Zurmo-Stable-3.1.1
Cross Site Scripting (XSS)
Assigned CVE Number:
CVE-2017-7188

Proof-of-Concept

Submitted by:
Author: Faiz Ahmed Zaidi
Organization: Provensec LLC
Website: http://provensec.com/

National Vulnerability Database

(https://nvd.nist.gov/cvss/v2-calculator)

Overall CVSS Score: 4

CVSS v2 Vector(AV:N/AC:H/Au:S/C:P/I:P/A:P/E:ND/RL:OF/RC:C)

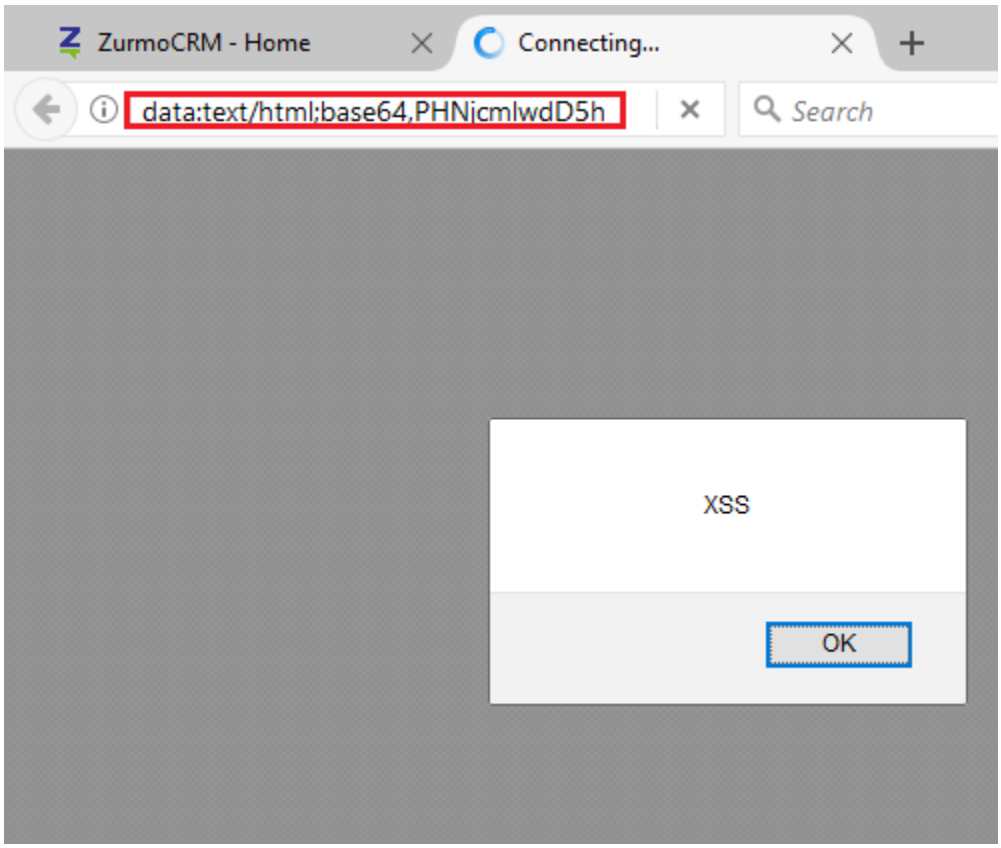
Proof-of-Concept

Hello,

I would like to report a vulnerability that I have found on zurmo-stable-3.1.1.7 in which is Cross-Site Scripting (XSS) attack is possible.

Hereby I am adding the information related to my finding so that you can have a brief view.

Technical Description: Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.
An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.



Vulnerability Type:
Cross Site Scripting (XSS)

Vendor of Product:
Zurmo Inc

Affected Product Code Base:
Zurmo CRM (http://zurmo.org/) - zurmo-stable-3.1.1.7b482704bc58

Affected Component:
https://localhost/zurmo/app/index.php/zurmo/default/toggleCollapse?returnUrl=
data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4=

Attack Type:
Remote

Attack Vectors:

Steps:

1.Login to zurmo-crm (tested on super user).
2.Open the url
"https://localhost/zurmo/app/index.php/zurmo/default/toggleCollapse?returnUrl
=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4=".
3.XSS gets executed
(xss payload is base64 encoded).

Reference:
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
