


[HTML5SEC-50] Local and session storage in plain text 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-20201213-120256.png		
Rank:	0 j0008v:		

Description

Summary

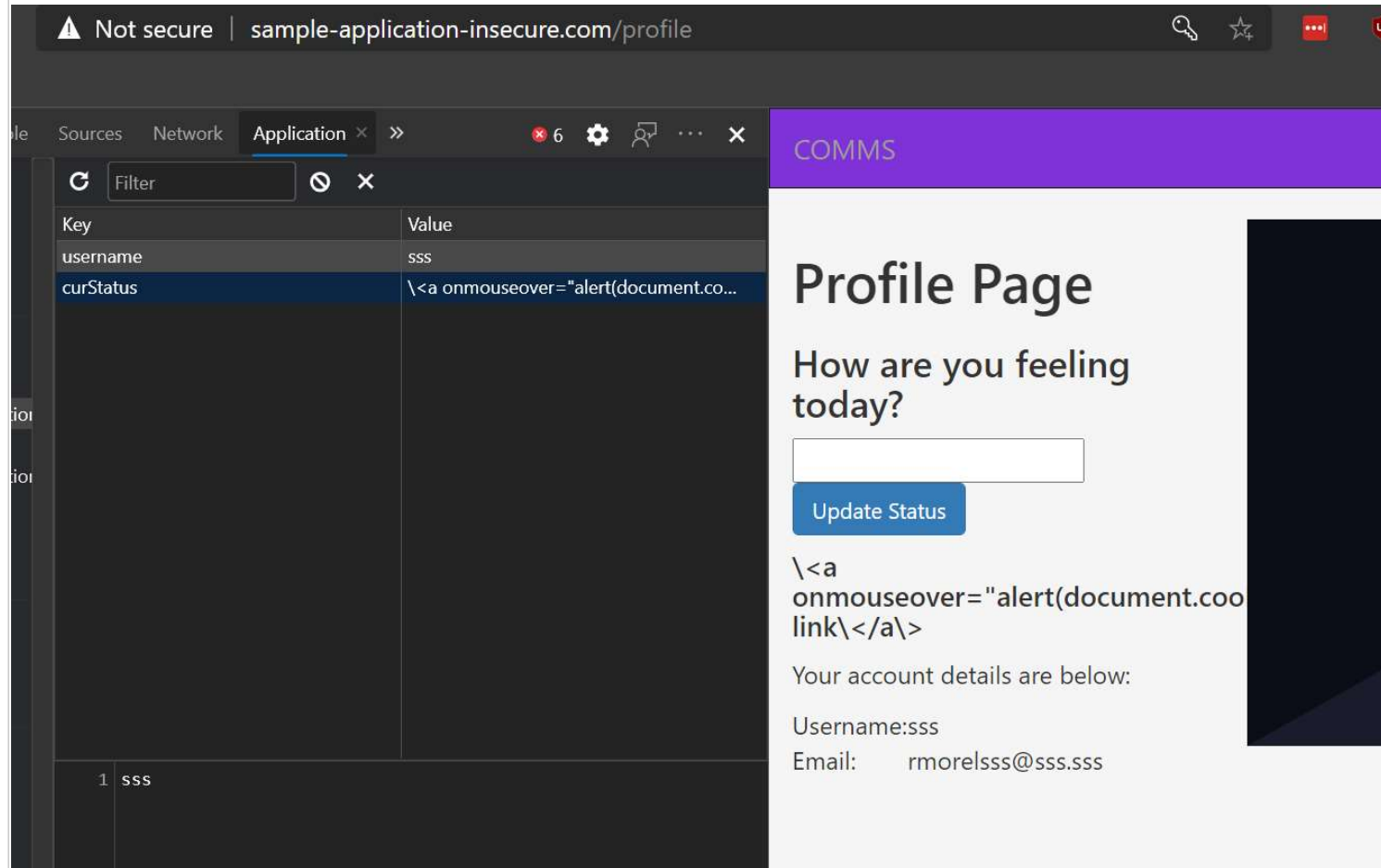
Able to steal local storage values using XSS

URL

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

Description

Their are several values stored in plain text in local and session storage that can be stolen in an XSS attack.



Steps to reproduce

1. Login
2. Go to profile page
3. Open dev tools and inspect the local and session storage
4. Username and email should not be stored on the client side
5. Status update should be encrypted

Recommended fix

Remove username and email from client storage

Encrypt the status update using a 3rd party library then decrypt before printing to profile page.

Generated at Sun Dec 13 12:54:40 UTC 2020 by Robert Morel using Jira 1001.0.0-SNAPSHOT#100152-sha1:d8e2c464c38df4d324e50756a9cf9ad44685efeb.