

master

...

[Research](#) / [codoforum](#) / [readme.md](#)

matuhn Update readme.md

History

1 contributor

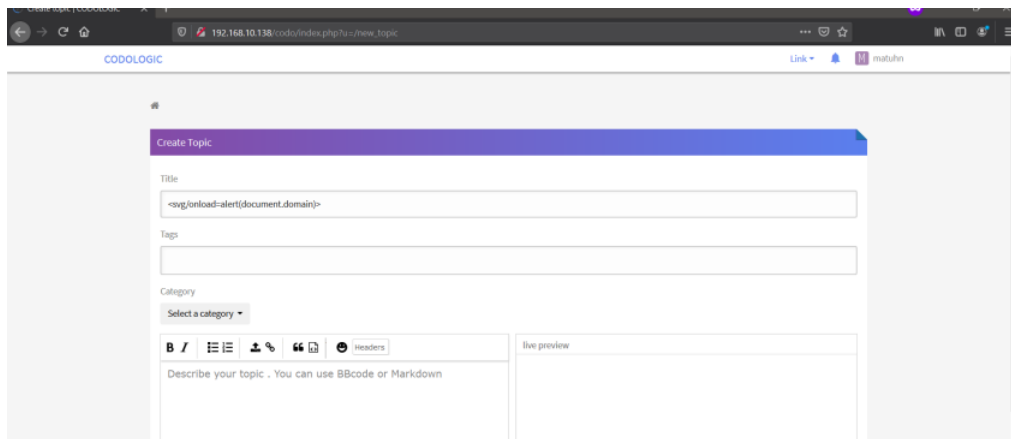
32 lines (28 sloc) | 1.29 KB

...

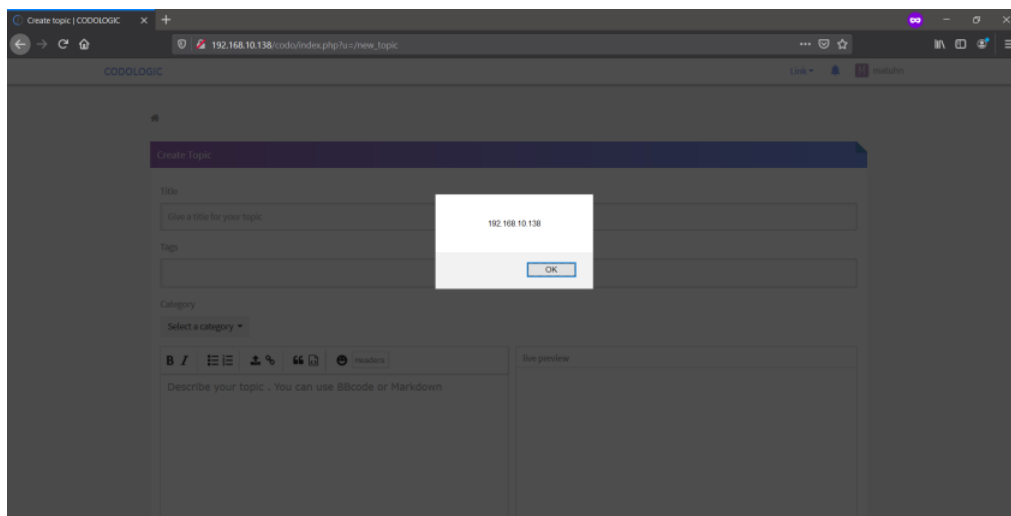
This is what I achived when research on [Codoforum](#)

Reflected XSS

Firstly, login into a user account, and create a new topic with title `<svg/onload=alert(document.domain)>`




Secondly, do nothing and refresh the page



It causes by this block of code


```
<div class="modal-header">
  <h4 class="modal-title">{_t("Pending draft")}</h4>
  <button type="button" class="close" data-dismiss="modal"><span
    aria-hidden="true">&times;</span><span class="sr-only">Close</span></button>
</div>
<div class="modal-body">
  <p>{_t("Your previous draft for topic ")}<span id="codo_draft_topic_title"></span>
    {_t("is pending")}</p>
  <p>{_t("If you continue, ")}<span id="codo_draft_topic_title"></span>
    {_t("your previous draft will be discarded.")}</p>
</div>
<div class="modal-footer">
```

Vendor confirmed



Khoa Bùi Đức Anh <khoabda305@gmail.com>
tới Codologic
any reply?
Vào Th 5, 27 thg 2, 2020 vào lúc 07:23 Khoa Bùi Đức Anh <khoabda305@gmail.com> đã viết:

09:15, Th 5, 27 thg 2 (5 ngày trước) ☆ ↶ ⋮



Codologic
tới tôi
Hi,
Sorry for the late reply.
We tested out the bugs you pointed out and have successfully reproduced them.
We are in a bit of a busy schedule to some server issues with some other product so we are having delays with development on codoforum.
We will probably release a new version with a fix in 2 weeks.
Regards

22:13 (41 phút trước) ☆ ↶ ⋮



Codologic Hôm qua
tới tôi ^



Từ admin@codologic.com Codologic •
Đến anhkhoafto@gmail.com Bùi Đức Anh Khoa •
Ngày 23:52, 13 Th2, 2020
Mã hóa tiêu chuẩn (TLS).
[Xem chi tiết bảo mật](#)

Hi,

Yes, we were able to reproduce the issue.
But since this is a self-XSS we will not be fixing it on priority
although you can go ahead and log a CVE.

Regards

[Hiển thị văn bản được trích dẫn](#)

--

Regards,

Team Codologic

REPORT TIMELINE

02/13/2020: Discovered the vulnerability

02/13/2020: Vendor confirmed

02/17/2020: CVE-2020-9007

Stored XSS

Create a post with Tags : 1" onmouseover="alert(1)

XSS will be fired if you put your mouse on tags

REPORT TIMELINE

02/24/2020: Discovered the vulnerability

03/03/2020: Vendor confirmed

Reflected XSS

Go to : [http://URL/codo/index.php?u=user/profile/11110%22%20accesskey=%22X%22%20onclick=%22alert\(1\)](http://URL/codo/index.php?u=user/profile/11110%22%20accesskey=%22X%22%20onclick=%22alert(1))

Use Alt+Shift+X , XSS will be fired

REPORT TIMELINE

02/24/2020: Discovered the vulnerability

03/03/2020: Vendor confirmed



Khoa Bùi Đức Anh <khoabda305@gmail.com>

tới Codologic

09:15, 27 thg 2, 2020 (5 ngày trước)



any reply?

Vào Th 5, 27 thg 2, 2020 vào lúc 07:23 Khoa Bùi Đức Anh <khoabda305@gmail.com> đã viết:



Codologic

tới tôi

22:13 (44 phút trước)



Hi,

Sorry for the late reply

We tested out the bugs you pointed out and have successfully reproduced them.

We are in a bit of a busy schedule to some server issues with some other product so we are having delays with development on codoforum.
We will probably release a new version with a fix in 2 weeks.

Regards