New issue

Jump to bottom

Reflected XSS Vulnerability on Docker: dotcms/dotcms:21.05.1 #20541

Closed r0ck3t1973 opened this issue on Jun 15, 2021 · 2 comments

Labels Type : Bug

r0ck3t1973 commented on Jun 15, 2021

Describe the bug
Hi Team
I found small reflected xss dotcms/dotcms:21.05.1
install: Docker: dotcms/dotcms:21.05.1

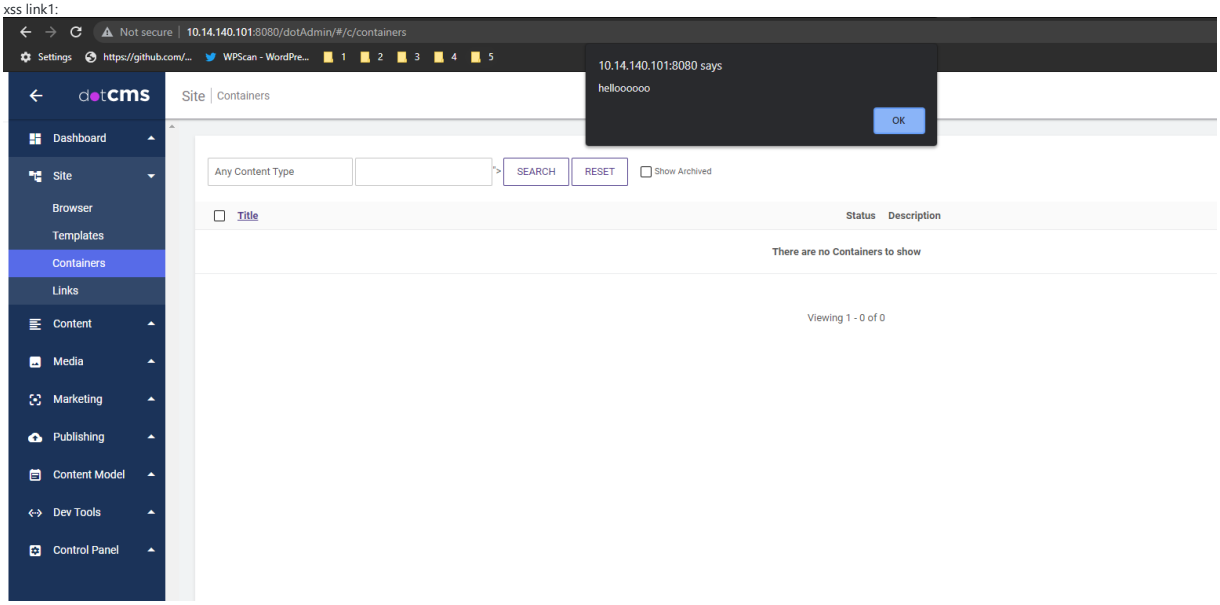
To Reproduce

1. Login Admin panel
2. vuln link1: 'dotAdmin/#/c/containers'
3. vuln link2: 'dotAdmin/#/c/links'
4. insert payload: ">
5. para: 'SEARCH'
6. Boom XSS

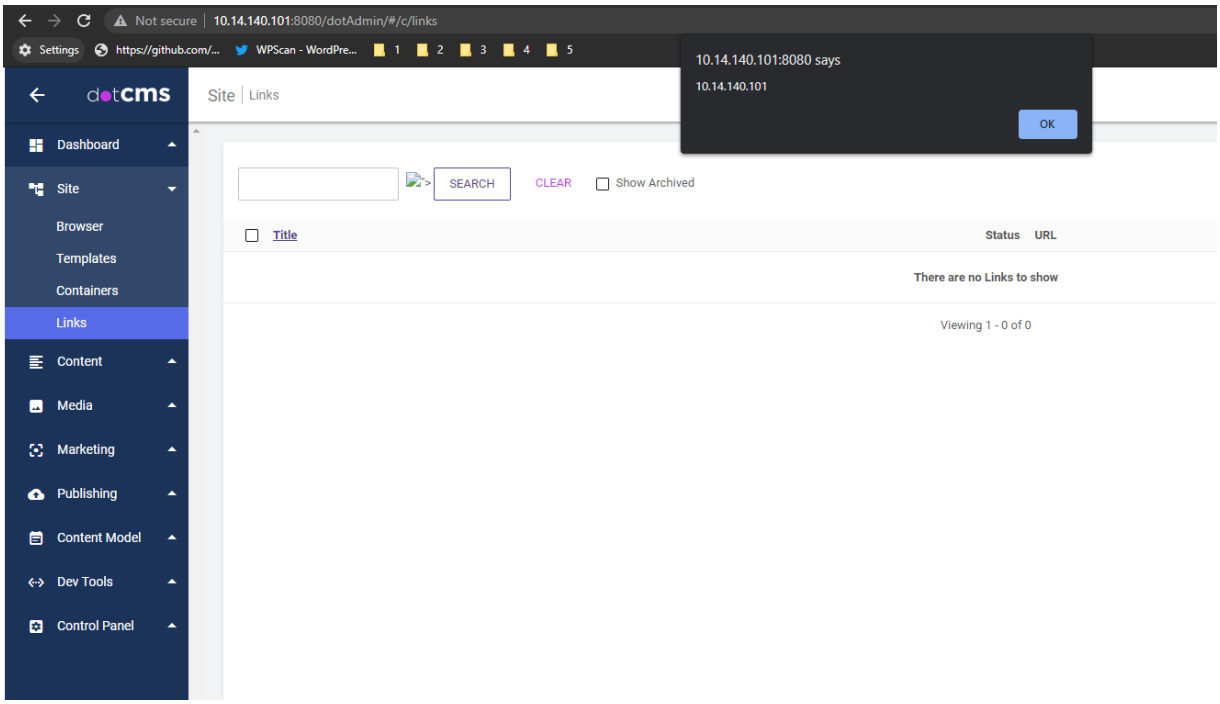
impact
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Screenshots

xss link1:



xss link2:



Desktop (please complete the following information):

- OS: Win 10
- Browser Chrome: Version 91.0.4472.77 (Official Build) (64-bit)

r0ck3t1973 added the Type : Bug label on Jun 15, 2021

wezell commented on Jun 15, 2021 — Contributor

This is a known issue with some of the older admin screens and takes administrative access to exploit. Additionally, dotCMS does not allow `http-referers` from outside of the known list of sites that it serves, which prevents XSS vulnerabilities like these from being exploitable in the wild.

https://dotcms.com/security/SI-16

wezell closed this as completed on Jun 15, 2021

r0ck3t1973 commented on Jul 10, 2021 • edited — Author

CVE-2021-35361

Assignees

No one assigned

Labels

Type : Bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants