

XML External Entity (XXE) Vulnerability in Latest Release #676

Open HatBoy opened this issue on Mar 21, 2019 · 1 comment

HatBoy commented on Mar 21, 2019

Hi, I would like to report XML External Entity (XXE) vulnerability in latest release.

Description:

XML External Entity (XXE) vulnerability in quokka/utlis/atom.py 157 line and auokka/core/content/views.py 94 line, Because there is no filter authors, title.

Steps To Reproduce:

1.Create a article, title and authors can insert XML payload.

2.Open the url:
















<http://192.168.100.8:8000/author/{author}/index.rss><http://192.168.100.8:8000/author/{author}/index.atom>

can see the title and authors has inserted into the XML.

CMS Home Articles Pages Administration ▼

ADMIN123 ▼

List (5) Create 20 items ▼ WITH SELECTED ▼

<input type="checkbox"/>		Title	Category	Authors	Date	Modified	Language	Published	View
<input type="checkbox"/>	 	test	test	admin	2019-03-20	2019-03-21	en		Preview
<input type="checkbox"/>	 	<script>alert(5)</script>	test	dj, <script>alert(2)</script>	2019-03-21	2019-03-21	en		View
<input type="checkbox"/>	 	<script>alert(5)</script>	test	dj, <script>alert(2)</script>	2019-03-21	2019-03-21	en		Preview
<input type="checkbox"/>	 	test	test	tttt	2019-03-21	2019-03-21	en		View
<input type="checkbox"/>	 	<script>alert(5)</script>	test	dj, <script>alert(2)</script>	2019-03-21	2019-03-21	en		Preview

← → ↺ ⌂ ① 不安全 | 192.168.100.8:8000/tag/script-alert-5-script/index.rss

☆ 🌐 📄 📁 📂 📅 📆 📇 📈 📉 📊 📋 📌 📍 📎 📏 📐 📑 📒 📓 📔 📕 📖 📗 📘 📙 📚 📛 📜 📝 📞 📟 📠 📡 📢 📣 📤 📥 📦 📧 📨 📩 📪 📫 📬 📭 📮 📯 📰 📱 📲 📳 📴 📵 📶 📷 📸 📹 📺 📻 📼 📽 📾 📿 📰 📱 📲 📳 📴 📵 📶 📷 📸 📹 📺 📻 📼 📽 📾 📿

http://192.168.100.8:8000/Quokka Site | Tag | RSS feeden-usAll rights reserved.Thu, 21 Mar 2019 14:46:53 GMTThu, 21 Mar 2019 16:34:05 GMTscript-alert-5-scriptPySS2Gen-1.1.0http://blogs.law.harvard.edu/tech/rsshttp://192.168.100.8:8000/test/script-alert-5-script.html<![CDATA[<script>alert(5)</script>]]>dj, <script>alert(2)</script><quokka.core.content.models.Tag object at 0x7fc145bad3c8>]9e582bb105e977cfcb00abd6365ee389fe573d5Thu, 21 Mar 2019 14:46:53 GMT

← → ↺ ⌂ ① 不安全 | 192.168.100.8:8000/tag/script-alert-5-script/index.atom

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom">
  <title type="text">Quokka Site | Tag | atom feed</title>
  <id>http://192.168.100.8:8000/tag/script-alert-5-script/index.atom</id>
  <updated>2019-03-21T14:48:10Z</updated>
  <link href="http://192.168.100.8:8000/" />
  <link href="http://192.168.100.8:8000/tag/script-alert-5-script/index.atom" rel="self" />
  <generator>Werkzeug</generator>
  <entry xml:base="http://192.168.100.8:8000/tag/script-alert-5-script/index.atom">
    <title type="text"><script>alert(5)</script></title>
    <id>http://192.168.100.8:8000/test/script-alert-5-script.html</id>
    <updated>2019-03-21T14:48:10Z</updated>
    <published>2019-03-21T14:46:53Z</published>
    <link href="http://192.168.100.8:8000/test/script-alert-5-script.html" />
    <author>
      <name>dj, <script>alert(2)</script></name>
    </author>
    <content type="html"><![CDATA[
      <script>alert(5)</script>
    ]]></content>
  </entry>
</feed>
```

author by jin.dong@dbappsecurity.com.cn

 marcosptf mentioned this issue on May 19, 2019

fixing vulnerability: XXE #679

Open

marcosptf commented on Jul 17, 2019

Collaborator

was removed WIP from pr and fixed this issue:
hotfix ready to merge: please make your comments and reviews:
[#679](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

