harsh-bothra / **CVE-2020-23868**

Last active 2 years ago

Cross-Site Scripting in NeDi 1.9C

CVE-2020-23868

```
Product: NeDi - Find IT

CVE: Use CVE-2020-23868

Version: 1.9C

Vulnerability: Reflected Cross-Site Scripting

Vulnerability Description:  NeDi 1.9C allows Cross-Site Scripting via "d" parameter at "inc/rt-popup.ph" page.

# Steps to Reproduce

1. Log in to the application with provided credentials.
2. Navigate to "https://<nedi_server_ip>/inc/rt-popup.php" page.
3. Add "d" parameter at the end of the URL with XSS Payload like below:
> https://<nedi_server_ip>/inc/rt-popup.php?d=<img src=1 onerror=alert(document.domain)>
4. Observe that the XSS Payload provided in Step-3 is executed.
```