


## [CMSMS](#) | [CMS Made Simple](#)

- [1: Home](#)
- [2: About](#)
  - [2.1: About Us](#)
  - [2.3: Testimonials](#)
  - [2.4: Merchandise](#)
  - [2.5: Donations](#)
  - [2.7: About This Website](#)
  - [2.8: Sitemap](#)
- [3: Downloads](#)
  - [3.1: File Releases](#)
  - [3.2: Demo](#)
  - [3.3: CMSms Themes Site](#)
  - [3.4: Modules](#)
  - [3.5: Tags](#)
- [5: Support](#)
  - [5.1: Documentation](#)
  - [5.2: FAQ](#)
  - [5.3: Blog](#)
  - [5.4: IRC](#)
  - [5.5: Participate](#)
  - [5.6: Report Bug or Feature Request](#)
  - [5.7: Mailing Lists](#)
  - [5.9: CMS Made Simple Hosting](#)
  - [5.10: Professional Services](#)
  - [5.11: Commercial License](#)
- [6: Forum](#)
  - [6.1: Rules](#)
  - [6.2: Announcements](#)
- [7: Development](#)
  - [7.1: Roadmap](#)
  - [7.3: CMSMS Forge](#)
  - [7.5: Translationcenter](#)

## CMS MADE SIMPLE FORGE

## CMS Made Simple Core

- [Summary](#)
- [Files](#)
- [Bug Tracker](#)
- [Feature Requests](#)
- [Code](#)
- [Forge Home](#)
- [Project List](#)
- [Recent Changes](#)
-  [Login](#)

 [Back to List](#)

## [#12321] Cross Site Scripting Vulnerability on "Logic" via Content Manager feature in CMS Made Simple v2.2.14



Created By: luuthehienhbit ([luuthehienhbit@gmail.com](mailto:luuthehienhbit@gmail.com))  
Date Submitted: Mon Jun 15 04:23:15 -0400 2020

Assigned To:  
Version: 2.2.14  
CMSMS Version: 2.2.14  
Severity: None  
Resolution: Won't Fix  
State: Closed  
Summary:  
Cross Site Scripting Vulnerability on "Logic" via Content Manager feature in CMS Made Simple v2.2.14  
Detailed Description:

**\*\*Expected behaviour**  
An authenticated malicious user can take advantage of a Stored XSS vulnerability on "Logic" via Content Manager feature in CMS Made Simple v2.2.14 feature.

**\*\*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.

**\*\*Steps to reproduce**  
1. Log into the Admin.  
2. Go to "Content Manager"  
3. Click "Logic"  
4. Add Payload on Page Specific Metadata:  
'><details/open/ontoggle=confirm(1337)>  
5. View Content Page

## History

### Comments



Date: 2020-09-15 04:08  
Posted By: Rolf ([rolf1](#))

Thanks for your report. The Logic field is meant to put code in and it is only accessible for approved administrators... If you don't trust your admins, don't give them access to (this field in) the admin panel.

#### Updates

Updated: 2020-11-03 14:42  
state: Open => Closed

Updated: 2020-09-15 04:08  
resolution\_id: 5 => 8  
severity\_id: 3 => 12

Updated: 2020-06-15 05:32  
summary: Cross Site Scripting Vulnerability on "Logic" via Content Manager feature in CMS Made Simple v2.2.14 => Cross Site Scripting Vulnerability on "Logic" via Content Manager feature in CMS Made Simple v2.2.14  
resolution\_id: => 5

- [1: Home](#)
- [2: About](#)
- [3: Downloads](#)
- [4: Support](#)
- [6: Forum](#)
- [7: Development](#)

CMS made simple is Free software under the GNU/GPL licence.

Website designed by [Steve Sicherman](#)