## 漏洞简介

Portainer是一个轻量级的管理 UI，它允许您轻松管理不同的 Docker 环境（Docker 主机或 Swarm 集群）。在最新的版本2.6.0中存在多个存储型跨站脚本XSS漏洞。

## 漏洞利用

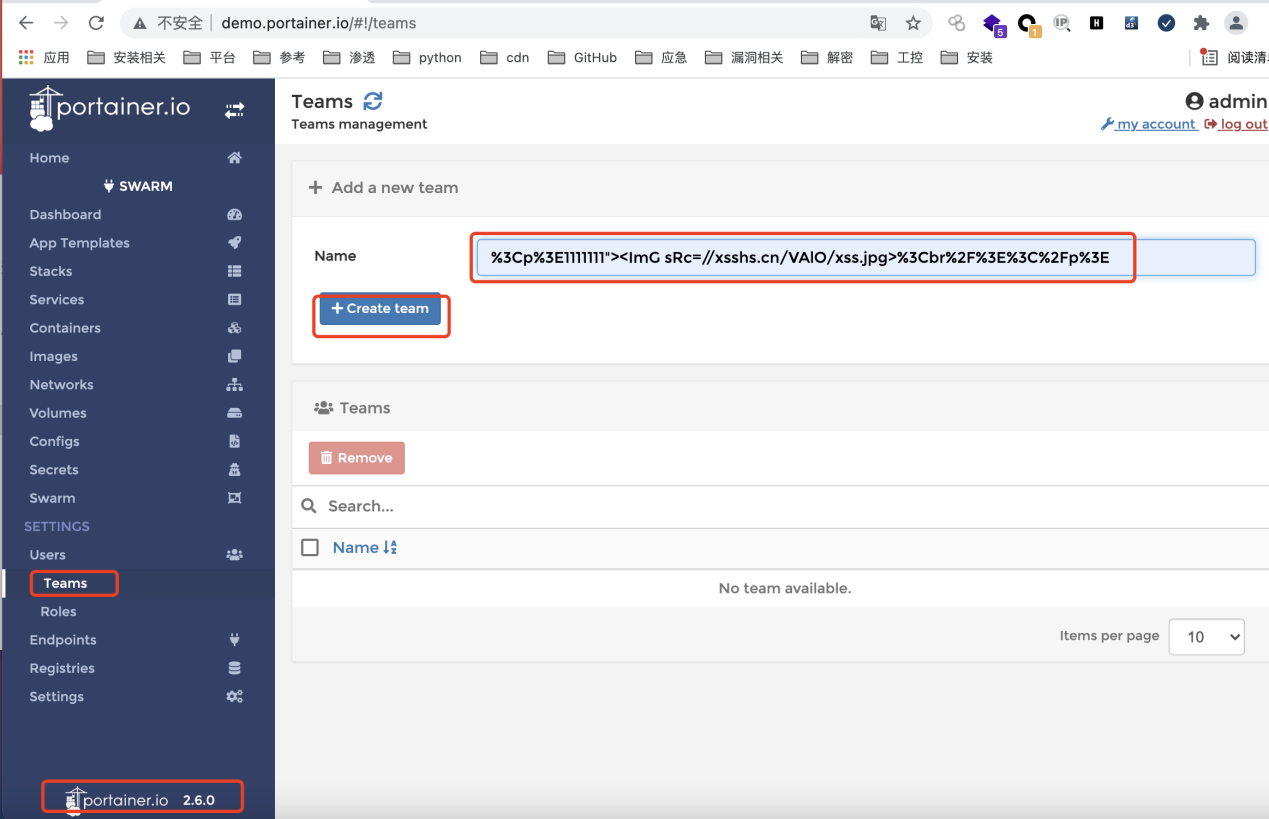
我们以官网最新版本为例：

[http://demo.portainer.io/](http://demo.portainer.io/#!/teams)

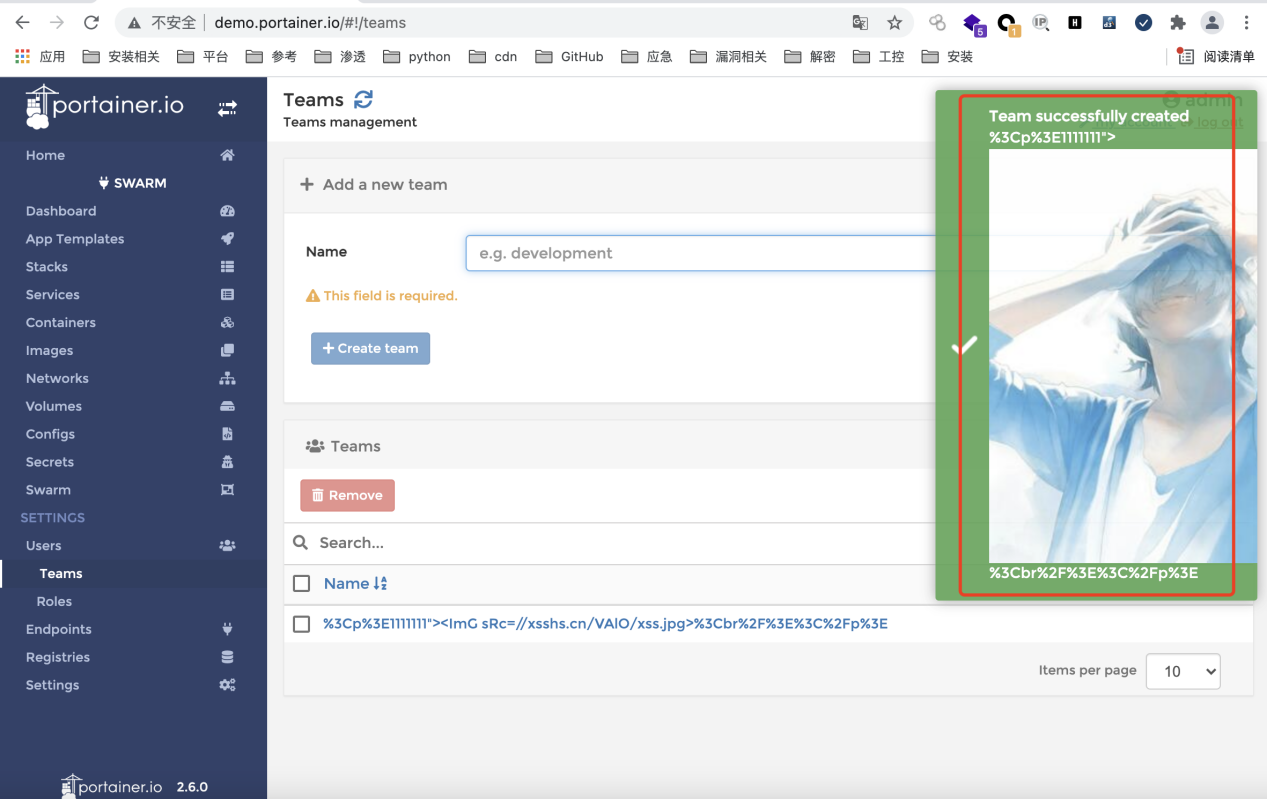
### 第一处：

首先登陆后台然后路径依次为：Users-Teams-Create team

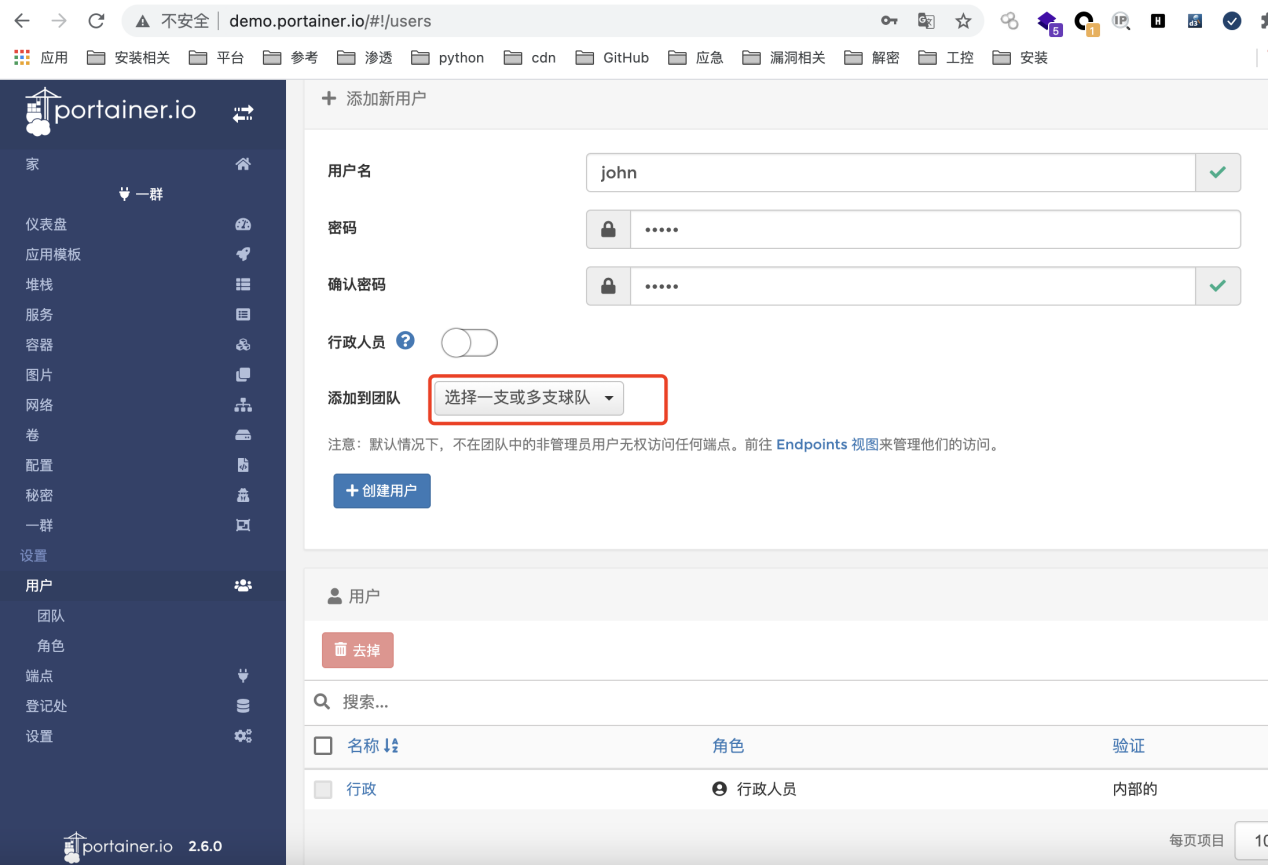
<http://demo.portainer.io/#!/teams>

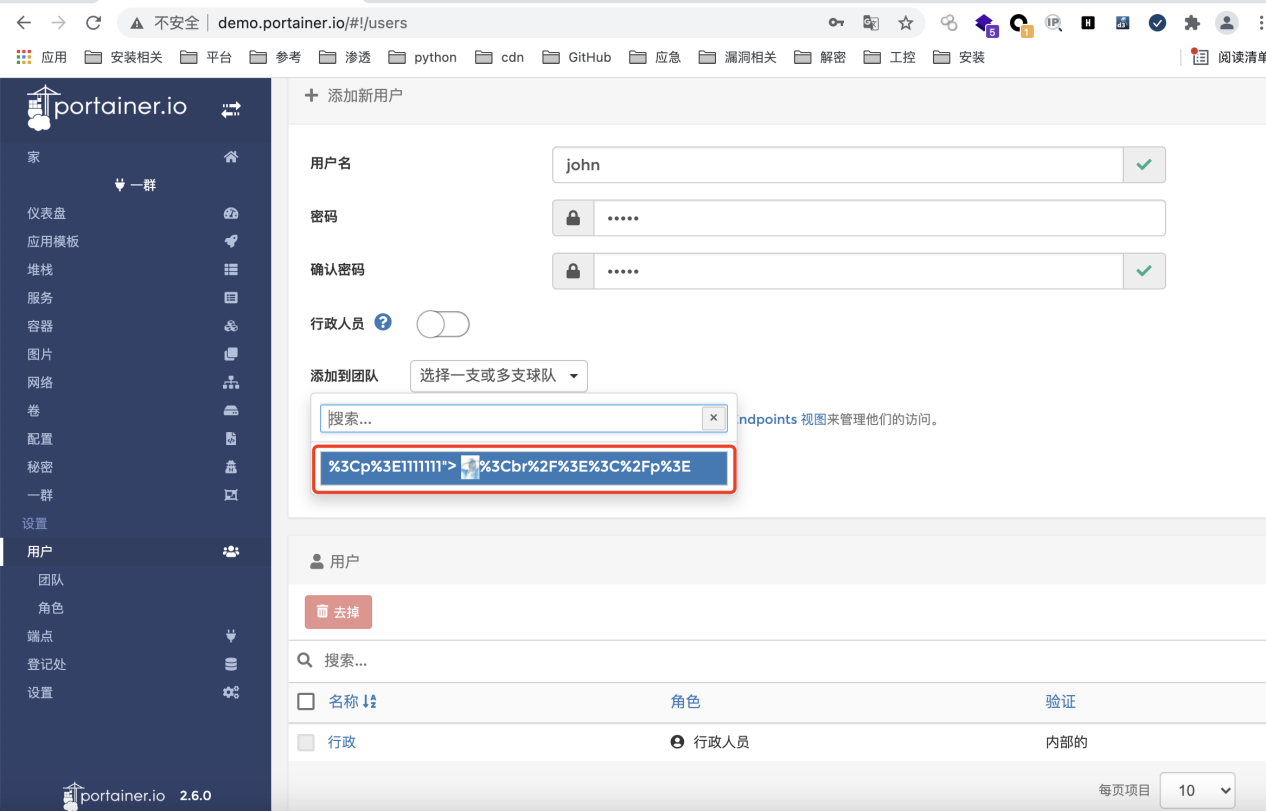


添加成功后从提示信息可以看到触发成功



当我们将用户添加到团队时，同样可以触发：





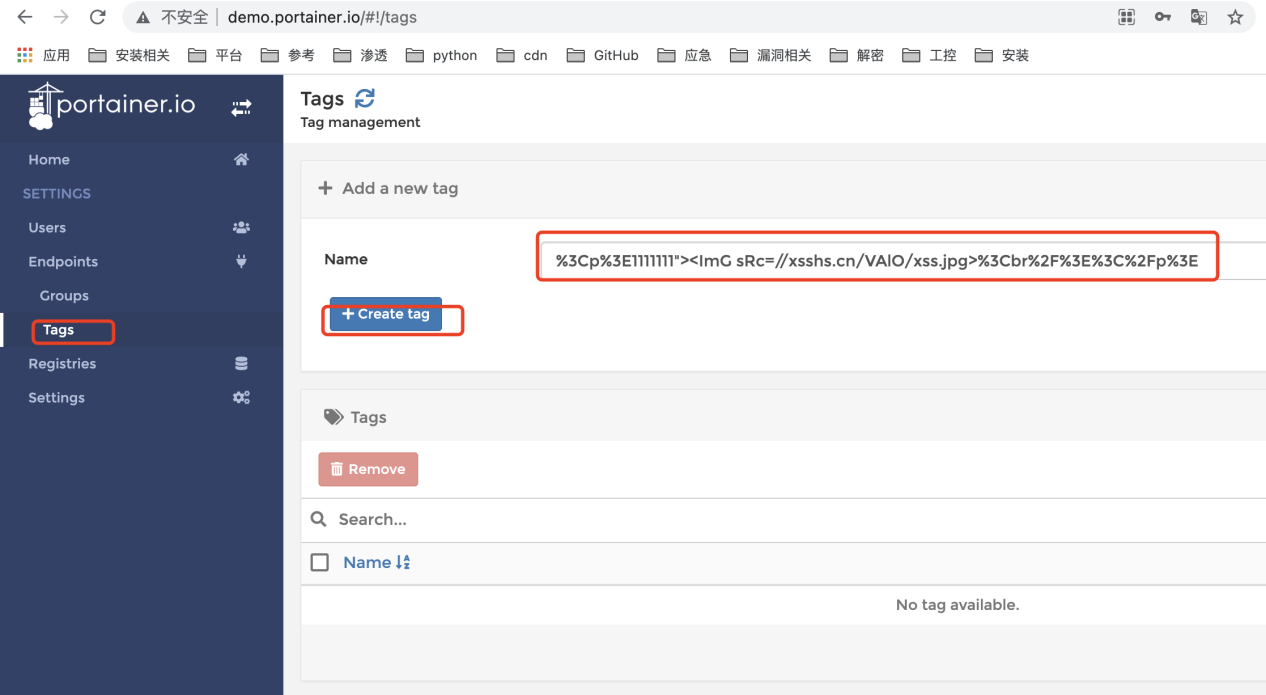
利用此XSS可以获取用户登陆的信息以及插入广告等恶意操作：

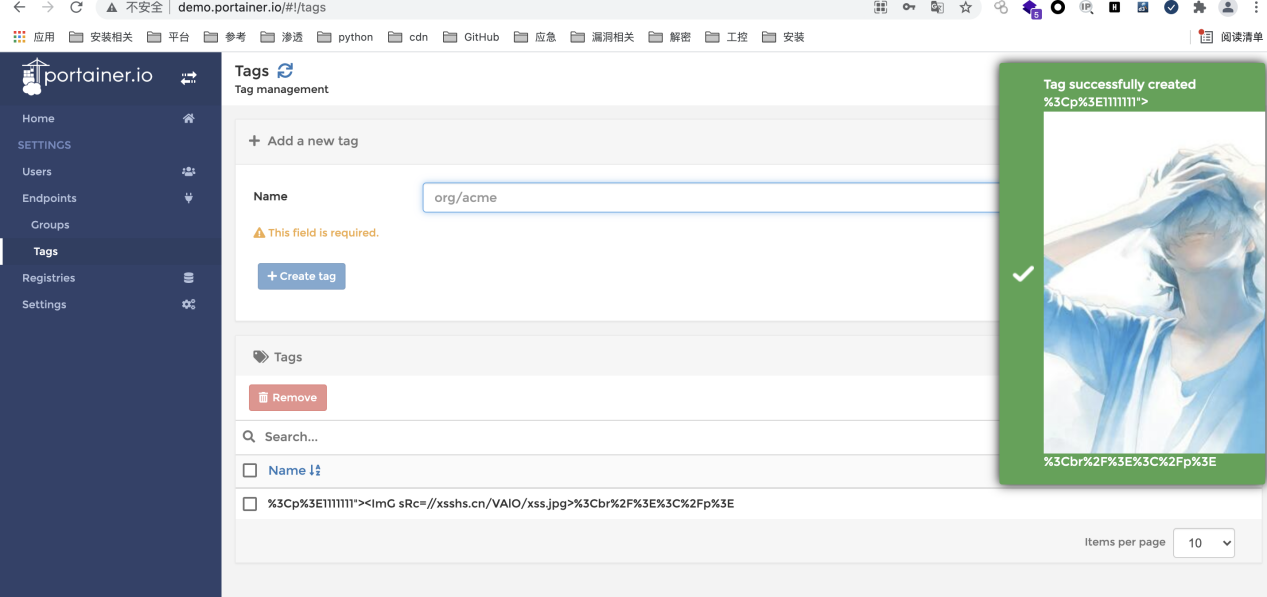


### 第二处

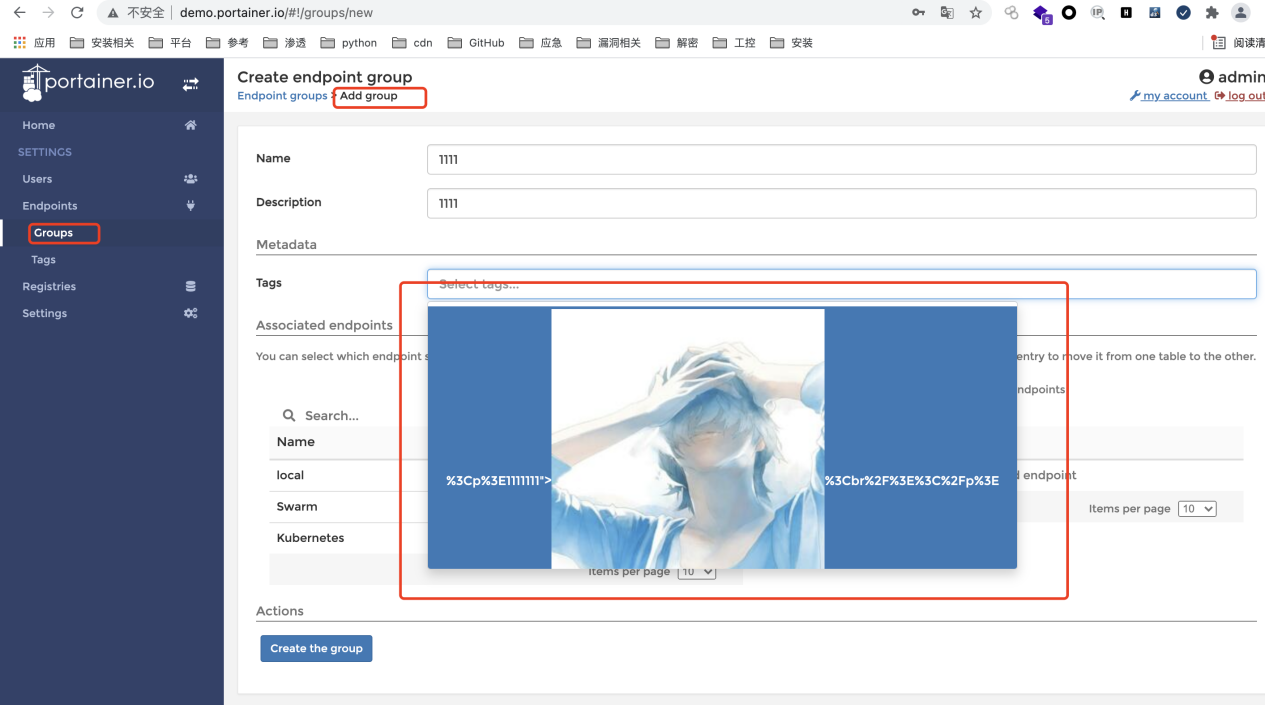
1. <http://demo.portainer.io/#!/tags>

路径为Endpoints-Tags-Name





当group选择tags时可能会选择含有xss的tags，这将会导致被获取敏感信息。

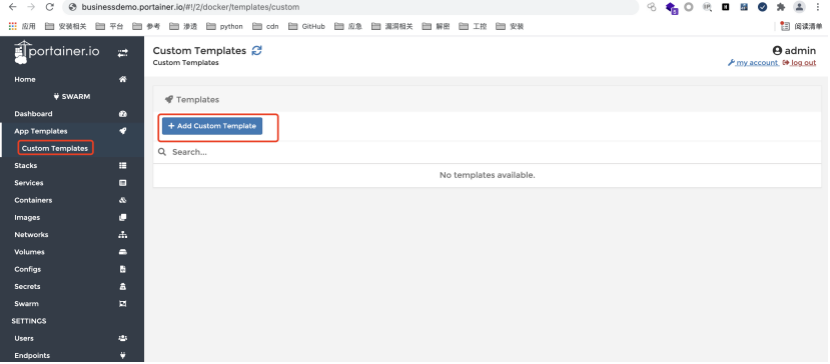


### 第三处

路径依次为：

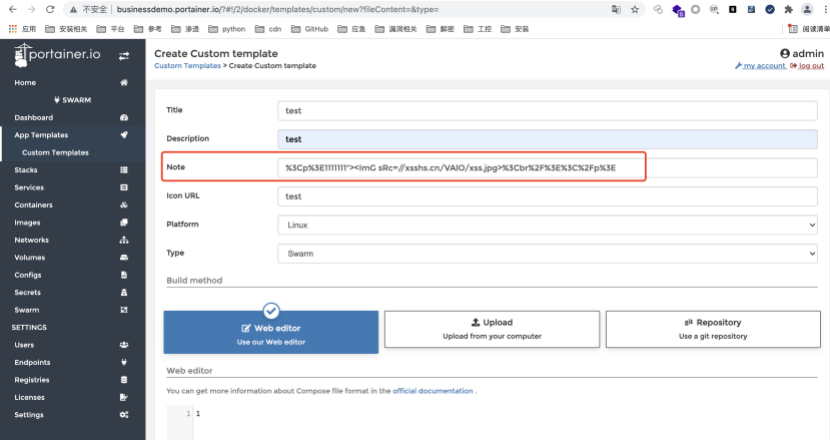
APP templates-Custom Templates-Add Custom Templates

[http://businessdemo.portainer.io/#!/2/docker/templates/custom](http://businessdemo.portainer.io/" \l "!/2/docker/templates/custom)

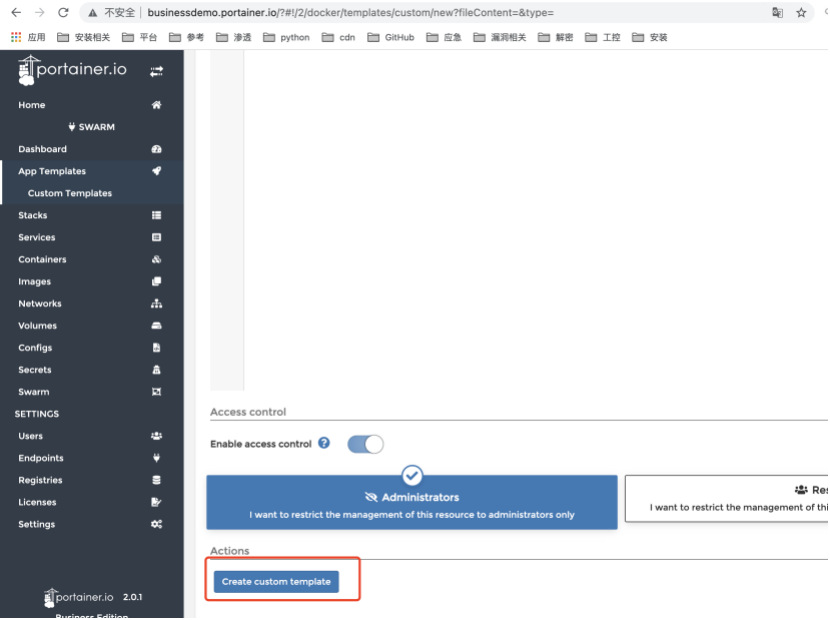


在Node插入XSS代码payload：

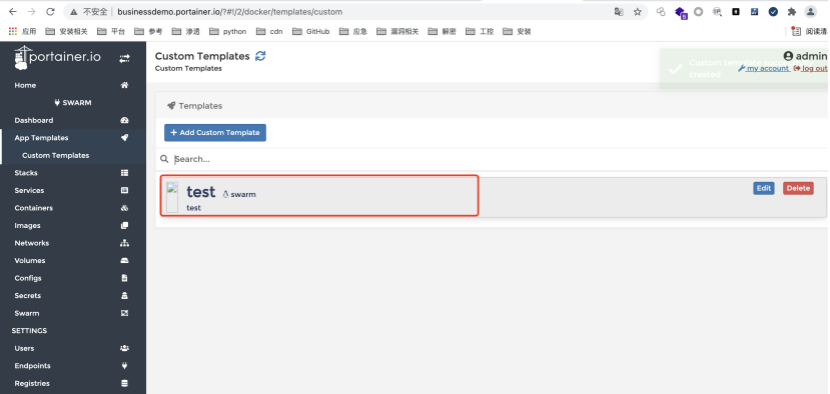
%3Cp%3E1111111"><ImG sRc=//xsshs.cn/VAlO/xss.jpg>%3Cbr%2F%3E%3C%2Fp%3E



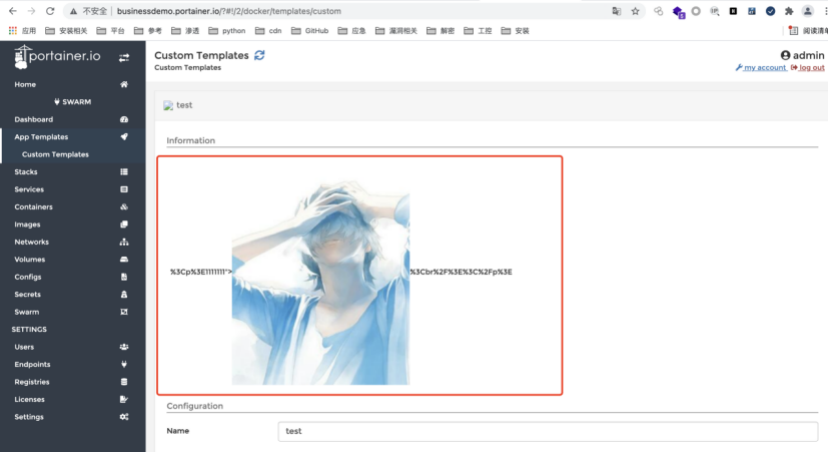
然后创建：



然后我们进入自定义的test：



成功触发xss跨站脚本攻击语句：



建议对Node进行xss严格过滤。

## 实际环境测试

在实际环境中也会触发存储XSS漏洞：

