[#12503] A Reflected cross-site scripting (XSS) in 'm1_fmmessage' parameter

Created By: fuzzyap1 (fuzzyap1)
Date Submitted: Thu Dec 09 10:15:23 -0500 2021

Assigned To: CMS Made Simple Foundation (cmsmsfoundation)
Version: 2.1.5
CMSMS Version: 2.1.5
Severity: Minor
Resolution: None
State: Open
Summary:

A Reflected cross-site scripting (XSS) in 'm1_fmmessage' parameter
Detailed Description:

```
Technical description:
A Reflected cross-site scripting (XSS) vulnerability in CMS Made Simple 2.2.15
exists in the admin console via the global parameters of 'm1_fmmessage'
parameter. Once the user completes an action, the page returns a link with
'm1_fmmessage' parameters this vulnerability allows an attacker to execute
JavaScript in the context of the victim's browser if the victim opens a
vulnerable page containing an XSS payload.lead to cookie stealing, defacement
and more.

on case Steps to exploit:
1) Navigate to http://www.cmsms.com/admin/moduleinterface.php and delete any
file in 'file manage'
2) Insert your payload in the response url "m1_fmmessages" parameter
such as:
http://www.cmsms.com/admin/moduleinterface.php?mact=FileManager,m1_,defaultadmin,0&__c=34f443492bff76e8334&m1_fileactiondelete=&m1_path=%2Fupl
3) Refresh the page

Proof of concept (Poc):
The following payload will allow you to run the javascript :
<ScRiPt>alert(1)</ScRiPt>
```

History

- *1:* Home
- *2:* About
- *3:* Downloads
- *5:* Support
- *6:* Forum
- *7:* Development