[HTML5SEC-49] Registration page in IFrame 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		

Attachments:	image-20201213-115130.png
Rank:	0|i0008n:

Description

Summary

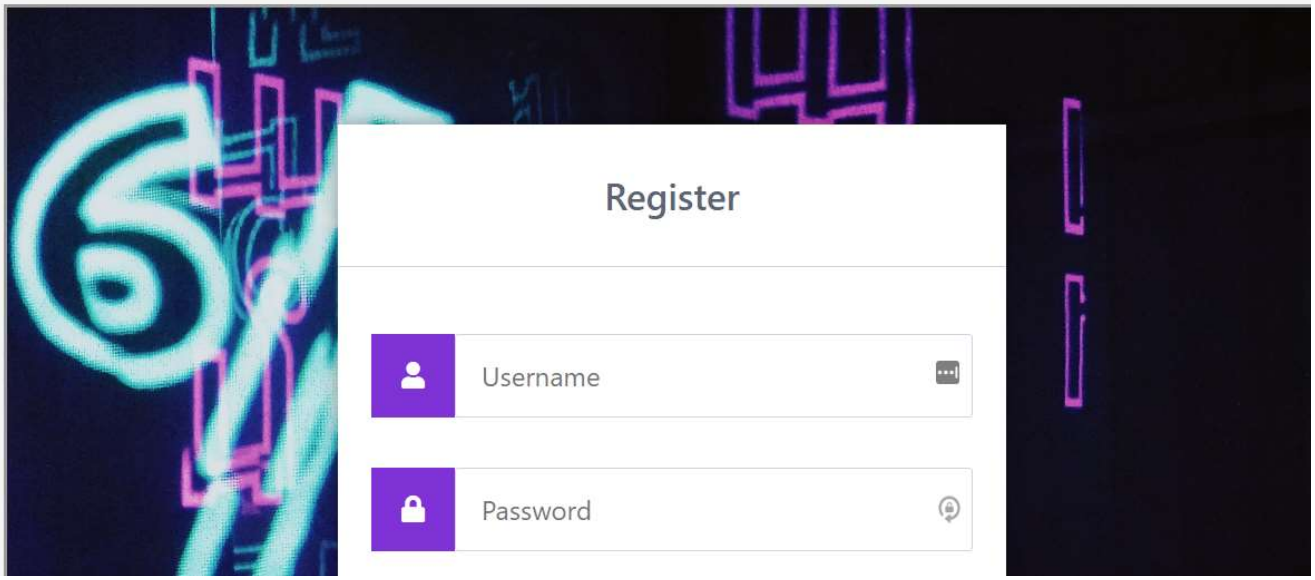
Able to display application in an IFrame leading to potential XSS

URL

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

Description

If I host the forms in an IFrame on evil.com then I can extract passwords from users.



Steps to reproduce

1. Create an IFrame that displays the register page
2. Use phishing to get user to click on link for evil.com
3. Extract the information and then send the login to the legitamate site.
4. Username, email and password obtained.

Recommended fix

Add an HTTP header in .htaccess or at server level of

X-Frame-Options SAMEORIGIN

Generated at Sun Dec 13 12:54:29 UTC 2020 by Robert Morel using Jira 1001.0.0-SNAPSHOT#100152-sha1:d8e2c464c38df4d324e50756a9cf9ad44685efeb.