

New issue

[Jump to bottom](#)

search.js v4.12.1 Cross-Site Scripting #1549

Closed

1 task

Ares-X opened this issue on Mar 30, 2021 · 5 comments · Fixed by #1551

Labels needs discussion

Projects Triage

Ares-X commented on Mar 30, 2021

Bug Report

Steps to reproduce

1. create a simple docsify project

file tree

```
.
├── README.md
├── _sidebar.md
├── index.html
├── test
└── xss.md
```

index.html

```
<!DOCTYPE html>

<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>test</title>
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
  <meta name="description" content="Description">
  <meta name="viewport" content="width=device-width, user-scalable=no, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0">
  <link rel="stylesheet" href="//cdn.jsdelivr.net/npm/docsify/lib/themes/vue.css">
  <link rel="stylesheet" href="/css/sidebar.css">
</head>
<body>

  <div id="app"></div>

  <script>
    window.$docsify = {
      loadSidebar: true,
      homepage: './README.md',
      alias: {
        '/.*_sidebar.md': './_sidebar.md',
      },
      autoHeader: true,
      auto2top: true,
      search: {
        noData: {
          '/': 'No results!'
        },
        paths: 'auto',
        placeholder: {
          '/': 'Search'
        },
      },
      hideOtherSidebarContent: true,
      depth: 1
    },
    name: 'test',
  }
</script>

<script src="//cdn.jsdelivr.net/npm/docsify/lib/docsify.min.js"></script>
<script src="//cdn.jsdelivr.net/npm/docsify/lib/plugins/search.js"></script>

</body>
</html>
```

xss.md

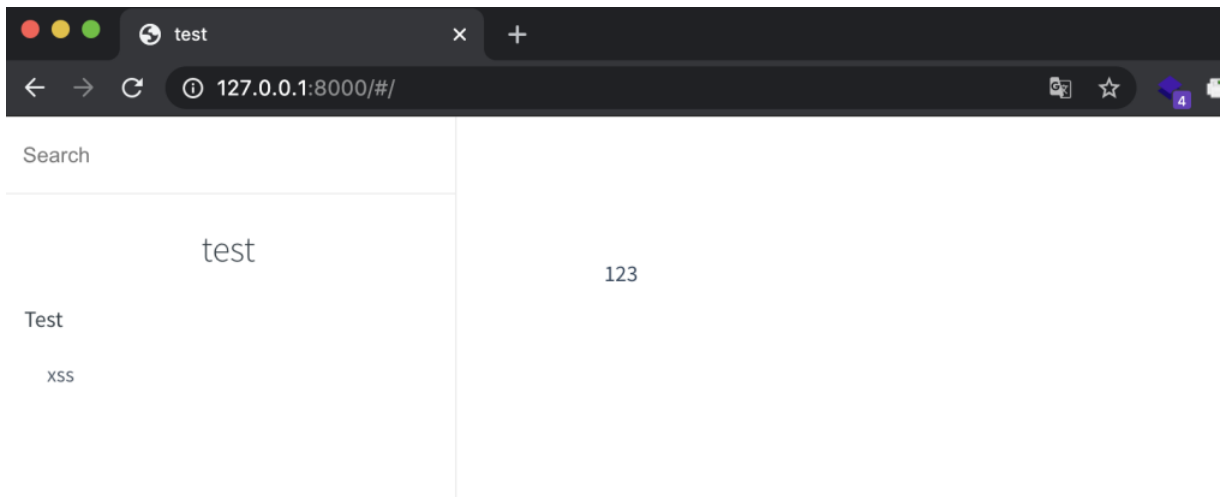
```
# xss test

xss"><img src=1 onerror=alert(1)><"
```

_sidebar.md

```
- Test
- [xss](./test/xss.md)
```

2. start a http server



when user search something near XSS payload and the javascript which should rendering as markdown will be execute

3. input x in search filed



What is current behaviour

What is the expected behaviour

Other relevant information

☐ Bug does still occur when all/other plugins are disabled?

- Your OS: Mac OS
- Node.js version: v12.19.0
- npm/yarn version:
- Browser version:
- Docsify version: 4.12.1
- Docsify plugins: search.js

Please create a reproducible sandbox

<https://xl9pw.csb.app/>

Mention the docsify version in which this bug was not present (if any)

 **project-bot** (bot) added this to Needs Review in **Triage** on Mar 30, 2021


sy-records commented on Apr 1, 2021 • edited ▾

Member

You should not write the wrong content...

docsify does not filter errors content in the body.

cc @docsifyjs/reviewers

 **sy-records** added the **needs discussion** label on Apr 1, 2021

Ares-X commented on Apr 1, 2021

Author

4 space or one tab for Code Blocks is a standard markdown syntax

```
# title  
code
```

i don't think this is a wrong content

sy-records commented on Apr 1, 2021

Member

Okay, I tested it without spaces...

```
xss"><img src=1 onerror=alert(1)><"
```

Ares-X commented on Apr 1, 2021

Author

with out Code Blocks syntax markdown will rendering code as html

The problem comes from the search plug didn't appropriate encode Code Blocks and let " escaped

xss test

code.lang-markup 749.22 x 80.31

```
xss"><img src=1 onerror=alert(1)><"
```

```
Sources HackBar EditThisCookie Network Memory Performance Application Security

/xss.md" class="ready sticky">

ar-toggle" aria-label="Menu">...</button>
r">...</aside>
ent">
kdown-section" id="main">
>...</h1>
ang="markup">

g-markup">xss"&gt;<span class="token tag"><span class="token tag"><span class="token punct
> <span class="token attr-name">src</span><span class="token attr-value"><span class="token
1</span> <span class="token attr-name">onerror</span><span><span class="token attr-value"><span
-equals">=</span>alert(1)</span><span class="token punctuation">&gt;</span></span>&lt;</c
```

xss test #text 21.77 x 18

...xss">

xss test

```
xss"><img src=1 onerror=alert(1)><"
```

```
Elements Console Sources HackBar EditThisCookie Network Memory Performance Applica

  <button class="sidebar-toggle" aria-label="Menu">...</button>
  <aside class="sidebar">
    <div class="search">
      <div class="input-wrap">...</div>
      <div class="results-panel show">
        <div class="matching-post">
          <a href="#/./test/xss?id=xss-test">
            <h2>xss test</h2>
            <p>
              "...
              <em class="search-keyword">x</em>
              "...
              "ss">" == $0
              
              "<"..."
            </p>
          </a>
```

sy-records commented on Apr 1, 2021

Member

Yes, here's what I removed, I'm revisiting



sy-records mentioned this issue on Apr 1, 2021

fix: Add escapeHtml for search #1551

Merged

9 tasks



sy-records closed this as completed in #1551 on Apr 11, 2021



project-bot (bot) moved this from Needs Review to Closed / Won't Fix in Triage on Apr 11, 2021

Assignees

No one assigned

Labels

needs discussion

Projects



Triage

Closed / Won't Fix

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

fix: Add escapeHtml for search
sy-records/docsify

2 participants

