[HTML5SEC-45] Invalid data submitted in registration form 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-20201213-113202.png
Rank:	0|i0007r:

Description

Summary

Able to enter script and html tags in register form - possibly leading to SQL or dom based injection.

URL

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

Description

Register form does not sanitize input so any value can be entered.

		id	username	password
⠿ Copy	🔴 Delete	13	user	$2y$10$qDIJ9Hd2UrTvomEonJHOL.hz8hEYcPEJHVE122VQx2U
⠿ Copy	🔴 Delete	15	admin	$2y$10$alzMs2v7fjHjQJW.PjnaiOQlMUUW5Ow5UjSem1ShaC9..
⠿ Copy	🔴 Delete	16	aaa	$2y$10$RU1m6yFkdwp4nPqtvTTcsetN9qK76hqx1j8.61JA1i9...
⠿ Copy	🔴 Delete	17	sss	$2y$10$CY.JZgjF2aGRFj/2yzg5XuUIyajcTulSlqSLVammf9j...
⠿ Copy	🔴 Delete	19	\<a onmouseover="alert(document.	$2y$10$v/YZ6n1qiLX3Uik7NXDvvO1TBln6aRIBEGRRekV4Eao..

Steps to reproduce

1. Go to register page
2. Enter a string with script tags in.
3. No block in place

Recommended fix

Prevent using HTML5 form attributes and REGEX. Sanitize all input using a 3rd party library.

Generated at Sun Dec 13 12:53:57 UTC 2020 by Robert Morel using Jira 1001.0.0-SNAPSHOT#100152-sha1:d8e2c464c38df4d324e50756a9cf9ad44685efeb.