

New issue

[Jump to bottom](#)

Stored XSS when deleting proxy host #1950


Closed
 I4rm4nd opened this issue on Mar 24 · 2 comments


Labels bug

I4rm4nd commented on Mar 24 · edited

Steps to reproduce:

1. Login as administrative user
2. Create a new proxy host entry with the payload `<script>alert('XSS')</script>.google.com` as domain
3. Hit save
4. Try to delete the newly added proxy host. XSS payload is executed.





 Nginx Proxy Manager

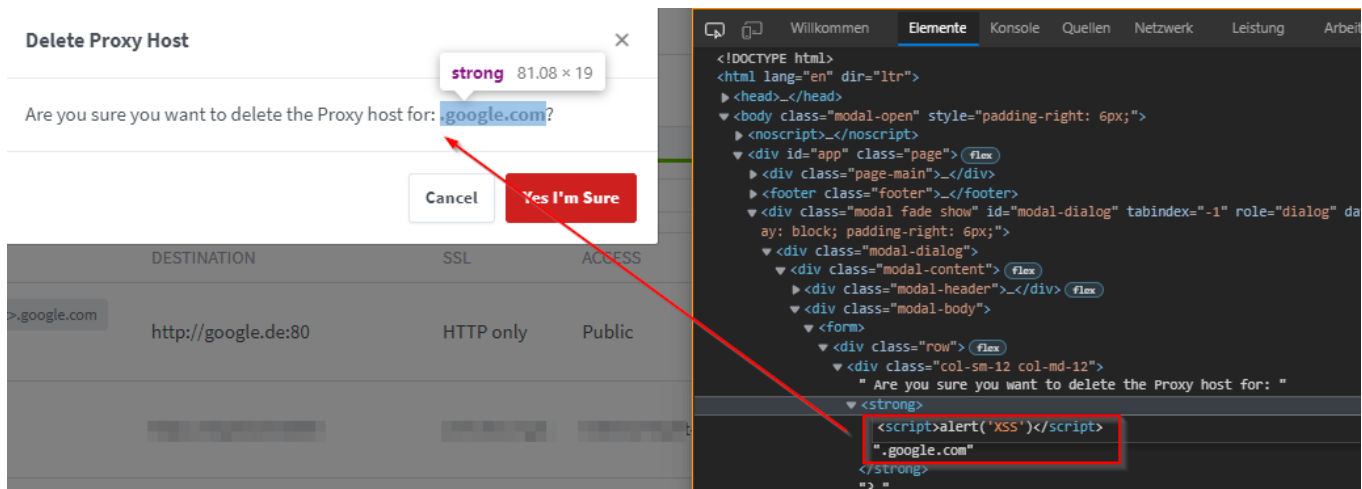
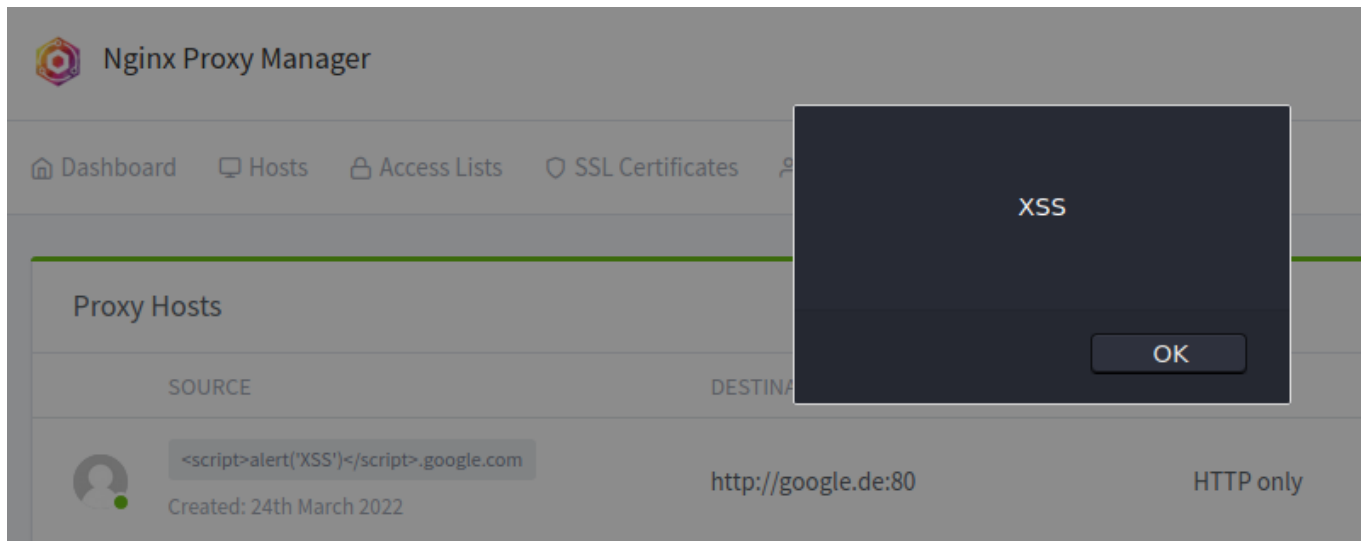

 Administrator

[Dashboard](#)
[Hosts](#)
[Access Lists](#)
[SSL Certificates](#)
[Users](#)
[Audit Log](#)
[Settings](#)

Proxy Hosts

?
Add Proxy Host

SOURCE	DESTINATION	SSL	ACCESS	STATUS
 <div> <div> <div><script>alert('XSS')</script>.google.com</div> <div>Created: 24th March 2022</div> </div> </div>	http://google.de:80	HTTP only	Public	<div>● Online</div> <div>⋮</div> <div> <div>Proxy Host #24</div> <div>Edit</div> <div>Disable</div> <div>Delete</div> </div>
				
				



Recommendation:

Implementing input validation and/or ensuring output sanitization as done for all other inputs/outputs.

Risk:

Low risk since high privileges are required.

l4rm4nd added the `bug` label on Mar 24

l4rm4nd commented on Mar 24

Author

Also works for redirection hosts with XSS domain payloads. If a redirection host is deleted, XSS payload is executed.

jc21 closed this as completed in [feaafdc](#) on Mar 24

 **jc21** added a commit that referenced this issue on Mar 24



Merge pull request [#1951](#) from NginxProxyManager/test-html-encode ...

✓ 3538f97

jc21 commented on Mar 24

Member

Thanks for the pickup.

Fixed in `develop` branch and will be out with the next release.



1

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

