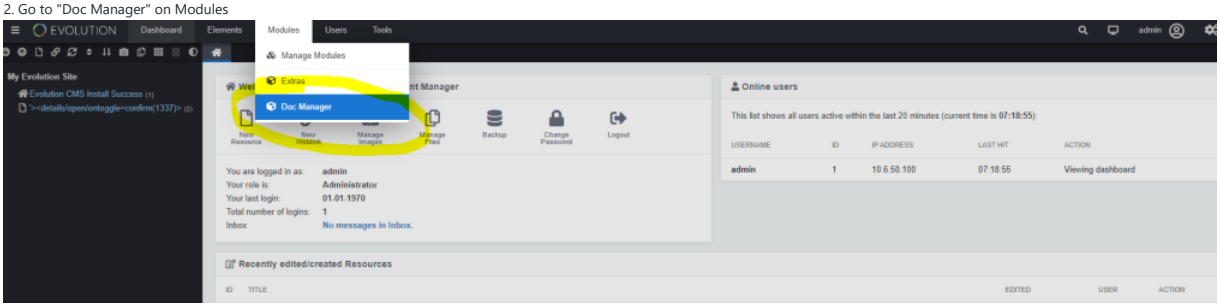
Cross Site Scripting Vulnerability on "Document Manager" feature in Evolution 2.0.2 #1473

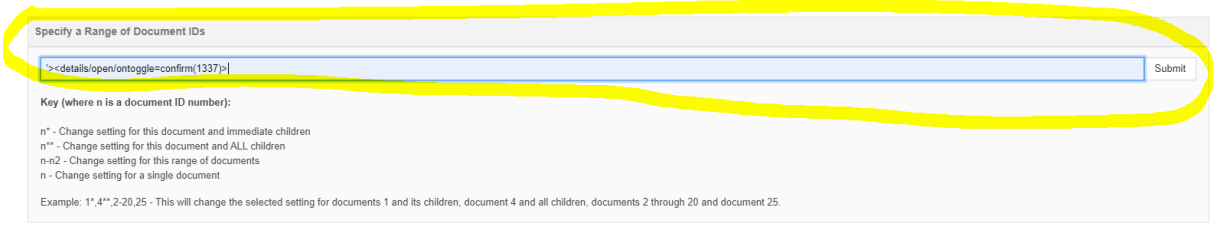
Open **luuthehienhbit** opened this issue on Jun 1, 2020 · 3 comments

luuthehienhbit commented on Jun 1, 2020

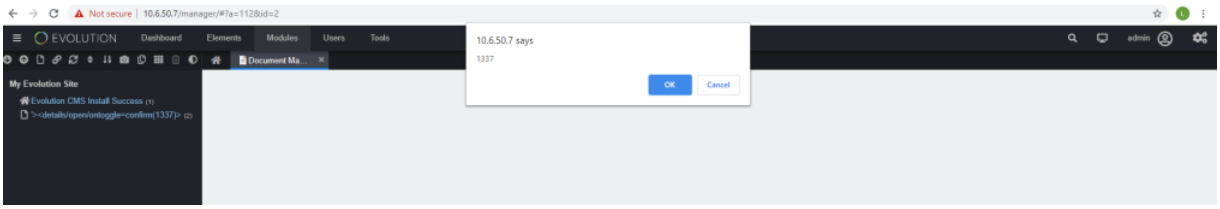
Describe the bug
An authenticated malicious user can take advantage of a Reflected XSS vulnerability in the "Document Manager" feature.
To Reproduce
Steps to reproduce the behavior:
1. Log into the /manager
2. Go to "Doc Manager" on Modules



3. Insert payload:
'><details/open/ontoggle=confirm(1337)>



4. Click "Submit"



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.
Versions
Evolution CMS 2.0.2

Dmi3yy commented on Jun 1, 2020

if you have access to manager panel you have full access and any XSS haven't sense, because you can do what you need without XSS)

luuthehienhbit commented on Jun 1, 2020 Author

Hello **@Dmi3yy**,
I think, admin is only allowed to use js / html in certain areas like edit plugin / module, theme / template, ... In other parts, if the admin is still allowed to use it arbitrarily, it will cause a risk, attack..etc, because a website will probably have 1 or more admin. An attacker with admin rights can take full advantage and lure victim with malicious intent through XSS :))

Dmi3yy commented on Jun 1, 2020

If you have any right in manager you can write in content any snippet. And get any results what you want. So XSS in manager panel haven't sense.

With many main snippet you can get info from DB or change some in DB. so you no need use XSS, becouse easy use snippet for that

Assignees
No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants