



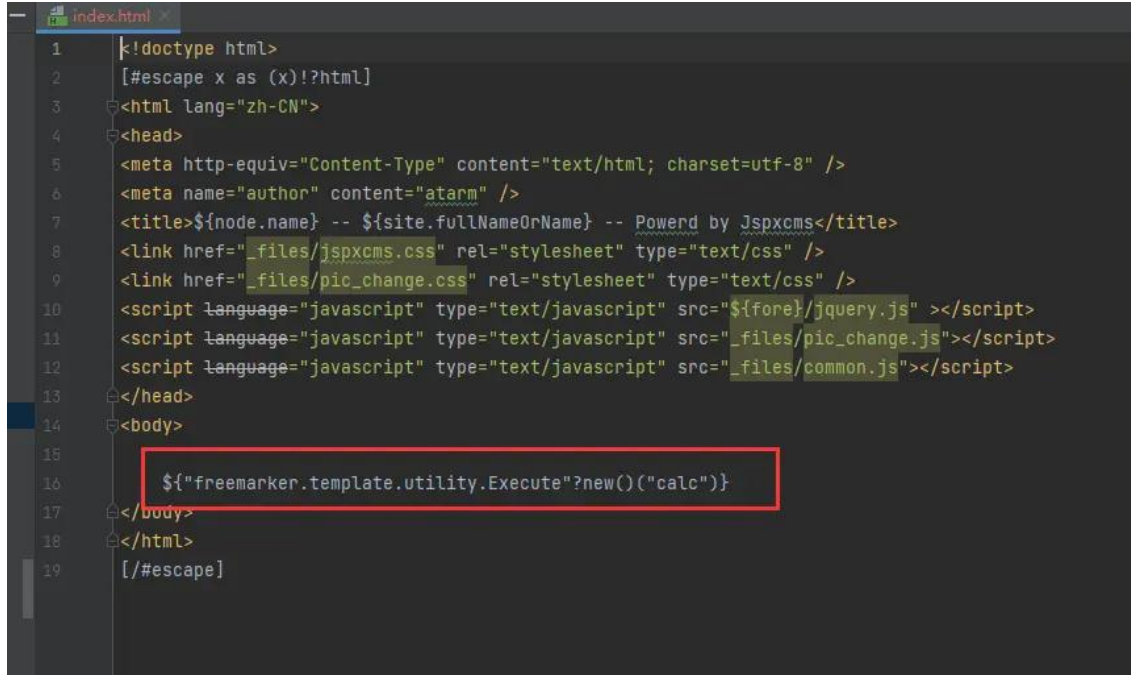
Jspxcms 存在命令执行10.2.0版本存在命令执行【模板文件】

Backlog #14QAZN Uranus Opened this issue 2022-01-11 13:28

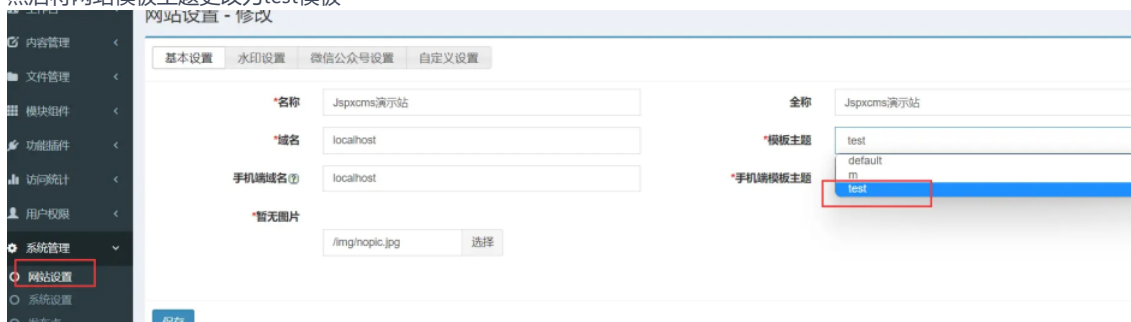
在Jspxcms后台文件管理目录下的模板文件允许我们上传自定义模板文件



因为目标站点使用了freemarker框架，所以我们构造一个执行calc的模板



然后将网站模板主题更改为test模板



Status

Backlog

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull request issue.

Branches

No related branch

Planned to start - Planned to start

Unscheduled - Unschedule

Top level

Not Top

Priority

Not specified

参与者 (3)





- 工作空间
- 工作流
- 操作日志

然后我们访问 <http://127.0.0.1:8088/>



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

可以看到命令已经执行了

Uranus created **任务** 11 months ago



freemarkerConfig 中增加

10 months ago

```
<!--<prop key="log_template_exceptions">false</prop--> <prop key="new_builtin_class_resolver">safer</prop>
```



jspxcms **owner** 9 months ago

模板其实属于程序的一部分，这个功能假定只有可信用户才会得到该项功能的授权。

如果实在需要把该功能赋予不受信任的用户，可以在freemarkerConfig以下配置：

```
<prop key="new_builtin_class_resolver">allows_nothing</prop>
```

但攻击者依然可以在模板中使用类似无限循环等方式进行攻击。

[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



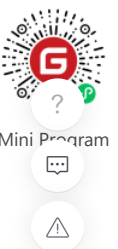
git@oschina.cn



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