Affected software:

No-CMS - v1.1.3

Description:

No-CMS is a basic and "less-assumption" CMS with some default features such as user authorization (including third-party authentication), menu, module and theme management. It is fully customizable and extensible, you can make your own module and your own themes. It provides freedom to make your very own CMS, which is not provided very well by any other CMS.

Type of vulnerability:

XSS Persistent

URL:

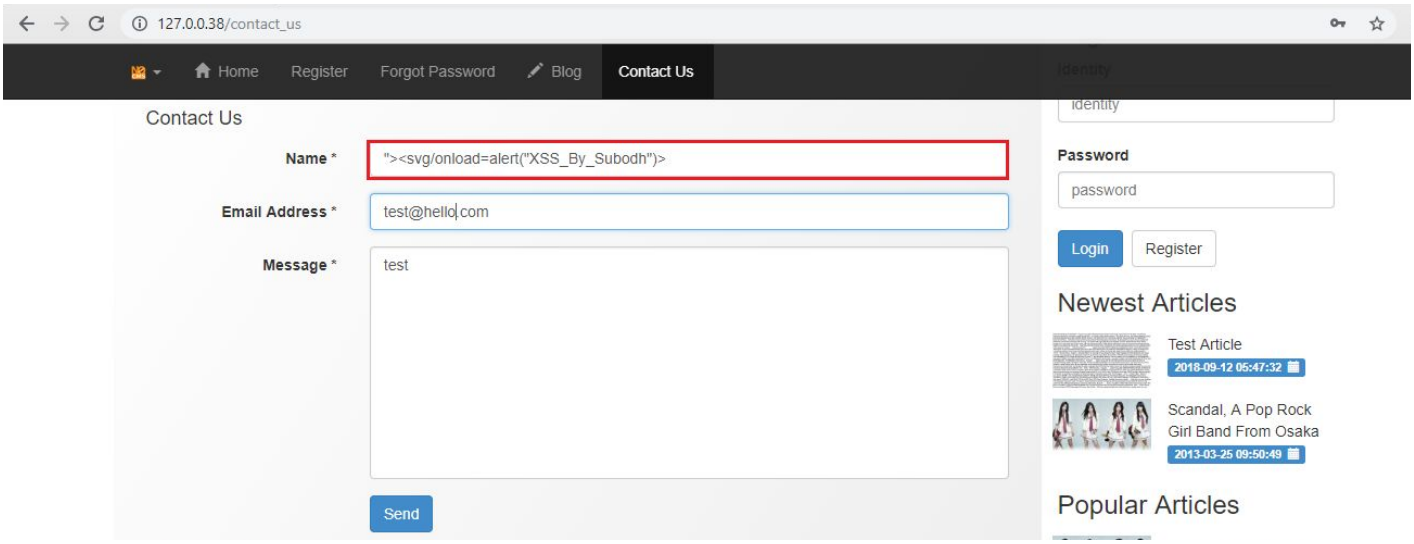
https://github.com/goFrendiAsgard/No-CMS

Vulnerability Description:

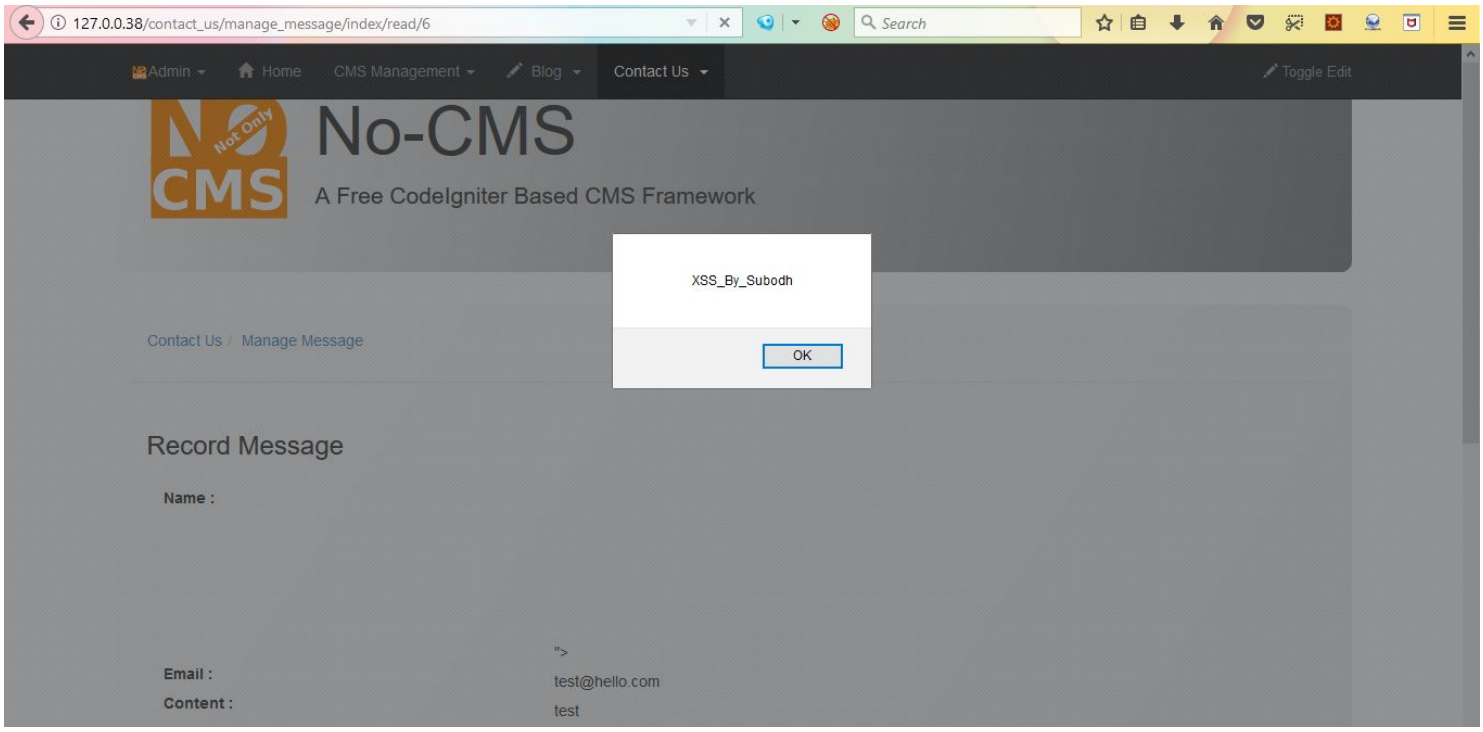
No-CMS is prone to a Persistent Cross-Site Scripting attack that allows a malicious user to inject HTML or scripts that can access any cookies, session tokens, or other sensitive information retained by the admin's browser and used with that site or can hijack admin's Browser.
Affected parameter:
VG48Z5PqVWname

Proof of concept

1. Open URL <Yoyrsite.com>/contact_us i.e. http://127.0.0.38/contact_us
2. Put XSS payload "><svg/onload=alert("XSS_By_Provensec")> in "VG48Z5PqVWname" parameter.



Now at the Admin end payload will be executed-
3 - Now, Login Admin account and open URL http://127.0.0.38/contact_us/manage_message
4 - Open Message sent with XSS payload (See Image2.png XSS payload is getting executed Here).



Author:

Subodh Kumar

Reference(s):

https://www.linkedin.com/in/subodh-kumar-8a00b1125/
https://twitter.com/Subodhk62060242
https://github.com/s-kustm