New issue

## XSS vulnerability in NotFoundExceptionMapper #7248

⊙ Closed blxbrgld opened this issue on Feb 18, 2020 · 10 comments · Fixed by #8207

Assignees area/security kind/bug Labels 中 1.3.1.Final

## blxbrgld commented on Feb 18, 2020

The no resource endpoint HTML page which is rendered on 404 errors introduces XSS vulnerability. Given as an example a GET endpoint which accepts a paging parameter in the form "start, offset" (i.e. 0,10). A request like:

/users?paging=0%2c-1sp137%3Cscript%3Ealert(1)%3C%2fscript%3Emzx4u

would lead to the following exception, and the 404 page in turn would execute the script (alert in our case).

RESTEASY003870: Unable to extract parameter from http request: javax.ws.rs.QueryParam("paging") value is '0,-1sp137<script>alert(1)</script>mzx4u'

## Implementation ideas

Enable the 404 HTML page only in DEV mode.

- blxbrgld added the area/housekeeping label on Feb 18, 2020
- smet added kind/bug and removed area/housekeeping labels on Feb 18, 2020

geoand commented on Feb 18, 2020 • edited 🕶

Contributor

Jump to bottom

Thanks for the report!

Isn't NotFoundExceptionMapper only enabled in dev-mode anyway?

Security label on Feb 18, 2020

asmet commented on Feb 21, 2020

@gastaldi would you have the cycles to check out this one?

Make sure this thing is only available in dev mode. And also, we should probably deal with escaping better than we currently do.

If you don't have the time, please say so. Thanks!

gastaldi commented on Feb 21, 2020

Collaborator

Sure, I can have a look

A gastaldi self-assigned this on Feb 21, 2020

Collaborator

The NotFoundExceptionMapper is only enabled in dev-mode indeed. The 404 page that this issue refers to is the one handled by Resteasy containing the error.

gastaldi commented on Feb 21, 2020 • edited 🔻

Collaborator

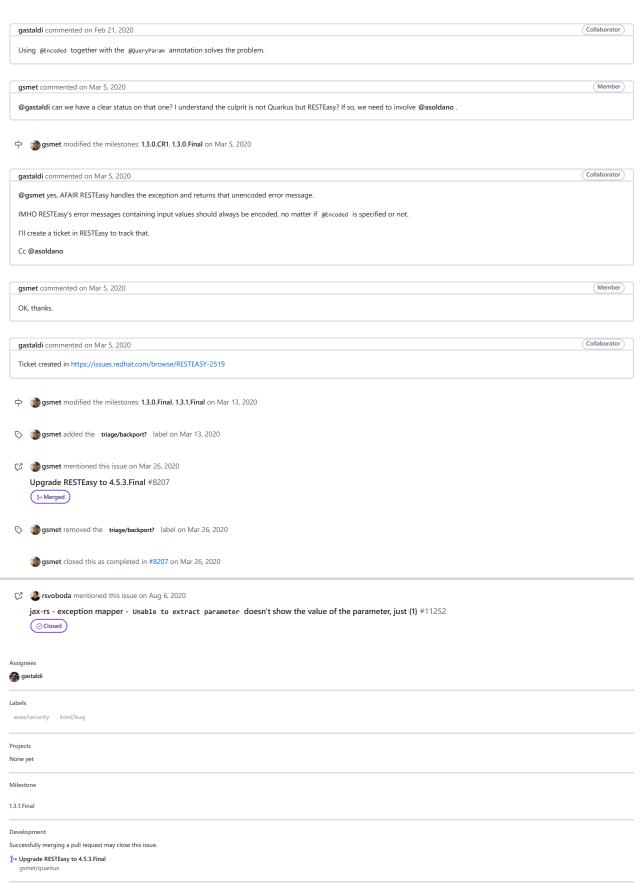
Remark: I am not even sure why a 404 is returned. It would be better to return 400 (Bad Request) instead.

EDIT: It's part of the spec:

A WebApplicationException thrown during construction of field or property values using 3 or 4 above

is processed directly as described in Section 3.3.4. Other exceptions thrown during construction of field or property values using 3 or 4 above are treated as client errors: if the field or property is annotated with @MatrixParam, @QueryParam or @PathParam then an implementation MUST generate an instance of NotFoundException (404 status) that wraps the thrown exception and no entity; if the

annotated with MHeaderParam or @CookieParam then an implementation MUST generate an instance of BadRequestException (400 status) that wraps the thrown exception and no entity.



5 participants

