xCss / Valine Public

Code Issues 34 Pull requests 7 Actions Projects Wiki ···

New issue

Jump to bottom

a fatal bug that can kill the comment system（用户恶意修改 UA 评论 可影响正常评论加载） #366

Closed sqlsec opened this issue on Jun 16, 2021 · 2 comments

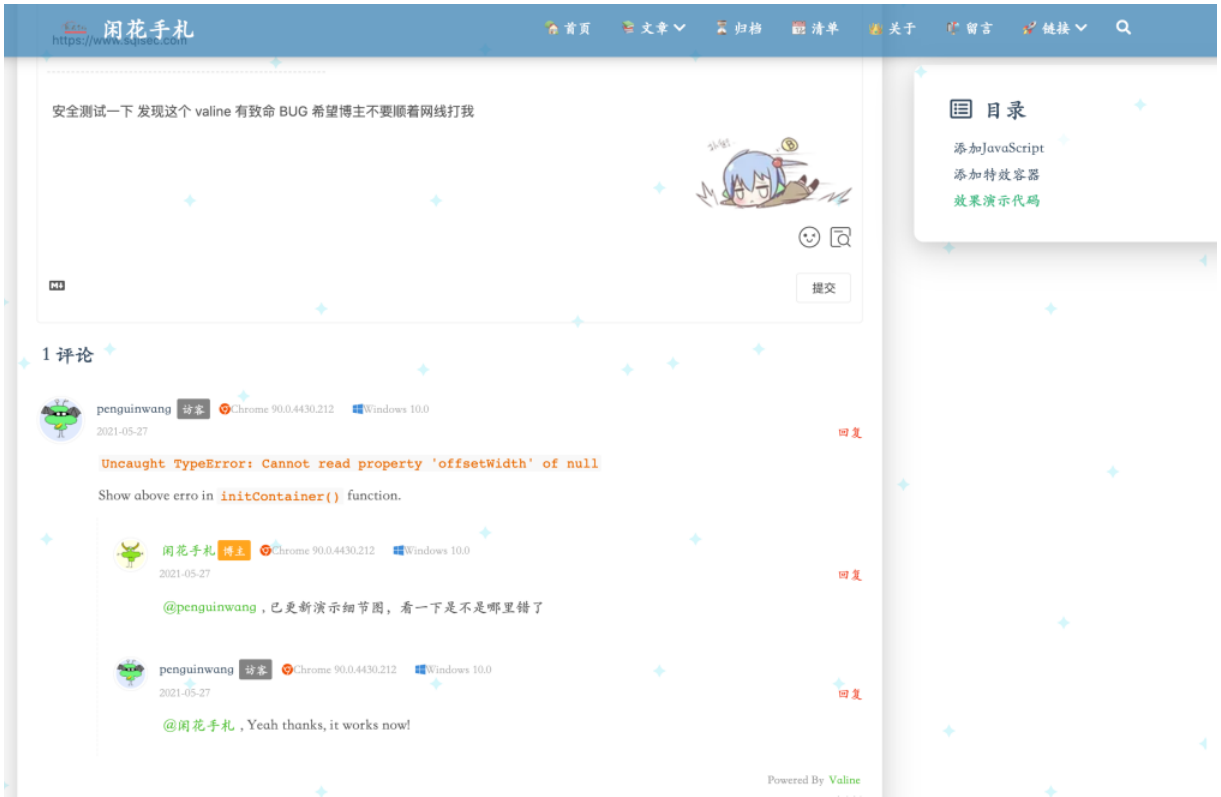
Labels wontfix

sqlsec commented on Jun 16, 2021

如果您想报告错误，请提供以下信息 If you want to report a bug, please provide the following information:

可复现问题的步骤 The steps to reproduce.

The latest version of valine is 1.4.14，Let's first look at the effect of normal page loading comments:



安全测试一下 发现这个 valine 有致命 BUG 希望博主不要顺着网线打我

1 评论

penguinwang 访客 Chrome 90.0.4430.212 Windows 10.0
2021-05-27

`Uncaught TypeError: Cannot read property 'offsetWidth' of null`

Show above erro in `initContainer()` function.

闲花手札 博主 Chrome 90.0.4430.212 Windows 10.0
2021-05-27

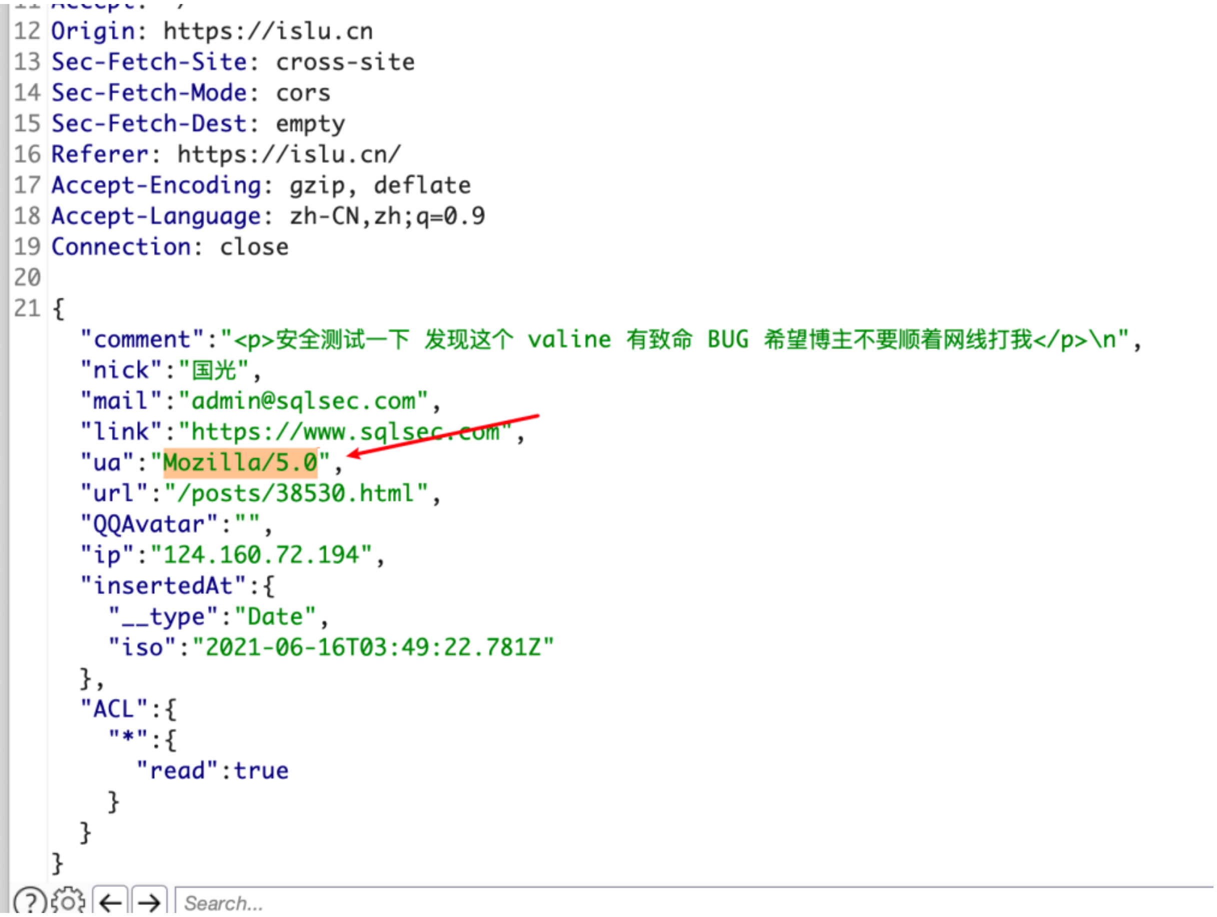
@penguinwang，已更新演示细节图，看一下是不是哪里错了

penguinwang 访客 Chrome 90.0.4430.212 Windows 10.0
2021-05-27

@闲花手札，Yeah thanks, it works now!

When the commented user UA is incomplete，such as：

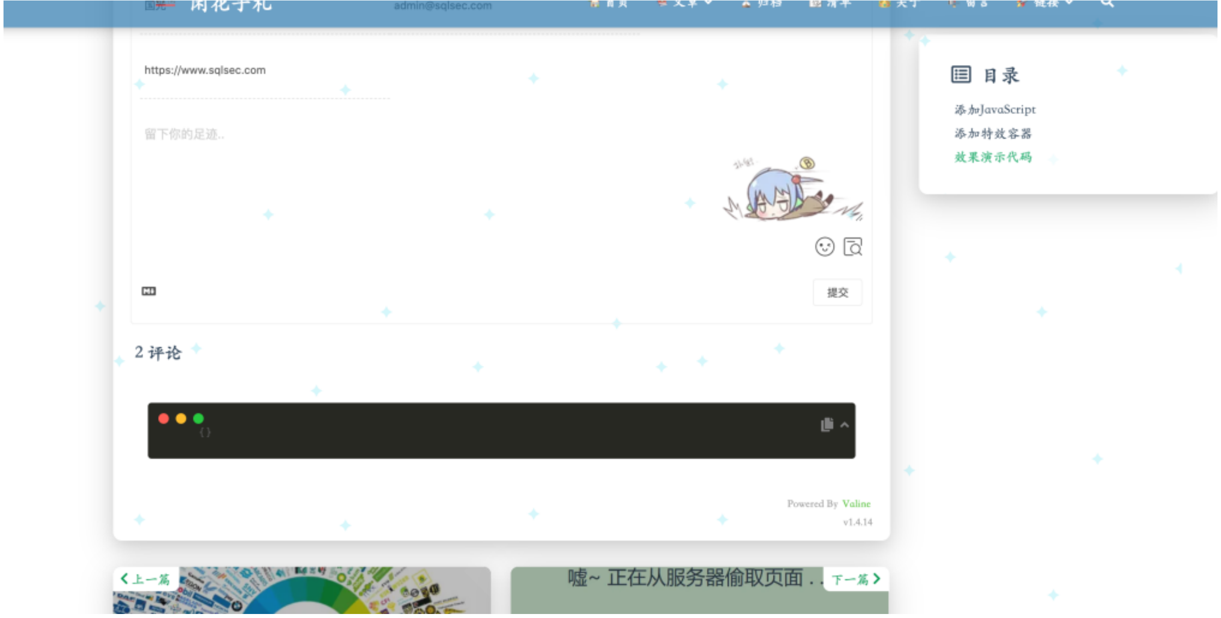
```
Mozilla/8.0
```



```
Accept: */*
Origin: https://islu.cn
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://islu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{
  "comment":"<p>安全测试一下 发现这个 valine 有致命 BUG 希望博主不要顺着网线打我</p>\n",
  "nick":"国光",
  "mail":"admin@sqlsec.com",
  "link":"https://www.sqlsec.com",
  "ua":"Mozilla/5.0",
  "url":"/posts/38530.html",
  "QQAvatar":"",
  "ip":"124.160.72.194",
  "insertedAt":{
    "__type":"Date",
    "iso":"2021-06-16T03:49:22.781Z"
  },
  "ACL":{
    "*":{
      "read":true
    }
  }
}
```

This will cause the entire comment system of the current page to be damaged and the comments cannot be loaded normally



可复现问题的网页地址

https://islu.cn/posts/38530.html

This website uses the latest version of valine, the comment cannot be loaded normally

受影响的Valine版本、操作系统，以及浏览器信息

- Valine 1.4.14
- OS：Windows/Linux/macOS
- Browser: Chrome、Firefox、Safair

总的来说就是 如果有用户恶意修改 UA 评论的话，会直接把那个页面评论打瘫痪掉，我是在排查我的一篇 300 多个评论文章的时候发现的，把 leancloud 从里到外排查了一遍 才发现了这个 BUG，希望作者大大后面可以修复这个尴尬的问题

👍 3

sqlsec changed the title ~~Found a fatal bug that can kill the comment system~~ **a fatal bug that can kill the comment system（用户恶意修改 UA 评论 可影响正常评论加载）** on Jun 16, 2021

xCss commented on Oct 21, 2021 Owner

@sqlsec 你好，我这边本地测试没法复现这个Bug 😥

👀 3

stale bot commented on Apr 16

This issue has been automatically marked as stale because it has not had recent activity. It will be closed if no further activity occurs. Thank you for your contributions.

stale bot added the **wontfix** label on Apr 16

sqlsec closed this as completed on May 31

Assignees

No one assigned

Labels

wontfix

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants