


## 11 Session Hijack via Self-XSS

Share:     

### TIMELINE

- 

jcardona submitted a report to [Rocket.Chat](#). Aug 19th (2 years ago)

**Summary:** It's possible to hijack a session by tricking the user to perform a Self-XSS on the drag and drop functionality in the chat.

**Description:** Self-XSS is an underrated vulnerability that can have a harmful impact on the users of the application like here, after we get access to the user's session we can read chats, change (some) info and lock the account by activating the 2FA.

**Releases Affected:**

  - Tested on 3.5.2 and 3.5.3 (current version)

**Steps To Reproduce:**

  1. Serve the image (payload) using Python's HTTP server.
  2. Trick the user to drag and drop the image inside a chat.
  3. Get the `Meteor.loginToken` from the server logs.
  4. Open that instance of Rocket Chat in a browser.
  5. Add the `Meteor.loginToken` as an item in the local storage.
  6. The site automatically redirects to the session.
  7. Profit!


**Supporting Material/References:**

  - GIF file explaining the PoC.
  - HTML file with the payload.

**Suggested mitigation**

  - Sanitize the drag and drop functionality of chat text box stripping the tags.


**Impact**

The attacker can gain access to the user session and read chats, change (some) info and lock the account by activating the Two-Factor Authentication, even alter the server configuration depending on the account privileges.
- 


markus-rocketchat changed the status to ● **Triaged**. Aug 20th (2 years ago)

Hi [@jcardona](#)

thank you for your report. Interesting attack style... we will think on how to mitigate that. I'll keep you posted here. If you have any additional information, please feel free to share.

Best  
Markus
- 


jcardona posted a comment. Oct 31st (2 years ago)

Hi [@markus-rocketchat](#), got any news on this one? I really want to post the write-up on a personal blog that I'm building.
- 

markus-rocketchat posted a comment. Nov 1st (2 years ago)

Hi [@jcardona](#)


apologies for the silence. We are still working on it. If you could give us a bit more time, that would help us implement a proper fix. And since you are the only one currently who reported it, you dont have to worry that someone else will take the credits from you. Thank you for your patience.

Best  
Markus
- 


markus-rocketchat posted a comment. Nov 16th (2 years ago)

Hi [@jcardona](#)

i just wanted to let you know that we are still working on it and our initial idea to fix it turned out not to be sufficient. So we are still working on it, and hoping to have a fix soon.

Best  
Markus
- 


jcardona posted a comment. Nov 18th (2 years ago)

Hi [@markus-rocketchat](#), thank you very much for the update if there is something I can help with, don't hesitate to ask me.
- 

markus-rocketchat closed the report and changed the status to ● **Resolved**. Dec 17th (2 years ago)

Hi [@jcardona](#)

thanks again for your report. We included a fix in the latest release. Please apologize the delay in me notifying you, I was ooo.

<https://github.com/RocketChat/Rocket.Chat/pull/19593>
- 

jcardona requested to disclose this report. Dec 18th (2 years ago)



Hi [@jcardona](#)

I have added you to our White Hat Hall of Fame. <https://docs.rocket.chat/contributors/contributing/security#whitehat-hall-of-fame>

I also requested a CVE-ID for this report, which will be associated with it.



This report has been disclosed.

Jan 17th (2 years ago)