

Cross-site Scripting (XSS) - Stored in snipe/snipe-it

Valid Reported on Nov 21st 2021

0

Description

Cross site scripting vulnerability in checkout page in notes field

Proof of Concept

1.Login to the demo page.
Go to accessories , select any product and add payload in the checkout notes
click save and open the product xss will trigger
payload = ">

Impact

This vulnerability is capable of stolen the user cookie

References

- <https://portswigger.net/web-security/cross-site-scripting>

CVE

CVE-2021-4018

(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity

Medium (6.3)


Visibility

Public

Status

Fixed

Found by




Asura-N

@asura-n

noisy

Fixed by



snipe

@snipe

maintainer

This report was seen 424 times.

- We are processing your report and will contact the **snipe/snipe-it** team within 24 hours. a year ago
- Asura-N modified the report a year ago
- Asura-N modified the report a year ago
- We have contacted a member of the **snipe/snipe-it** team and are waiting to hear back. a year ago
- snipe validated this vulnerability a year ago
- Asura-N has been awarded the disclosure bounty ✓
- The fix bounty is now up for grabs
- snipe marked this as fixed in 5.3.3 with commit ff81e6 a year ago
- snipe has been awarded the fix bounty ✓
- This vulnerability will not receive a CVE ✗

Jamie Slome a year ago

Admin

CVE published! 🎉

Chat with us

Sign in to join this conversation

2022 © 418sec

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)