->settings['avataruploadpath'];
$lang->load("messages", true);
} else {
$avatarpath = $mybb->settings['avataruploadpath'];
}
$filename = "avatar_".$uid.".".$ext;
$file = upload_file($avatar, $avatarpath, $filename);
```

/Upload/inc/functions_upload.php 232 ~ 250 line

Because ./inc does not exist in the blacklist of settings.php , it can bypass the migration and when you look at the code, it uses the set path to upload the upload path. Therefore, we can write limited files in the inc directory.

5. Avatar Upload

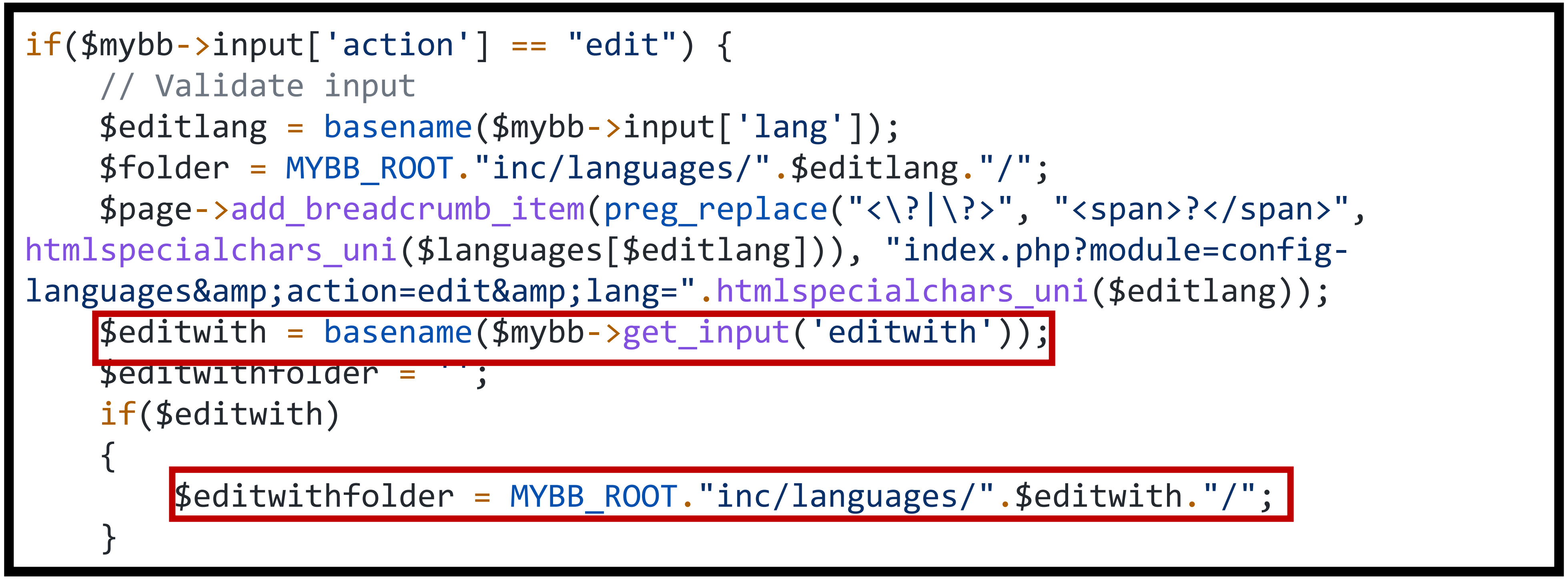


```php
function upload_file($file, $path, $filename="") {
    global $plugins, $mybb;
    $upload = array();
    if(empty($file['name']) || $file['name'] == "none" || $file['size'] < 1) {
        $upload['error'] = 1;
        return $upload;
    }
    if(!$filename) {
        $filename = $file['name'];
    }
    $upload['original_filename'] = preg_replace("#/$#", "", $file['name']); // Make the
filename safe
    $filename = preg_replace("#/$#", "", $filename); // Make the filename safe
    $moved = @move_uploaded_file($file['tmp_name'], $path."/".$filename);
```

/Upload/inc/functions_upload.php 926 ~ 945 line

When uploading avatar, upload it using the upload_file function, and at this time, my settings are entered in the $path variable.

6. LFI

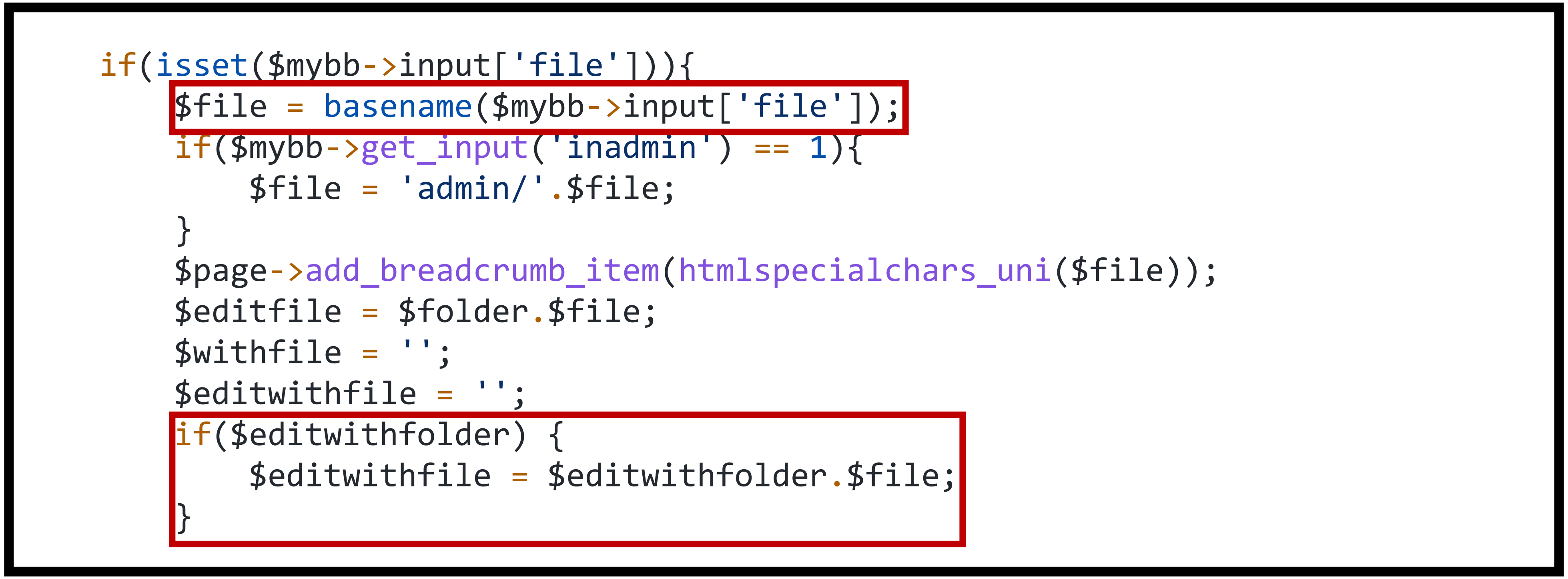


```
if($mybb->input['action'] == "edit") {
    // Validate input
    $editlang = basename($mybb->input['lang']);
    $folder = MYBB_ROOT."inc/languages/".$editlang."/";
    $page->add_breadcrumb_item(preg_replace("<\?|\?>", "<span>?</span>",
htmlspecialchars_uni($languages[$editlang])), "index.php?module=config-
languages&amp;action=edit&amp;lang=".htmlspecialchars_uni($editlang));
    $editwith = basename($mybb->get_input('editwith'));
    $editwithfolder = '';
    if($editwith)
    {
        $editwithfolder = MYBB_ROOT."inc/languages/".$editwith."/";
    }
```

/Upload/admin/modules/config/languages.php 375~389 line

If you look at the code, you set the user input with the basename applied to the editwith variable, and if editwith is not null, declare the editwithfolder variable to set the directory

7. LFI

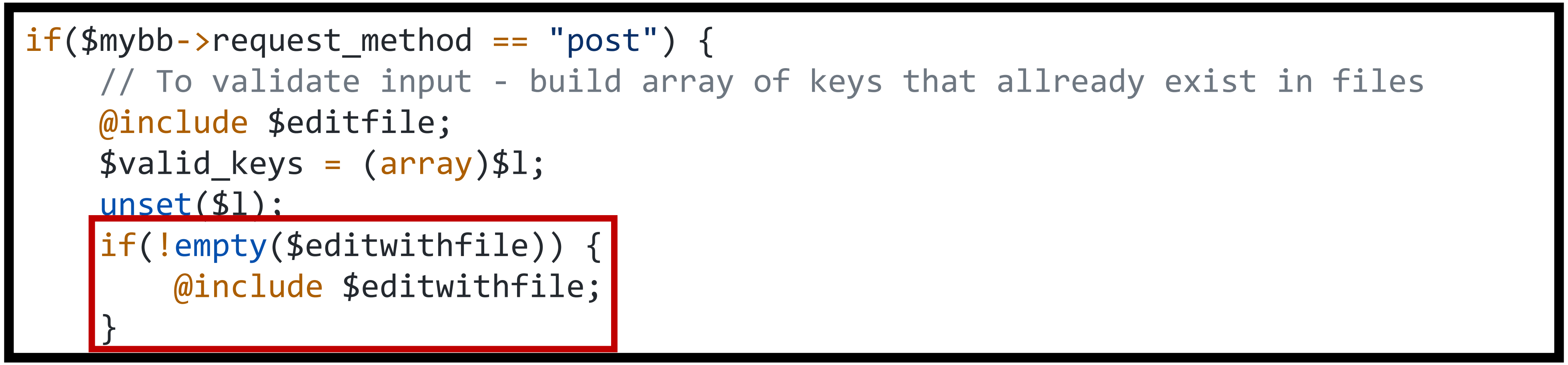


```
if(isset($mybb->input['file'])){
    $file = basename($mybb->input['file']);
    if($mybb->get_input('inadmin') == 1){
        $file = 'admin/'.$file;
    }
    $page->add_breadcrumb_item(htmlspecialchars_uni($file));
    $editfile = $folder.$file;
    $withfile = '';
    $editwithfile = '';
    if($editwithfolder) {
        $editwithfile = $editwithfolder.$file;
    }
```

/Upload/admin/modules/config/languages.php 375~389 line

And If the file user input exists, create a variable called file using the basename function, and create the editwithfile variable by combining the previously declared editwithfolder variable and the file variable.

8. LFI



```php
if($mybb->request_method == "post") {
    // To validate input - build array of keys that allready exist in files
    @include $editfile;
    $valid_keys = (array)$l;
    unset($l);
    if(!empty($editwithfile)) {
        @include $editwithfile;
    }
```

/Upload/admin/modules/config/languages.php 439~451 line

Look at the code. If the request method is , the editfile variable and editwithfile variable are called through the include function, and the editwithfile variable has the value I set, so you can see that Local File Inclusion exploitation is possible.