VULNERABLE A Stored Cross-Site Scripting (XSS) injection vulnerability exists in Emlog pro version 1.1.1 . An attacker can inject arbitrary javascripts in /admin/configure.php via footer_info param.

Date: 21/1/2022

Exploit Author: Trương Hữu Phúc

Contact me:

+ **Github**: https://github.com/truonghuuphuc

+ **Facebook**: https://www.facebook.com/DdosFulzac.auz1/

+ **Email**: phuctruong2k@gmail.com

Product: Emlog pro

Version: 1.1.1

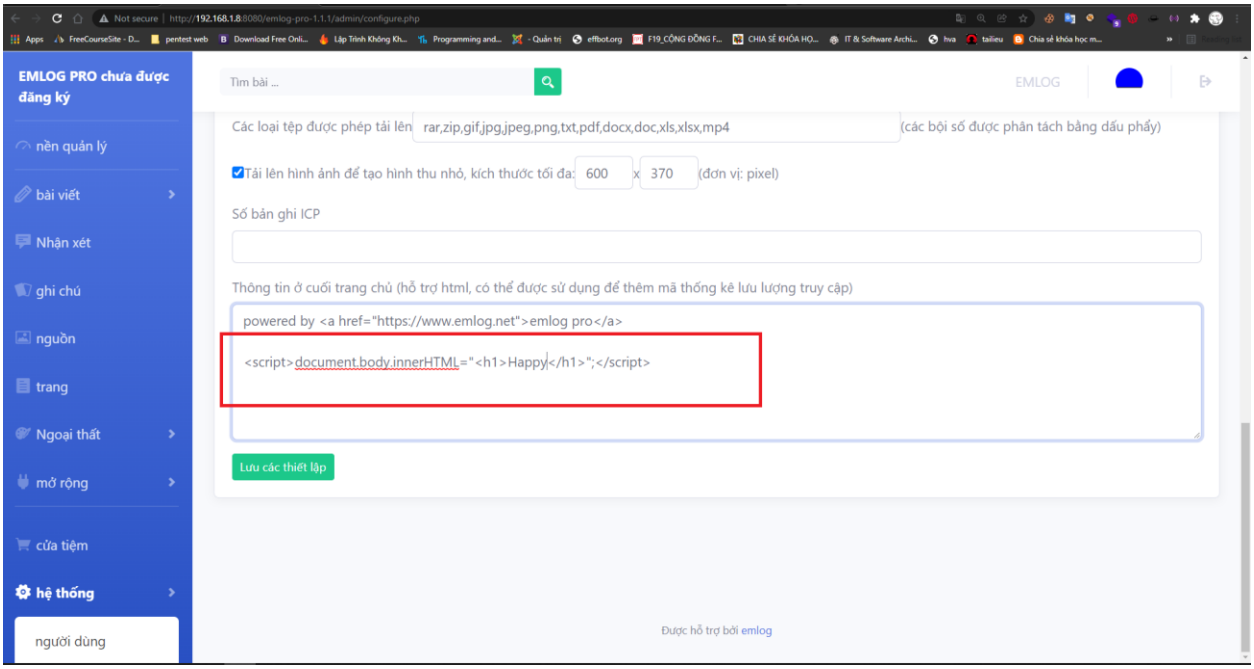
Description: The vulnerability is present in the "**/admin/configure.php**" and can be exploited throuth a POST request via the '**footer_info**' param.

Impact: An attacker can send javascripts code through any vulnerable form field to change the design of the website or any information displayed to the user, saving the information persistently on the site (e.g. database).

Suggestions: You should limit tag script and HTML Event Attributes.https://www.w3schools.com/tags/ref_eventattributes.asp

Proof of concept (POC):

Injection javascript:



As can be seen from the following evidence, the content of the injection was correctly saved on the page (on the database) and executed.