[HTML5SEC-47] XSS in real time chat

Created: 13/Dec/20 Updated: 13/Dec/20

Status:	To Do
Project:	HTML5-Security
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Task	**Priority:**	Medium
Reporter:	Robert Morel	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Rank:	0|i00087:

Description

Summary

Script can be injected in to real time chat.

URL

http://sample-application-insecure.com/

Description

Multiple users are in the chat. If one user injects a payload it affects all current users.

Steps to reproduce

1. Log in
2. Go to the chat page
3. Open up a second chat
4. Inject payload <img src='https://a5h8v9a3.stackpathcdn.com/wp-content/uploads/Hacker5.jpg' onmouseover="alert('xxs on mouse')">
5. Payload appears for all participants.

Recommended fix

Sanitize all user inputted data

Generated at Sun Dec 13 12:54:15 UTC 2020 by Robert Morel using Jira 1001.0.0-SNAPSHOT#100152-sha1:d8e2c464c38df4d324e50756a9cf9ad44685efeb.