

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

Project: ms-mcms

Decompiled class file, bytecode version: 52.0 (Java 8)

```
@PostMapping("/{writeFileContent"})
@ResponseBody
public ResultData writeFileContent(@ApiIgnore ModelMap model, Http
String fileName = request.getParameter("fileName");
if (!this.checkFileType(fileName)) {
return ResultData.build().error();
} else {
String oldFileName = request.getParameter("oldFileName");
String fileContent = request.getParameter("fileContent");
this.LOG.debug(template);
FileWriter.create(new File(template)).write(fileContent);
if (!fileName.equals(oldFileName)) {
File newName = new File(template);
File oldName = new File(BasicUtil.getRealTemplatePath(oldName));
oldName.renameTo(newName);
FileUtil.del(BasicUtil.getRealTemplatePath(oldName));
return ResultData.build().success();
} else {
return ResultData.build().error();
}
}
```

Run: MSApplication

Console

2022-01-18 11:21:25.878 [INFO] 9428 [nio-8081-exec-1] org.apache.catalina.core.ContainerBase.[tomcat].[localhost].[/]:175 : Initializing Spring DispatcherServlet 'dispatcherServlet'

2022-01-18 11:21:25.878 [INFO] 9428 [nio-8081-exec-1] org.springframework.web.servlet.DispatcherServlet:157 : Initializing Servlet 'dispatcherServlet'

2022-01-18 11:21:26.286 [DEBUG] 9428 [nio-8081-exec-2] net.singsoft.basic.dao.IAppDao:68 : Cache Hit Ratio [net.singsoft.basic.dao.IAppDao]: 0.0

CLA

Gitee 已支持 CLA 协议签署

🔥 第三方功能集成, 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

效果演示

使用bp抓包发送payload

Burp Suite Community Edition v2020.2.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options APIH2 log4j2 RCE

Send Cancel < >

Request

Raw Params Headers Hex

File: /usr/share/ssl/certs/ca-certificates.crt

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,en-US;q=0.5,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 205

Cache-Control: no-cache

Pragma: no-cache

Host: localhost:8081

Origin: http://localhost:8081

Connection: close

Referer: http://localhost:8081/ms-template/115.do?template=/default

Cookie: JSESSIONID=2F8A892024680E30E1EE5E921915D9; Path=/; HttpOnly

Set-Cookie: JSESSIONID=2F8A892024680E30E1EE5E921915D9; Path=/; HttpOnly

Content-Disposition: inline; filename=rce

Content-Type: application/json

Date: Mon, 10 Jan 2022 09:25:22 GMT

Connection: close

Content-Length: 26

["result":true,"code":200]

Response

Raw Headers Hex

1 HTTP/1.1 200

2 Set-Cookie: JSESSIONID=2F8A892024680E30E1EE5E921915D9; Path=/; HttpOnly

3 Content-Disposition: inline; filename=rce

4 Content-Type: application/json

5 Date: Mon, 10 Jan 2022 09:25:22 GMT

6 Connection: close

7 Content-Length: 26

8

9 ["result":true,"code":200]

查看目录发现恶意文件成功写入

ms-mcms D:\IdeaProjects\ms-mcms

bin

doc

log

src

target

任意文件写

模板修改rce

.gitignore

evil

LICENSE

pom.xml

README.md

模板修改rce.zip



lz2y&r2 created **任务** 11 months ago



铭飞 10 months ago

感谢对开源产品的关注与支持，本月会全部同步更新



铭飞 changed **issue state** from **进行中** to **已完成** 10 months ago

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](#)

[eneration logs](#)

...

[Sign in](#) to comment



©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](#)

