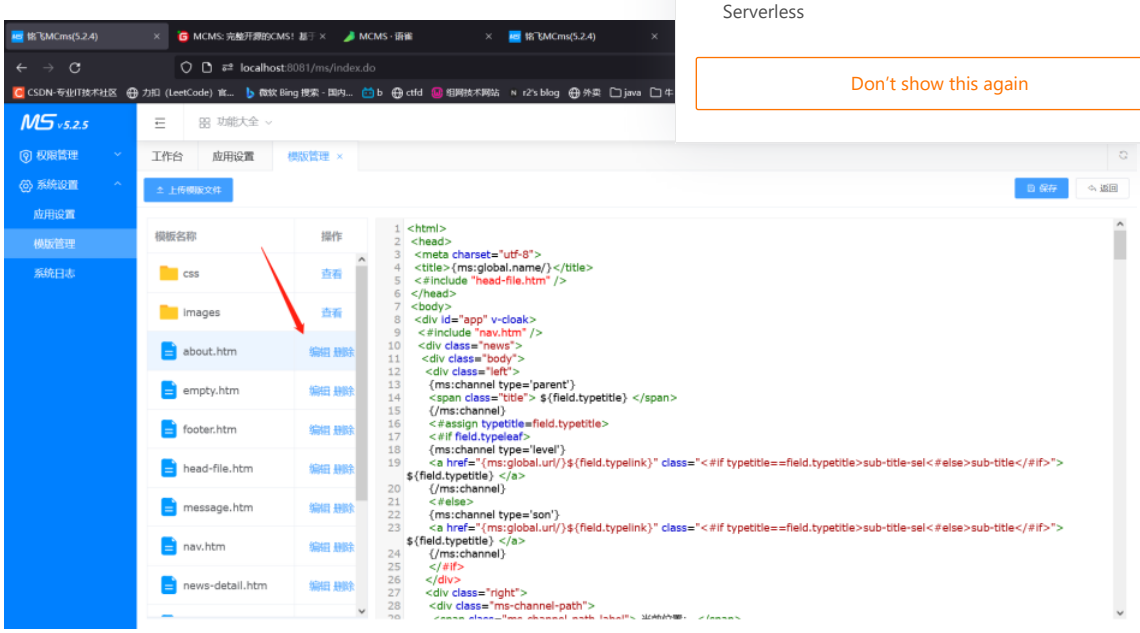
MCMS存在文件上传漏洞

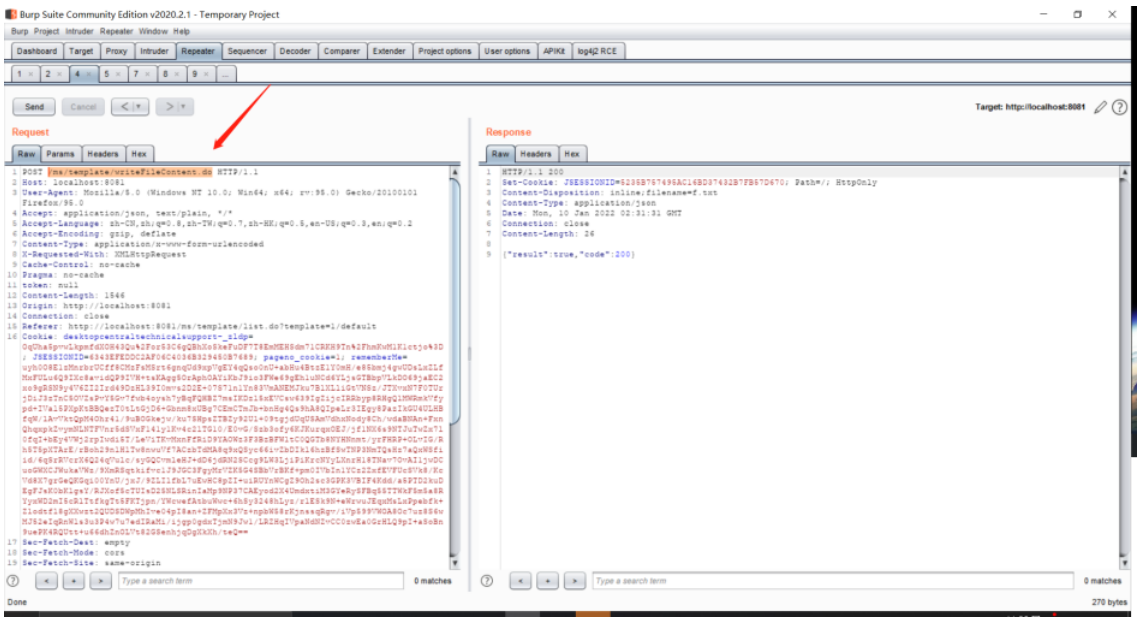
Done #I4Q4PX lz2y&r2 Opened this issue 2022-01-10 14:17

审计过程

后台提供了模板编辑功能



抓包发现，点击保存后，向后端 `/ms/template/writeFileContent.do` 发起了请求



跟一下后端代码，后端代码很简单，直接获取post的文件内容和文件名，然后创建文件并写入内容。正是这里存在任意文件写入漏洞，如果攻击者使用 `../` 进行目录穿越，则可以向靶机任意目录写入文件

Status
Done

Assignees
Not set

Labels
Not set

Milestones
5.2.6

Pull Requests
None yet
Successfully merging a pull reque
issue.

Branches
No related branch

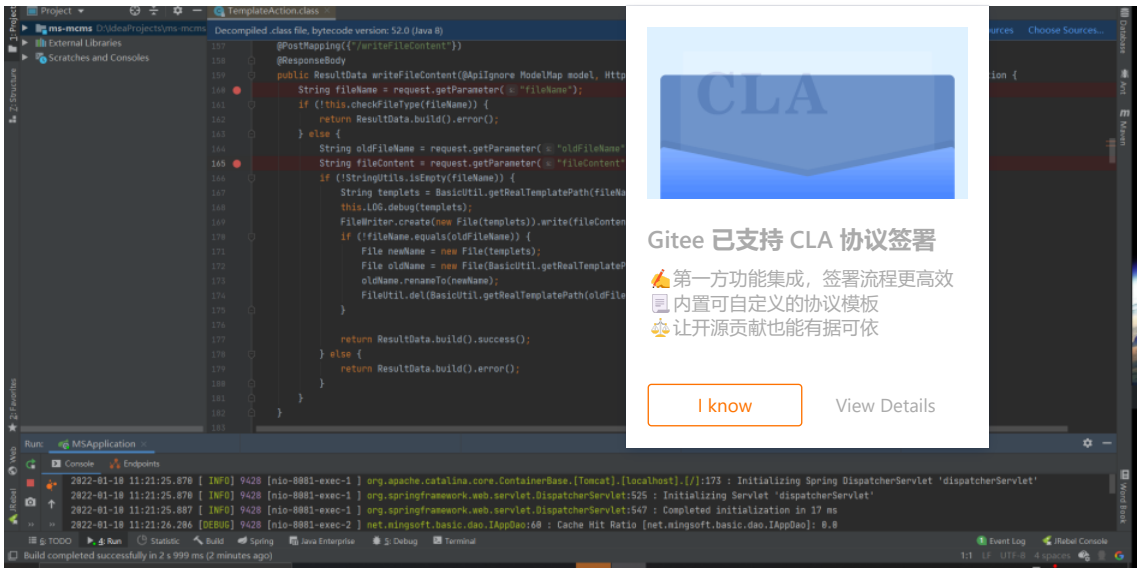
Planed to start - Planed t

Unscheduled - Unschedule

Top level
Not Top

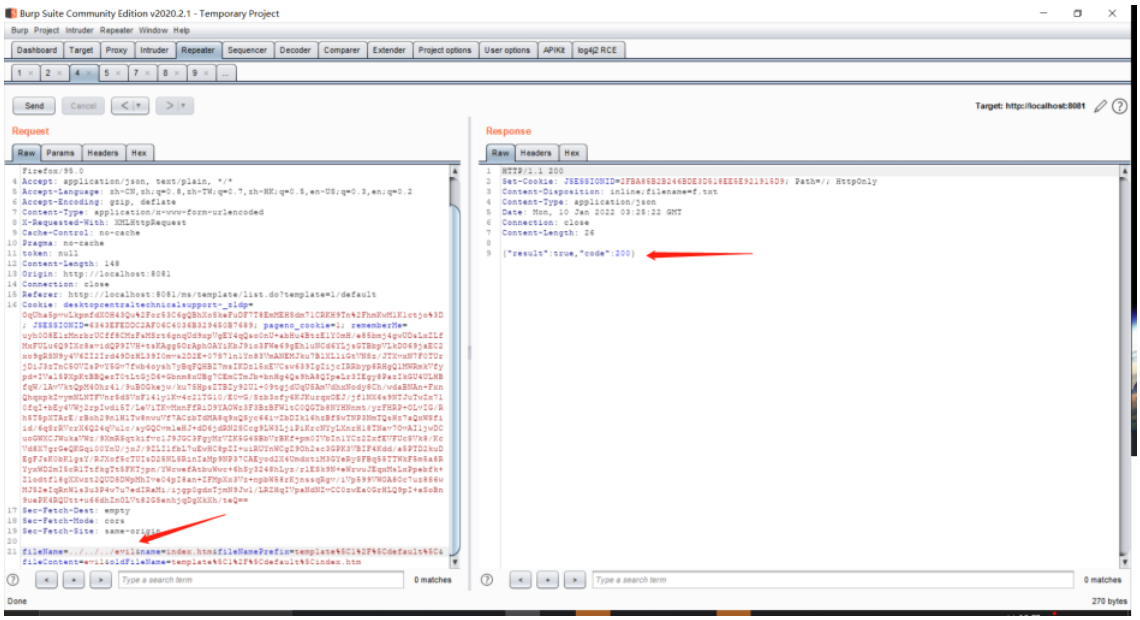
Priority
Not specified

参与者 (2)

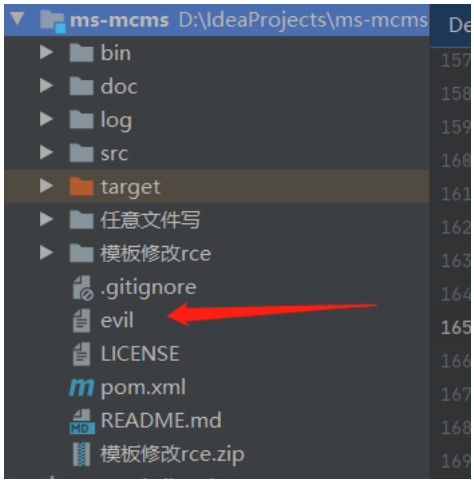


效果演示

使用bp抓包发送payload



查看目录发现恶意文件成功写入



```
172
173
174
175
```


lz2y&r2 created **任务** 11 months ago

eration logs

铭飞 owner 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

Sign in to comment