[#12325] Multiple Cross Site Scripting Vulnerability on CMS Made Simple v2.2.14

Created By: SonGohan (SonGohan)
Date Submitted: Thu Jun 18 04:44:26 -0400 2020

Assigned To: Ruud van der Velden (ruudvdvelden)
Version: 2.2.13
CMSMS Version: 2.2.14
Severity: Major
Resolution: Fixed
State: Closed
Summary:
Multiple Cross Site Scripting Vulnerability on CMS Made Simple v2.2.14
Detailed Description:

```
1. Cross Site Scripting Vulnerability on "Manage Shortcuts" feature in CMS Made
Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability
in the "Manage Shortcuts" feature in CMS Made Simple v2.2.14.
**To Reproduce
Steps to reproduce the behavior:
+ Log into the panel.
+ Go to "/admin/listbookmarks.php?__c=ddbff7efd8130513d47"
+ Select "Manage Shortcuts"
+ Click "Add Shortcut"
+  Insert Payload in "Title":
                // # "><svg/onload=prompt(/SonGohan22/)>
                "><svg/onload=alert(document.domain)>
                "><img src onerror=alert("SonGohan22")>
+  Click "Submit"
+  View the preview to trigger XSS.
+  View the preview to get in request and such Stored XSS.
2. Cross Site Scripting Vulnerability on "Categories" via "Settings - New
Module" feature in CMS Made Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability
on "Categories" via "Settings - New Module" feature in CMS Made Simple v2.2.14.
**To Reproduce
Steps to reproduce the behavior:
+ Log into the panel.
+ Go to
"/admin/moduleinterface.php?mact=News,m1_,admin_settings,0&__c=bc3d9521e52526ae002"
+ Select "Categories"
+  Click "Add Category"
+  Insert Payload in "Name" or "Parent":
                // # "><svg/onload=prompt(/SonGohan22/)>
```

                ">><svg/onload=alert(document.domain)>
                ">><img src onerror=alert("SonGohan22")>
+ Click "Submit"
+ View the preview to trigger XSS.
+ View the preview to get in request and such Stored XSS.
3. Cross Site Scripting Vulnerability on "Options" via "Settings - New Module"
feature in CMS Made Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability
on "Options" via "Settings - New Module" feature in CMS Made Simple v2.2.14.
**To Reproduce
Steps to reproduce the behavior:
+ Log into the panel.
+Go to
"/admin/moduleinterface.php?mact=News,m1_,admin_settings,0&__c=bc3d9521e52526ae002"
+ Select "Options"
+ Insert Payload in "Email address to receive notification of news submission:"
or "The Subject of the outgoing email:":
                // # "><svg/onload=prompt(/SonGohan22/)>
                ">><svg/onload=alert(document.domain)>
                ">><img src onerror=alert("SonGohan22")>
+ Click "Submit"
+ View the preview to trigger XSS.
+ View the preview to get in request and such Stored XSS.
4. Cross Site Scripting Vulnerability on "Content Editing Settings" via
"Settings - Global Settings" feature in CMS Made Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability
on "Content Editing Settings " via "Settings - Global Settings" feature in CMS
Made Simple v2.2.14
**To Reproduce
Steps to reproduce the behavior:
+ Log into the panel.
+ Go to "/admin/siteprefs.php?__c=bc3d9521e52526ae002"
+ Select "Content Editing Settings"
+ Insert Payload in "Path for the {page_image} tag:" or "Path for thumbnail
field:", "Path for {content_image} tag:":
                // # "><svg/onload=prompt(/SonGohan22/)>
                ">><svg/onload=alert(document.domain)>
                ">><img src onerror=alert("SonGohan22")>
+ Click "Submit"
+ View the preview to trigger XSS.
+ View the preview to get in request and such Stored XSS.
5. Cross Site Scripting Vulnerability on "Admin Search" via "Extensions" feature
in CMS Made Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability
on "Admin Search" via "Extensions" feature in CMS Made Simple v2.2.14
**To Reproduce
Steps to reproduce the behavior:
+ Log into the panel.
+ Go to
"/admin/moduleinterface.php?mact=AdminSearch,m1_,defaultadmin,0&__c=bc3d9521e52526ae002"
+ Select "Admin Search"
+ Insert Payload in "Search Text":
                // # "><svg/onload=prompt(/SonGohan22/)>
                ">><svg/onload=alert(document.domain)>
                ">><img src onerror=alert("SonGohan22")>
+ Click "Submit"
+ View the preview to trigger XSS.
+ View the preview to get in request and such Stored XSS.
6. Cross Site Scripting Vulnerability on "Maintenance Mode" via "Settings -
Global Settings" feature in CMS Made Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability
on "Maintenance Mode" via "Settings - Global Settings" feature in CMS Made
Simple v2.2.14
**To Reproduce
Steps to reproduce the behavior:
+ Log into the panel.
+ Go to "/admin/siteprefs.php?__c=bc3d9521e52526ae002"
+ Select "Maintenance Mode"
+ Insert Payload in "Exclude these IP addresses from the "Site Down" status":
                // # "><svg/onload=prompt(/SonGohan22/)>
                ">><svg/onload=alert(document.domain)>
                ">><img src onerror=alert("SonGohan22")>
+ Click "Submit"
+ View the preview to trigger XSS.
+ View the preview to get in request and such Stored XSS.
7. Cross Site Scripting Vulnerability on "News" via "Content" feature in CMS
Made Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Stored XSS
vulnerabilityon "News" via "Content" feature in CMS Made Simple v2.2.14
**To Reproduce
Steps to reproduce the behavior:
+ Log into the panel.
+ Go to
"/admin/moduleinterface.php?mact=News,m1_,defaultadmin,0&__c=5cee6670e2dc3bc2e30"
+ Select "Add Article"
+ Insert Payload in "URL (slug)" or "Extra":
                // # "><svg/onload=prompt(/SonGohan22/)>
                ">><svg/onload=alert(document.domain)>
                ">><img src onerror=alert("SonGohan22")>
+ Click "Submit"
+ View the preview to trigger XSS.
+ View the preview to get in request and such Stored XSS.
8. Cross Site Scripting Vulnerability on "Design Manager" via "Layout" feature
in CMS Made Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Reflected XSS
vulnerability on "Design Manager" via "Layout" feature in CMS Made Simple
v2.2.14
**To Reproduce
Steps to reproduce the behavior:
+ Log into the panel.
+ Go to
"/admin/moduleinterface.php?mact=DesignManager,m1_,defaultadmin,0&__c=5cee6670e2dc3bc2e30"
+ Select "Stylesheets"
+ Click "Create a new Stylesheet"
+ Insert Payload in "*Name":
                // # "><svg/onload=prompt(/SonGohan22/)>
                ">><svg/onload=alert(document.domain)>
                ">><img src onerror=alert("SonGohan22")>
+ Click "Submit"
+ View the preview to trigger XSS.
+ View the preview to get in request and such Reflected XSS.
9. Cross Site Scripting Vulnerability on "Design Manager" via "Layout" feature
in CMS Made Simple v2.2.14
**Describe the bug
An authenticated malicious user can take advantage of a Reflected XSS
vulnerability on "Design Manager" via "Layout" feature in CMS Made Simple
v2.2.14
**To Reproduce
Steps to reproduce the behavior:
+ Log into the panel.
+ Go to
"/admin/moduleinterface.php?mact=DesignManager,m1_,defaultadmin,0&__c=5cee6670e2dc3bc2e30"
+ Select "Designs"
+ Click "Create a new Design"
Insert Payload in "*Name":
                // # "><svg/onload=prompt(/SonGohan22/)>
                ">><svg/onload=alert(document.domain)>
                ">><img src onerror=alert("SonGohan22")>
+ Click "Submit"
+ View the preview to trigger XSS.
+ View the preview to get in request and such Reflected XSS.
**Expected behavior
The removal of script tags is not sufficient to prevent an XSS attack.
You must HTML Entity encode any output that is stored back to the page.

**Impact
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.
**Screenshots
**Desktop (please complete the following information):
- OS: Ubuntu
- Browser: Firefox
- Version: 76.0.1

History

Comments

Date: 2020-09-18 07:59
Posted By: Ruud van der Velden (ruudvdvelden)

1. Valid but won't fix as it will only address the user who exploits this vulnerability.
We will work towards a better solution in the future

Date: 2020-09-18 08:36
Posted By: Ruud van der Velden (ruudvdvelden)

2. fixed
3. fixed
7. Url slug won't be fixed: value not accepted on submit
Extra field fixed

Date: 2020-09-18 09:06
Posted By: Ruud van der Velden (ruudvdvelden)

4. fixed in svn
5. Can't reproduce and can't imagine it goes beyond the submitting user itself
6 fixed in svn.
8. Won't fix: affects only submitting user. Name not stored
9. Won't fix: affects only submitting user. Name not stored

Thanks for reporting

Date: 2020-11-03 14:20
Posted By: Rolf (rolf1)

CMSMS 2.2.15 has been released

Updates

Updated: 2020-11-03 14:20
state: Open => Closed

Updated: 2020-09-18 09:06
resolution_id: 5 => 7

Updated: 2020-09-18 07:59
resolution_id: => 5
assigned_to_id: 12532 => 18365