Stored Cross Site Scripting vulnerability in the checked_out_to parameter in snipe/snipe-it

0

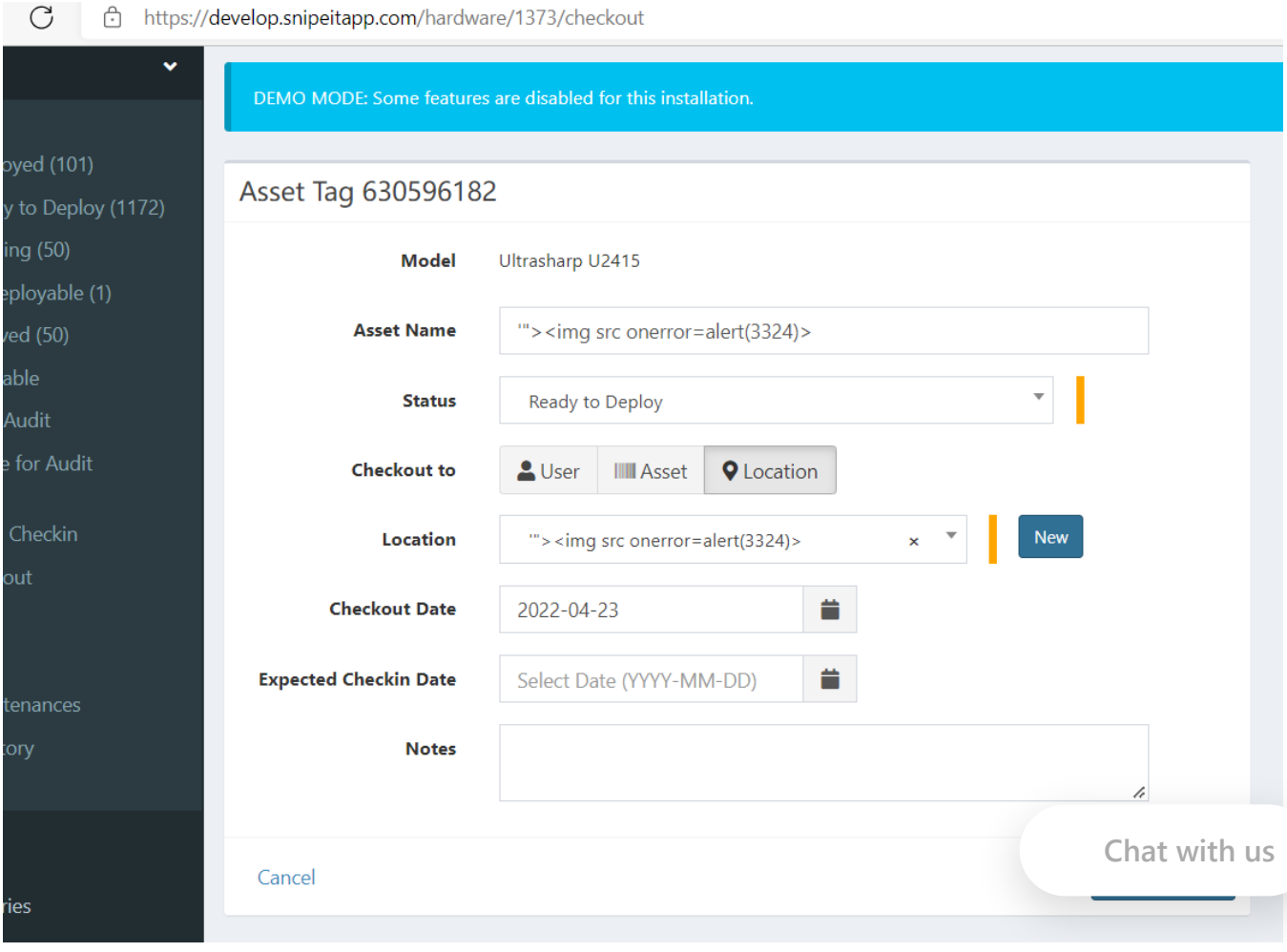
Valid Reported on Apr 23rd 2022

Description

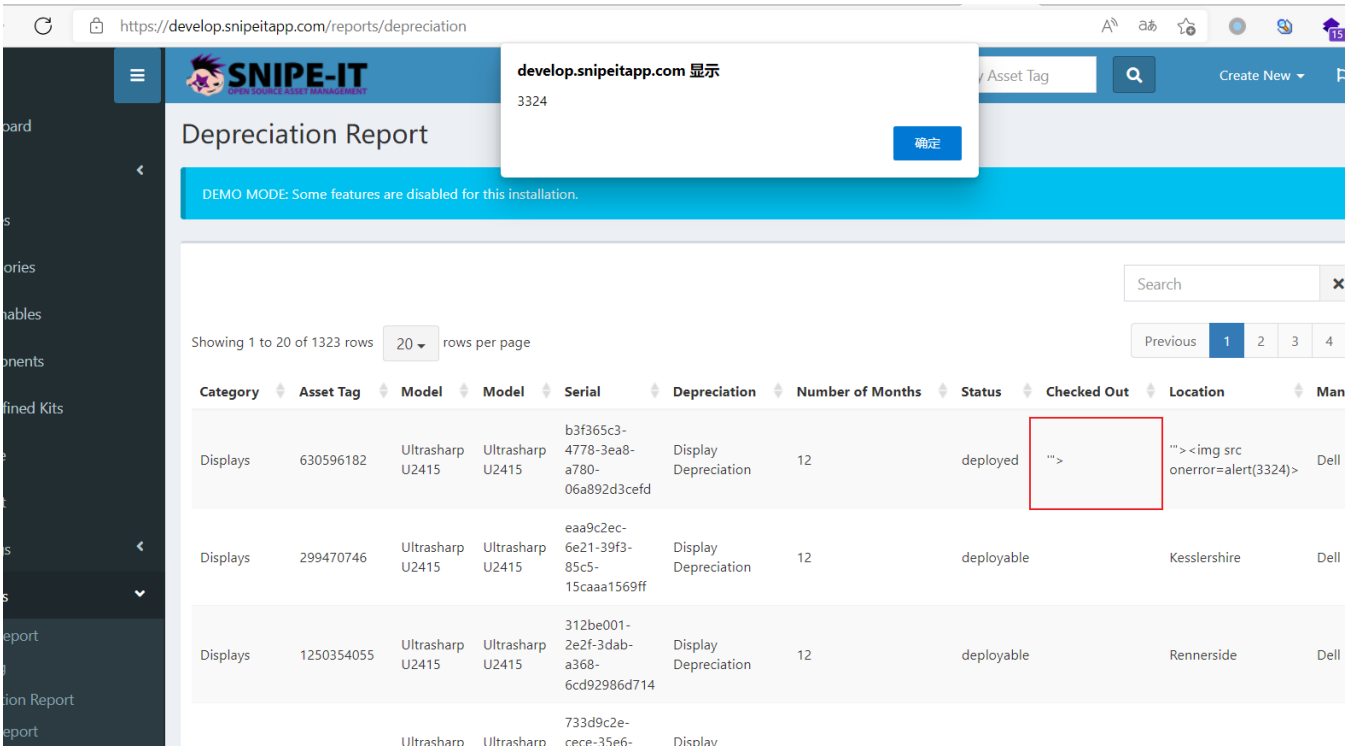
The checked_out_to is not escaped, which leads to a XSS problem.

Proof of Concept

1.Login to the demo account
2.Report->Depreciation Report
3.Choose a Asset and goto Assets menu and check it out. new a location which is `'"><img src onerror=alert(3324)>` and check the asset to this location



4.Return to Depreciation Report,refresh,a lert will be triggered




```
"><img src onerror=alert(3324)>
```

Impact

The vulnerability is capable of stolen the user Cookie.

Occurrences

DepreciationReportTransformer.php L101

CVE
CVE-2022-1445
(Published)

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

Severity
Critical (9)

Registry

Packagist

Affected Version
5.4.3

Visibility
Public

Status
Fixed

Found by

mylong
@mylong
unranked

Fixed by

snipe
@snipe
maintainer

This report was seen 693 times.

We are processing your report and will contact the **snipe/snipe-it** team within 24 hours. 7 months ago

mylong modified the report 7 months ago

mylong submitted a patch 7 months ago

mylong submitted a patch 7 months ago

We have contacted a member of the **snipe/snipe-it** team and are waiting to hear back 7 months ago

snipe validated this vulnerability 7 months ago

mylong 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 **5.4.3** with commit **f623d0** 7 months ago

snipe has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

DepreciationReportTransformer.php#L101 has been validated ✔

Sign in to join this conversation