

[New issue](#)[Jump to bottom](#)

→ XSS within Route Error Page #46244

Closed

freakyclown opened this issue on Oct 14 · 4 comments · Fixed by #46269

Labels

actionpack

attached PR

security

freakyclown commented on Oct 14

After highlighting this issue to the Rails team via Hacker1, I was informed that this bug should be highlighted here upstream.

Whilst the issue is nothing critical, it is after all more of a self XSS, the ability to inject XSS attacks within the Rails framework is concerning. At a later date a vulnerability may be discovered that could leverage this issue or the code within this page could be reused elsewhere creating another attack vector that could be triggered by an attacker.

I am not an expert in Ruby or Rails and when I found this issue on a penetration test for a client, we discovered it was not an issue with the web application but one within Rails itself. The screenshot attached is therefore redacted of client identification.

Steps to reproduce

Request a page that does not have a matching routing to produce the Routing Error page.

Expected behavior

Expected behaviour is a error page with resources to help navigate the issue.

Actual behavior

Within the search box for Path, it is possible to create a XSS injection.

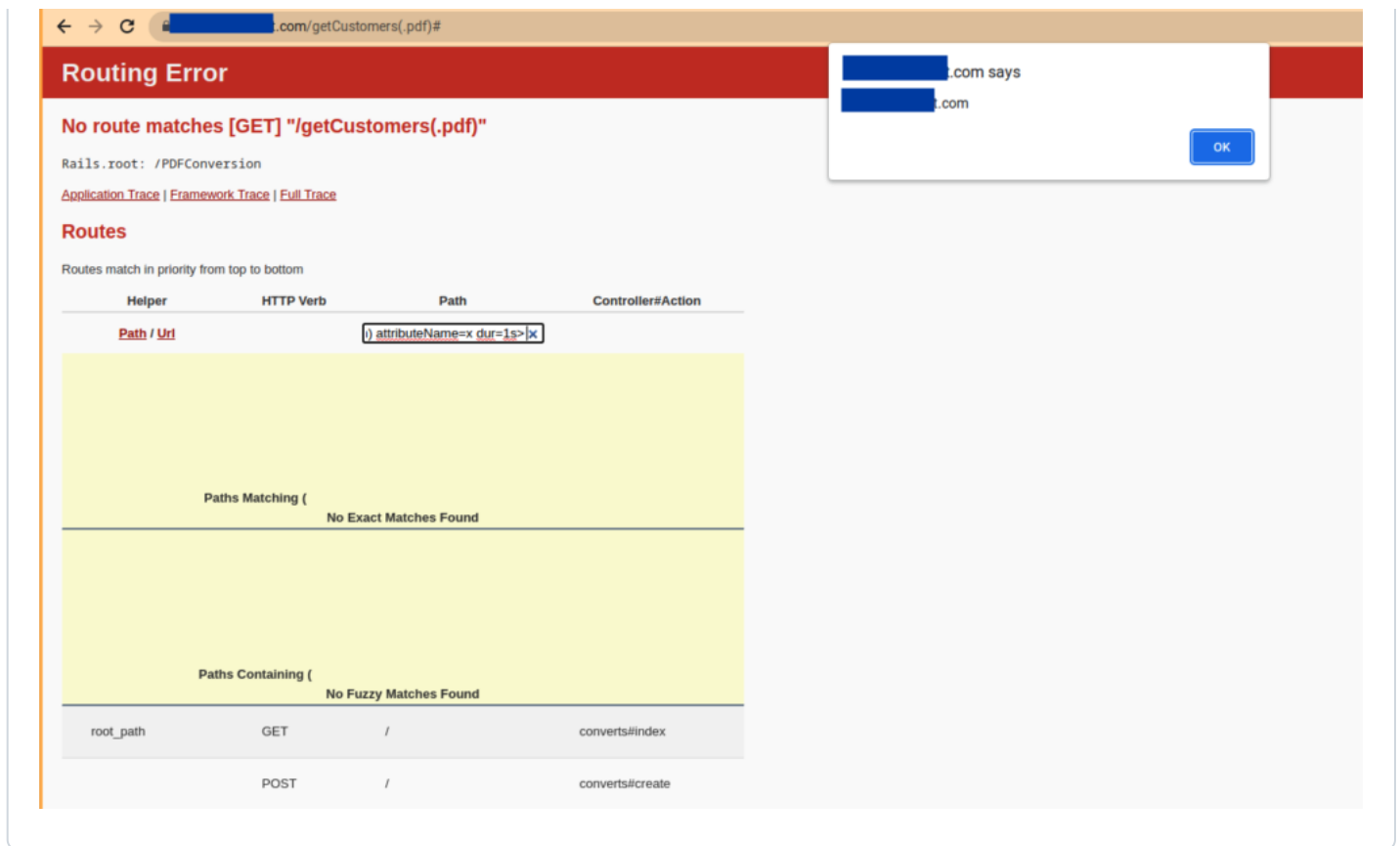
System configuration

Rails version:

No information on version from client

Ruby version:

No information on version from client.



 eileencodes added `security` `actionpack` labels on Oct 14

khall commented on Oct 14

Contributor

Can you be a bit more specific about how to reproduce the XSS injection?

freakyclown commented on Oct 17

Author

Sure, in the search bar input form. enter the following piece of code.

```
<svg><animate onend=alert(document.domain) attributeName=x dur=1s>
```

this will then bring up an alert box as per the image, giving proof of concept of the XSS vulnerability.

 codergeek121 added a commit to codergeek121/rails that referenced this issue on Oct 18


 Fix [rails#46244](#) Remove innerHTML usage to avoid self-XSS

✓ 9612fd5


 codergeek121 mentioned this issue on Oct 18

Fix [#46244](#) Remove innerHTML usage to avoid self-XSS [#46269](#)

 Merged

  **ghiculescu** added the `attached PR` label on Oct 20


 **codergeek121** added a commit to `codergeek121/rails` that referenced this issue on Oct 21

 Fix [rails#46244](#) Remove innerHTML usage to avoid self-XSS ✓ be177e4

 **byroot** closed this as completed in [#46269](#) on Oct 22

 **byroot** added a commit that referenced this issue on Oct 22

 Merge pull request [#46269](#) from `codergeek121/fix-xss-on-route-error-page` ... ✓ 87cf97b

 **byroot** added a commit that referenced this issue 24 days ago

 Merge pull request [#46269](#) from `codergeek121/fix-xss-on-route-error-page` ... ✓ cac3c8f

 **byroot** added a commit that referenced this issue 24 days ago

 Merge pull request [#46269](#) from `codergeek121/fix-xss-on-route-error-page` ... ✗ 1593b13

 **byroot** added a commit that referenced this issue 24 days ago

 Merge pull request [#46269](#) from `codergeek121/fix-xss-on-route-error-page` ... ✗ 5a7fa9a

ohsamarth commented 16 days ago

is there a fix for this issue for rails 5 yet?

 This was referenced 16 days ago

CVE 2022 3704 fix #46466

 Closed

Fixes for CVE-2022-3704 #46467

 Closed

ohsamarth commented 16 days ago

I have raised a Pull request for this issue against rails5.2-stable as well. Please check [#46467](#)

Assignees

No one assigned

Labels

actionpack attached PR security

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fix #46244 Remove innerHTML usage to avoid self-XSS**
codergeek121/rails

5 participants

