

New issue

[Jump to bottom](#)

[sidekiq <= v6.2, v5.1.3] Cross-site-scripting (XSS) #4852

🔒 Closed xhzeem opened this issue on Mar 24, 2021 · 8 comments

xhzeem commented on Mar 24, 2021 • edited

Hi there,
I found an XSS vulnerability affecting version **v5.1.3** and maybe anything below that.

PoC

```
[HOST]/sidekiq/queues/"onmouseover="alert('@xhzeem')"
```

mperham commented on Mar 24, 2021

Owner

This was fixed in [#2330](#). Is there a regression?

xhzeem commented on Mar 24, 2021


Author

Sorry I've updated the ticket
It's different in the link this time.

mperham commented on Mar 24, 2021

Owner

You need to give me something that works against master. Security issues that are fixed are not issues.

 mperham added a commit that referenced this issue on Mar 24, 2021 escape name in paging links, [#4852](#)

✓ 2a57abc

mperham commented on Mar 24, 2021

Owner

I'm unable to reproduce an issue in Sidekiq v5.1.0. I found and fixed one inconsistency but I don't see how it can be exploited as it requires a queue with that name to have jobs in it. Please give more detailed steps or close the issue.

xhzeem commented on Mar 24, 2021

Author

the payload I provided works against the latest version of master, I tested multiple setups, some only worked for IE and the other worked on all browsers, so I couldn't understand why,

If you have Internet Explorer you can open this link as a proof

```
[HOST]/sidekiq/queues/"<h1>xhzeem
```

The point is that modern browsers auto encode some characters to URL encoding which makes the " " converts into %22 but internet explorer doesn't do that you can see it there with no issue, even though I have another setup that is vulnerable and exploitable on chrome but I don't know why.

PoC: https://d.top4top.io/p_19096xn861.png

simply just use cURL and you will get it.

```
curl 'https://[HOST]/sidekiq/queues/"onmouseover="alert()"' -H 'Authorization: Basic YWRtaW46QHhoemVlbQ=='
```

xhzeem commented on Mar 24, 2021 • edited

Author

I don't write ruby, but I tried to trace back the issue and I believe it might be caused by those two lines.

[sidekiq/web/views/_poll_link.erb](#)
Lines 3 to 5 in 3b5ae30

```
3 <a id="live-poll" class="btn btn-primary active" href="%<%= root_path + current_path %>"><%= t('StopPolling') %></a>
4 <% else %>
5 <a id="live-poll" class="btn btn-primary" href="%<%= root_path + current_path %>?<%= qparams(poll: true) %>"><%= t('LivePoll') %></a>
```

 mperham closed this as completed in [64f7033](#) on Mar 25, 2021

mperham commented on Mar 25, 2021

Owner

I think you're right about the source, nice job!




IE is not a relevant browser these days, but thank you for reporting. I've added a check to the input.

  **xhzeem** changed the title ~~Cross-site-scripting (XSS)~~ [sidekiq <= v6.2] Cross-site-scripting (XSS) on Apr 3, 2021

  **xhzeem** changed the title ~~(sidekiq <= v6.2) Cross-site-scripting (XSS)~~ [sidekiq <= v6.2, v5.1.3] Cross-site-scripting (XSS) on Apr 3, 2021

abergmann commented on Apr 7, 2021

[CVE-2021-30151](#) was assigned to this issue.

  **mend-bolt-for-github**  mentioned this issue on Jan 28

CVE-2021-30151 (Medium) detected in sidekiq-5.2.9.gem - autoclosed ManageIQ/miq_bot#576

 Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

