Background storage XSS #27

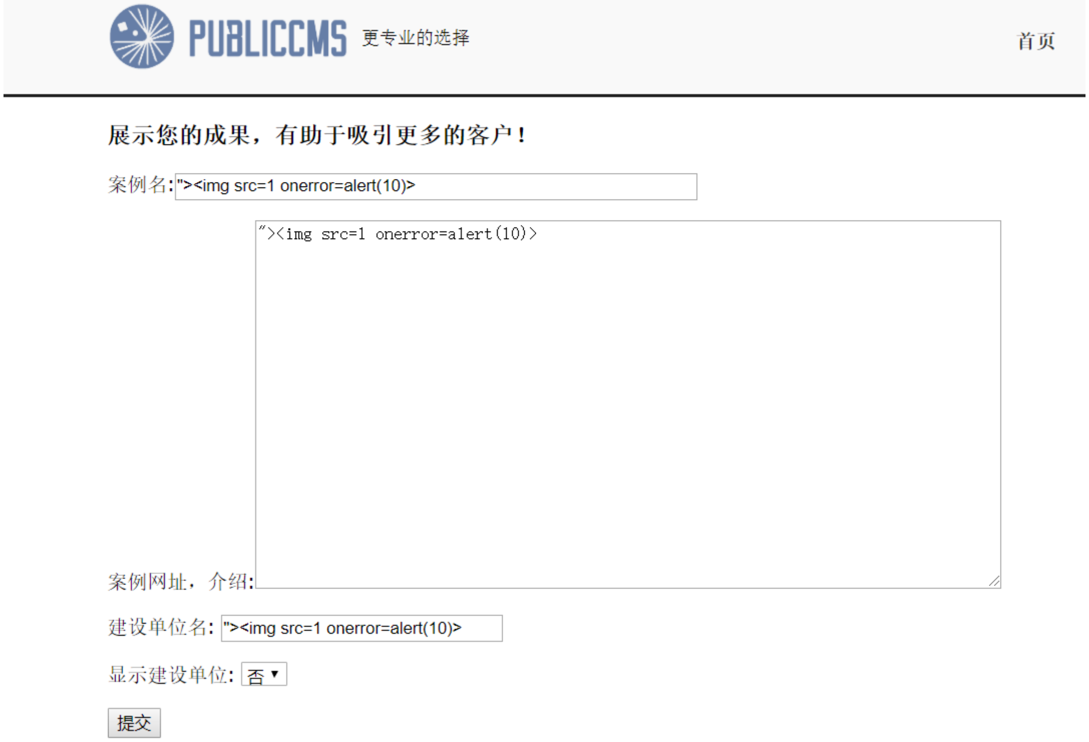
Closed wind226 opened this issue on Nov 19, 2019 · 5 comments

wind226 commented on Nov 19, 2019

Background storage XSS

step1：

https://cms.publiccms.com/case.html Submit case



展示您的成果，有助于吸引更多的客户！

案例名: "><img src=1 onerror=alert(10)>

案例网址，介绍: "><img src=1 onerror=alert(10)>

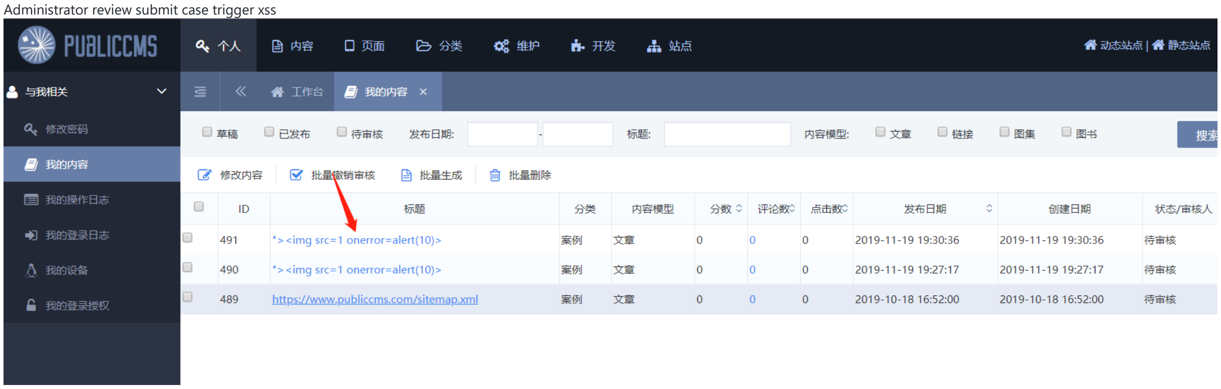
建设单位名: "><img src=1 onerror=alert(10)>

显示建设单位: 否

提交

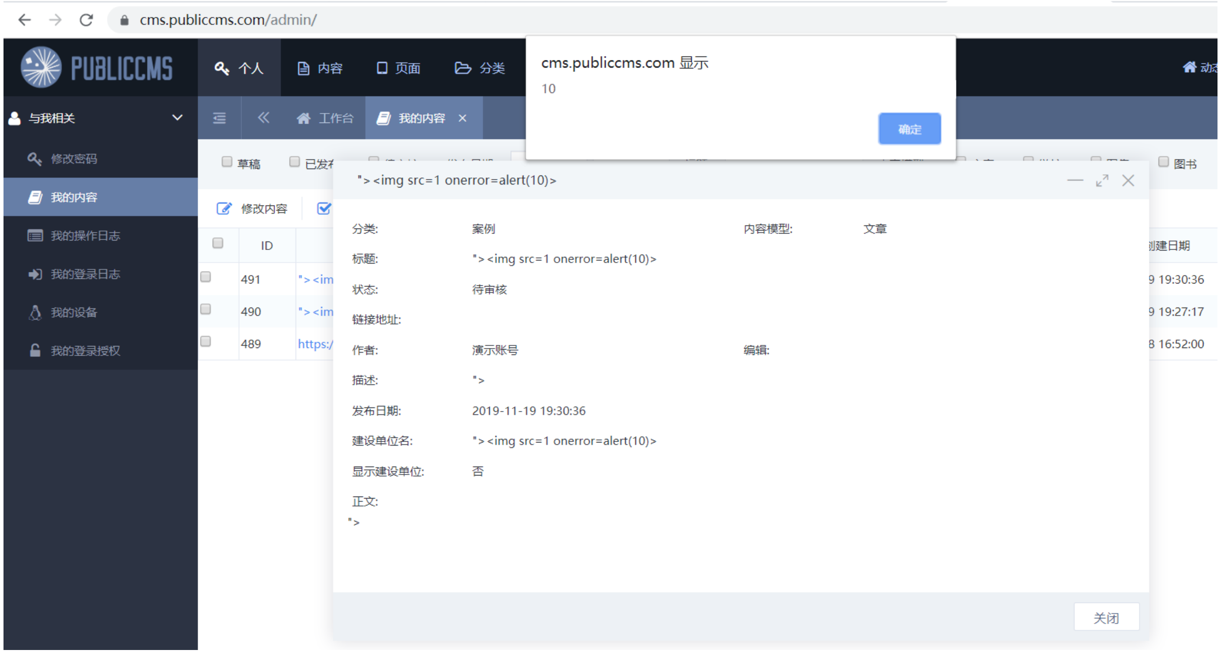
step2：

Administrator review submit case trigger xss



□	ID	标题	分类	内容模型	分数	评论数	点击数	发布日期	创建日期	状态/审核人
□	491	"><img src=1 onerror=alert(10)>	案例	文章	0	0	0	2019-11-19 19:30:36	2019-11-19 19:30:36	待审核
□	490	"><img src=1 onerror=alert(10)>	案例	文章	0	0	0	2019-11-19 19:27:17	2019-11-19 19:27:17	待审核
□	489	https://www.publiccms.com/sitemap.xml	案例	文章	0	0	0	2019-10-18 16:52:00	2019-10-18 16:52:00	待审核

Click to trigger xss



cms.publiccms.com 显示

10

"><img src=1 onerror=alert(10)>

分类: 案例　内容模型: 文章

标题: "><img src=1 onerror=alert(10)>

状态: 待审核

链接地址:

作者: 演示账号　编辑:

描述: ">

发布日期: 2019-11-19 19:30:36

建设单位名: "><img src=1 onerror=alert(10)>

显示建设单位: 否

正文:

">

sanluan commented on Nov 21, 2019 Owner

抱歉 这个问题暂时没办法避免 文章正文必须是富文本的
下个版本将会把投稿内容和普通内容区分开 审核前 取消投稿的预览

wind226 commented on Nov 21, 2019 Author

> 抱歉，这个问题暂时没办法避免文章正文必须是富文本的
> 下个版本将会把投稿内容和普通内容区分开审核前取消投稿的预览

你可以过滤敏感字符，或者转义双引号，单引号，尖括号就能避免xss

sanluan added a commit that referenced this issue on Nov 21, 2019

`https://github.com/sanluan/PublicCMS/issues/26` … b4d5956

sanluan commented on Nov 21, 2019 Owner

刚才提交了代码 目前的解决方法是标识投稿文章，对于未审核的投稿文章 默认做安全转义

wind226 commented on Nov 21, 2019 Author

> 先前提交了代码目前的解决方法是标识投稿文章，对于未审核的投稿文章默认做安全转义
> 做安全转义这个办法是可以

sanluan commented on Nov 21, 2019 Owner

非常感谢发现的这个bug

sanluan closed this as completed on Dec 7, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants