Yogosha

Reflected Cross Site Scripting

Submitted by : Pradeep , 4/2/18, 5:43:25 PM
Bug Bounty Connect Bug Bounty

Vulnerability

Cross Site Scripting (XSS)

Severity Level

HIGH More...

URL/Location

https://connect.nuxeo.com/nuxeo/site/studio/v2/project/project-name/workspace/ws.resources/nuxeo.war/%3Cimg%20src=s%20onerror=alert(1)%3E

Parameter

URL

Description

The below URL is vulnerable to Reflected XSS.

URL:

https://connect.nuxeo.com/nuxeo/site/studio/v2/project/*project-name*/workspace/ws.resources/nuxeo.war/<img >

Remediation:
Proper output encoding
Input sanitization

Please let me know if more info is needed

Proof of concept

URL:

Replace the project-name in URL with the project-name

https://connect.nuxeo.com/nuxeo/site/studio/v2/project/project-name/workspace/ws.resources/nuxeo.war/<img >