New issue

Jump to bottom

[SECURITY] - Stored Cross-site Scripting while deleting a scan engine in the Scan Engine deletion confirmation modal box! #460

Closed **TheBinitGhimire** opened this issue on Aug 19, 2021 · 0 comments

Labels Security **Work in Progress**

TheBinitGhimire commented on Aug 19, 2021 • edited Contributor

Issue Summary

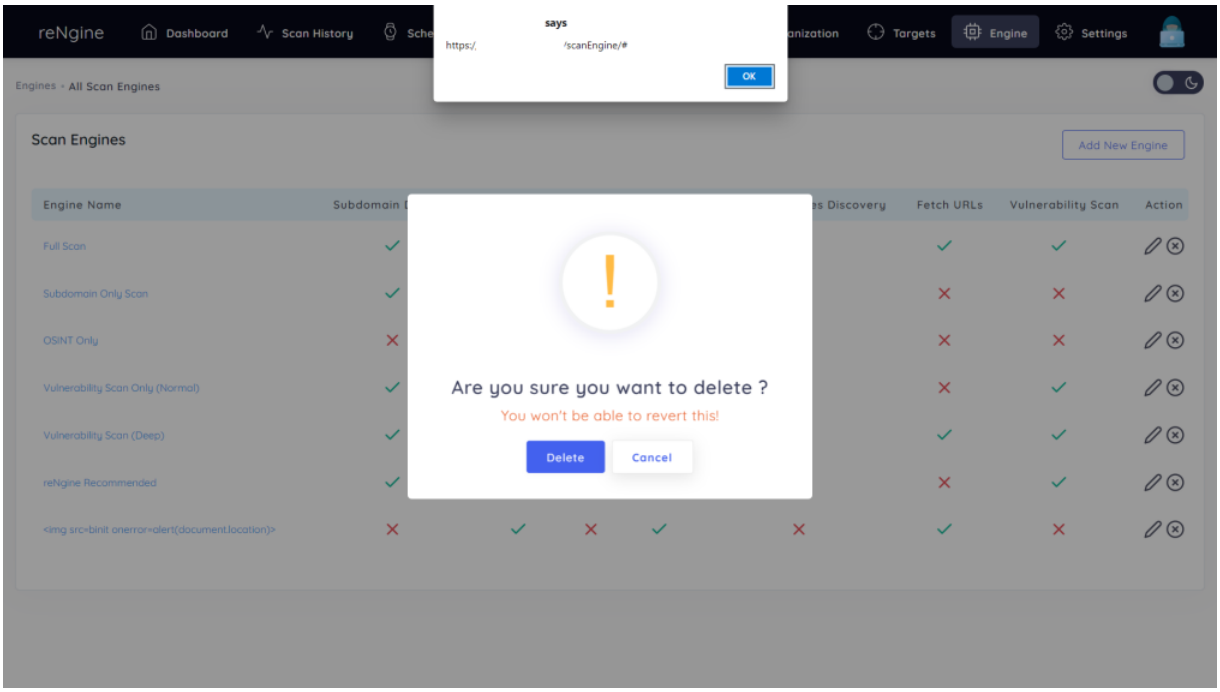
In reNgine v1.0, there is Stored Cross-site Scripting while deleting a Scan Engine in the Scan Engine deletion confirmation modal box!

Steps to Reproduce

1. Visit your reNgine instance, and login to your account.
2. Head over to the `/scanEngine/` endpoint.
3. Click on "Add New Engine" and write `<img src=binit onerror=alert(document.location)>` in the **Engine name** field.
4. Now, click on the "Add Engine" button to save the changes.
5. Click on the cross icon under the **Action** column, which is used for deleting the scan engine.

You will notice that, while displaying "Are you sure you want to delete {Scan_Engine_Name}?", it will render our Scan Engine Name as it is without performing any sort of sanitization, which results in our JavaScript code inside the XSS payload being executed.

This is how this vulnerability can be reproduced.



- I have confirmed that this issue can be reproduced as described on a latest version/pull of reNgine: **yes**

Technical details

- Debian 4.19.181-1

yogeshojha added Security **Work in Progress** labels on Aug 23, 2021

yogeshojha added a commit that referenced this issue on Aug 23, 2021

`Fixed #459 #460 XSS` `412c5ce`

yogeshojha closed this as completed in `3dc7f11` on Aug 23, 2021

Assignees

No one assigned

Labels

Security **Work in Progress**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants