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

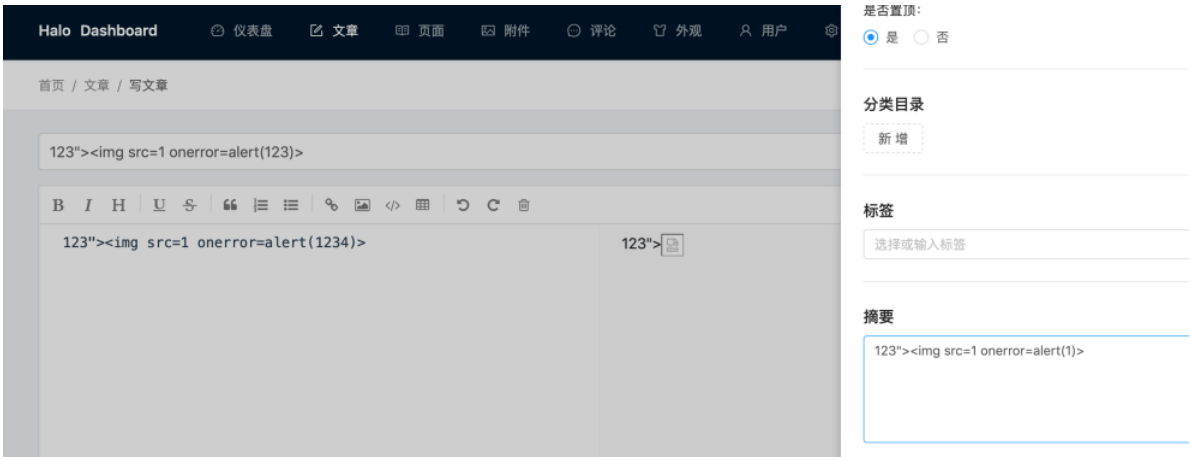
我确定我已经查看了 (标注 [ ] 为 [x])

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

我要申请 (标注 [ ] 为 [x])

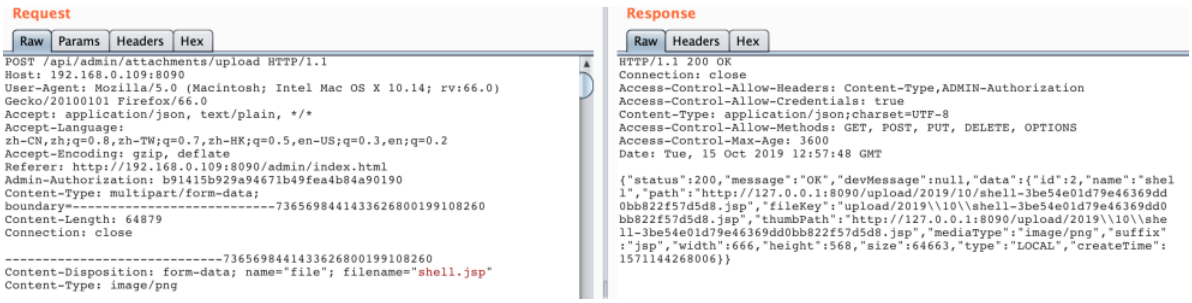
- [x] BUG 反馈
- [ ] 添加新的特性或者功能
- [ ] 请求技术支持

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。



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);
```



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

 **JohnNiang** closed this as completed on Oct 17, 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