[HTML5SEC-46] Dom based XSS in profile page

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-20201213-113452.png
Rank:	0|i0007z:

Description

Summary

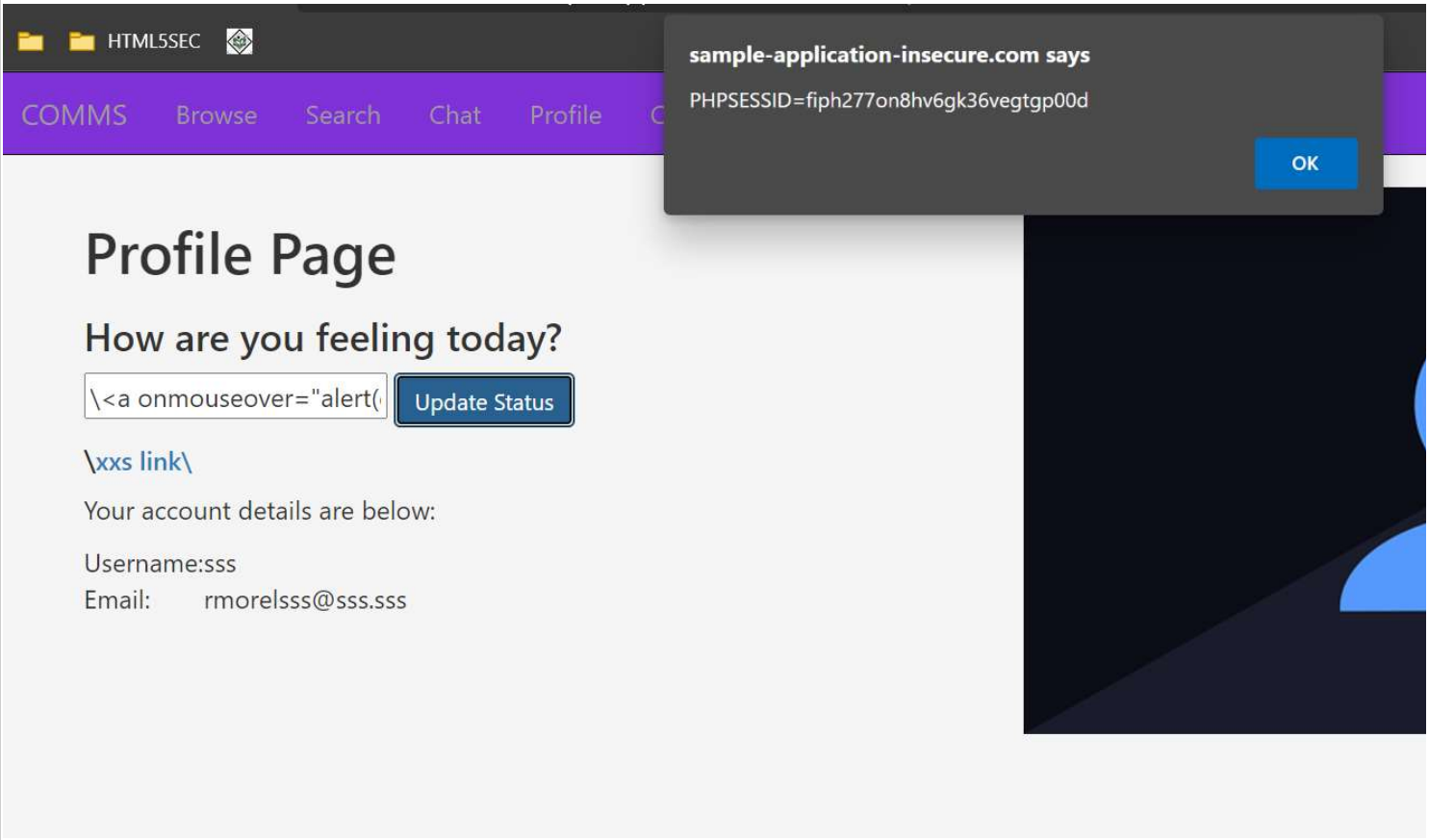
Able to enter script tags in status update form.

URL

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

Description

By entering a malicious string I am able to execute JavaScript payload.



Steps to reproduce

1. Login

2. Go to profile page
3. Enter xxs link in the status update field

Recommended fix

Sanitize all user input using a 3rd party library to prevent DOM based XSS.

Generated at Sun Dec 13 12:54:05 UTC 2020 by Robert Morel using Jira 1001.0.0-SNAPSHOT#100152-sha1:d8e2c464c38df4d324e50756a9cf9ad44685efeb.