

## Improper Access Control in snipe/snipe-it

0

✓ Valid

Reported on Feb 23rd 2022

### Description

It was found that if a user is not having access to the requested items module, a normal user with no access can still access and view the requested content.

It is a more detailed explanation of the given report where it was marked as invalid :

<https://huntr.dev/bounties/783cfb0c-7e4d-4fdd-86c6-bd92743aee41/>

### Proof of Concept

Create two users, one admin and one normal user(Only give view accessories access to the normal user)

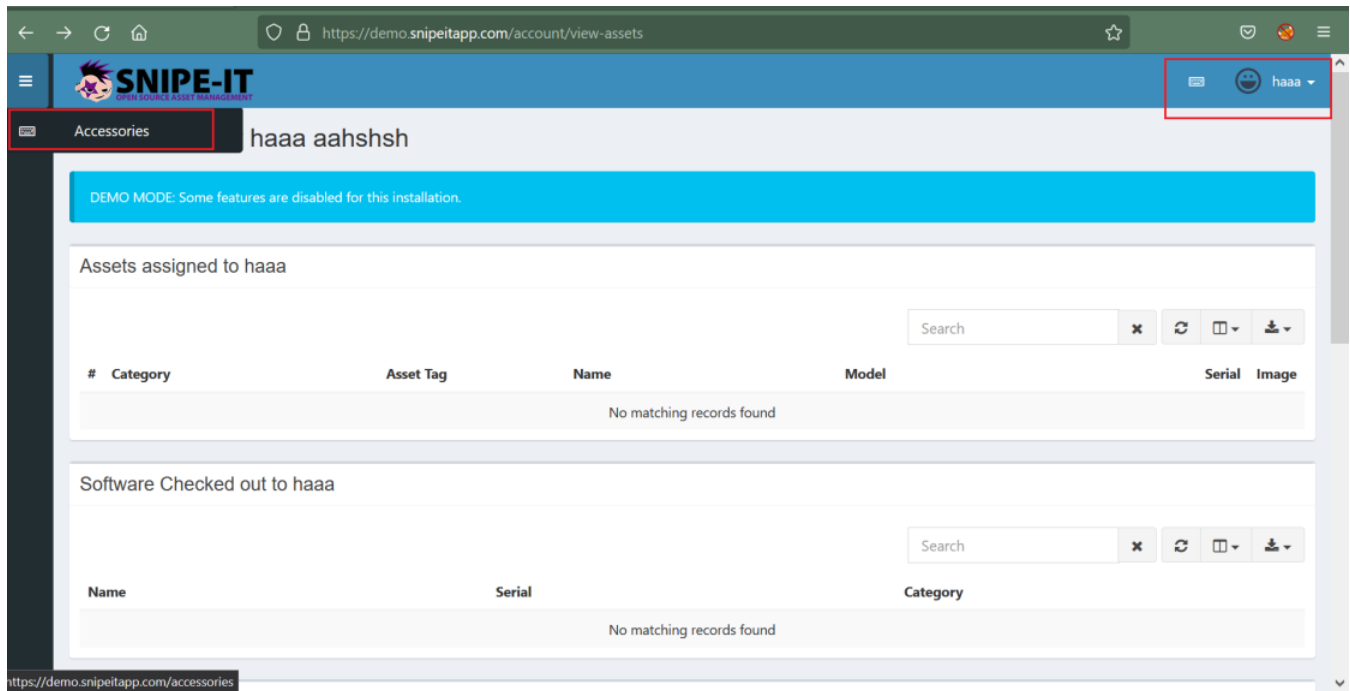
In the screenshot, you can see the normal user is not having access to the requested module. But with forced browsing, we can clearly see that the normal user can access the requested module.

### Screenshots

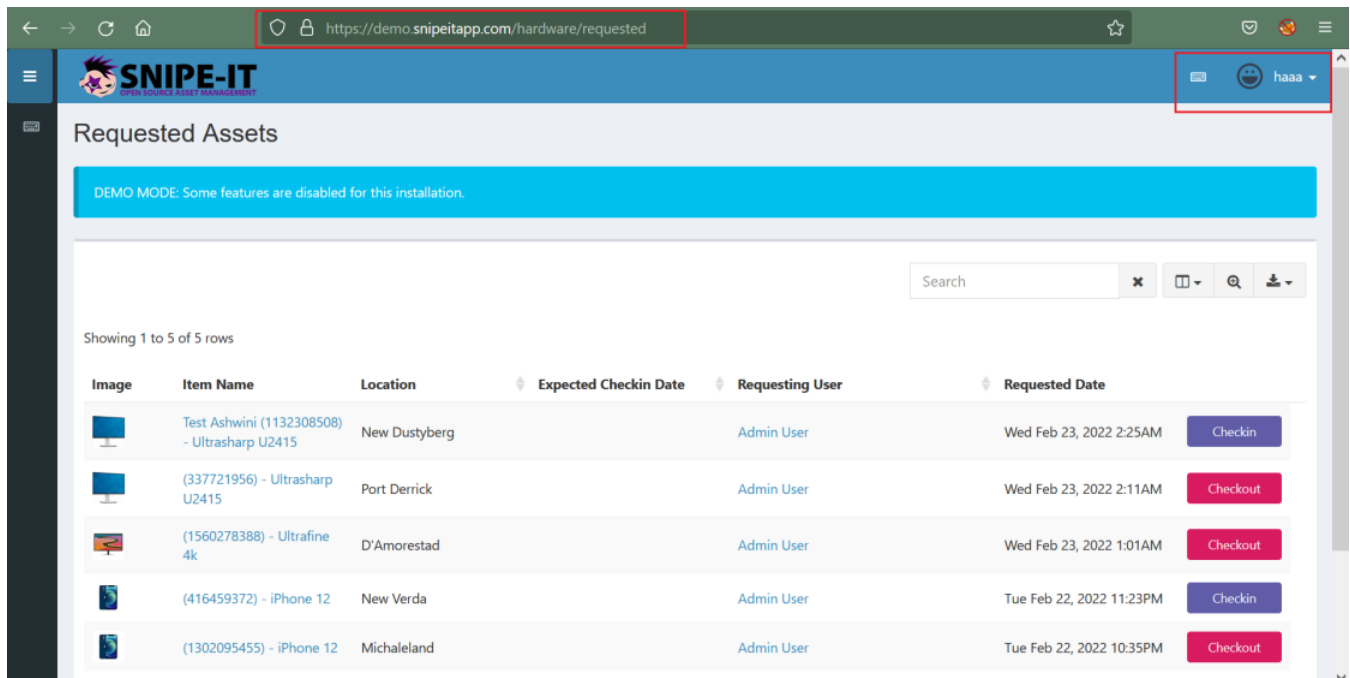
#### Accessories view permission to normal user

Accessories	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
View	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Create	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Edit	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Delete	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Checkout	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Checkin	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Chat with us



## Normal user view requested items



## Impact

This vulnerability will help an attacker view restricted content.

Chat with us

## CVE

CVE-2022-1511

(Published)

## Vulnerability Type

CWE-284: Improper Access Control

## Severity

Medium (6.5)

## Visibility

Public

## Status

Fixed

## Found by



shubh123-tri

@shubh123-tri

unranked ▼

## Fixed by



snipe

@snipe

maintainer

This report was seen 689 times.

We are processing your report and will contact the **snipe/snipe-it** team within 24 hours.

9 months ago

shubh123-tri modified the report 9 months ago

shubh123-tri modified the report 9 months ago

We have contacted a member of the **snipe/snipe-it** team and are waiting to hear back

9 months ago

We have sent a follow up to the **snipe/snipe-it** team. We will try again in 7 d

Chat with us

We have sent a second follow up to the **snipe/snipe-it** team. We will try again in 10 days.

9 months ago

We have sent a third and final follow up to the **snipe/snipe-it** team. This report is now considered stale. 8 months ago

**snipe** validated this vulnerability 7 months ago

**shubh123-tri** has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

**snipe** marked this as fixed in **5.4.4** with commit **2e9cf8** 7 months ago

**snipe** has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

part of 418sec

company

about

team

Chat with us

[terms](#)

[privacy policy](#)

[Chat with us](#)