[HTML5SEC-48] Chat hosted in external website

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|i0008f:

Description

Summary

Able to host the chat on a different domain which means I can join in discussions without being logged in.

URL

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

http://evil.com

Description

Data leak as outside actor can view chat and respond to messages.

Steps to reproduce

1. Login
2. Go to chat page
3. Open up evil.com
4. Send a message
5. evil.com is able to participate in the chat

Recommended fix

Set the origin on the websocket client and server to be http://sample-application-insecure.com/

Generated at Sun Dec 13 12:54:22 UTC 2020 by Robert Morel using Jira 1001.0.0-SNAPSHOT#100152-sha1:d8e2c464c38df4d324e50756a9cf9ad44685efeb.