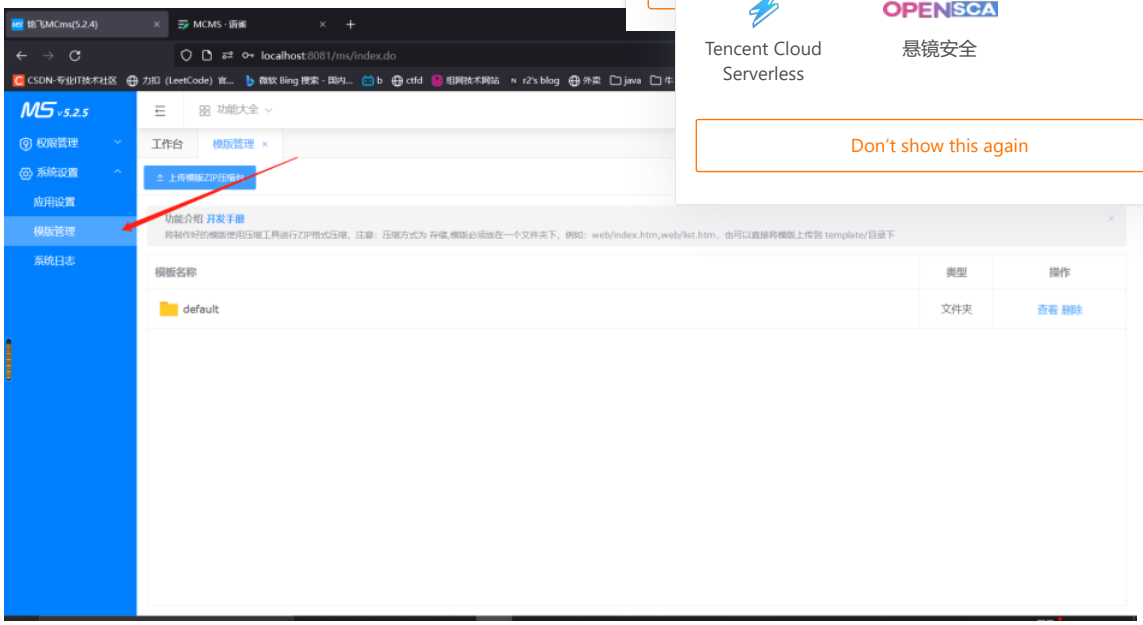
Issues / 详情

MCMS存在命令执行漏洞【模板修改】

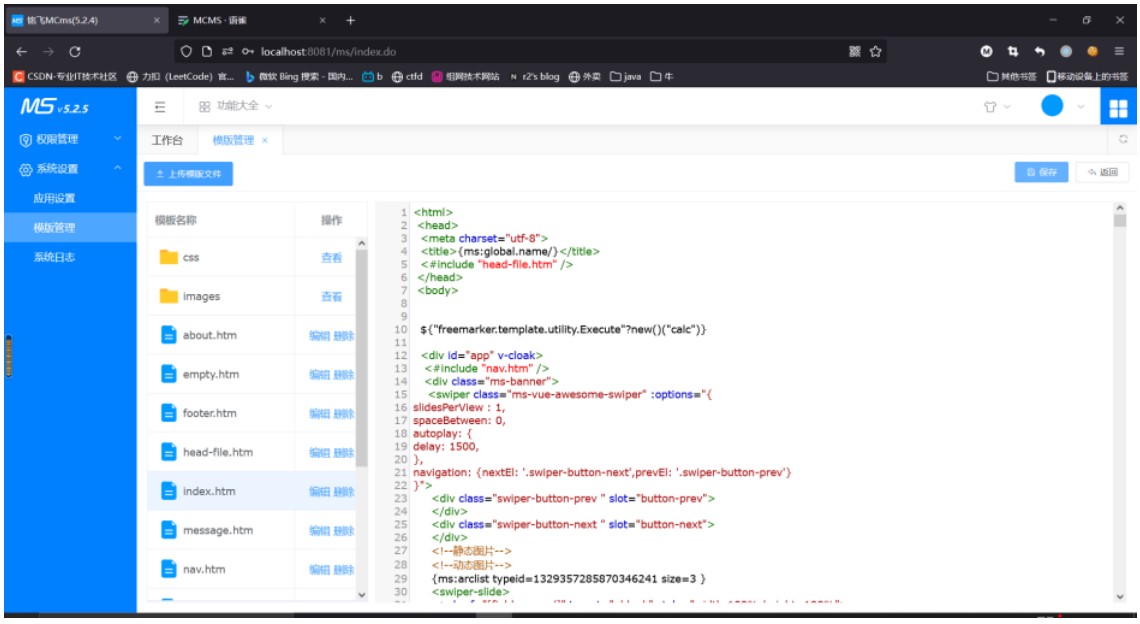
Done #I4Q4M6 lz2y&r2 Opened this issue 2022-01-10 14:1

在MCMS后台中存在模板管理功能，允许我们修改模板



查看源码后发现，MCMS使用的模板引擎为freemaker，因此我们可以构造对应的payload来进行ssti，修改index.htm的内容，添加如下payload

```
${"freemarker.template.utility.Execute"?new()("calc")}
```



点击保存后，访问http://localhost:8081/mcms/index.do，发现计算器弹出，验证了此处存在命令执行漏洞

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)

lz2y&r2 created **任务** 11 months ago Expand operation 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，像这类后台管理的问题。有处理意见？（如果后台管理员故意恶搞系统那不是分分钟的事，外部是不可能产生这个效果）

lz2y&r2 Reply **铭飞** owner 10 months ago

你好，建议安装完成后强制更改后台账号密码，由于默认密码和弱密码的存在，进入后台也未必是件难事。像模板注入这种类型的漏洞的确不太好修复，建议通过一定机制降低后台管理被恶意进入的可能性。但是如果其他漏洞是可以避免的还是建议修复一下

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

Sign in to comment