New issue

Jump to bottom

There is a stored xss vulnerability exists in DoraCMS #255

Open **afeng2016-s** opened this issue on Feb 19 · 0 comments

afeng2016-s commented on Feb 19

[Suggested description]
There is a storage XSS vulnerability in the background / admin / contenttemp module of doracms system.
The user can access index HTML and 404 HTML page number will trigger JS pop-up.

[Vulnerability Type]
Storage XSS vulnerability

[Vendor of Product]
https://github.com/doramart/DoraCMS

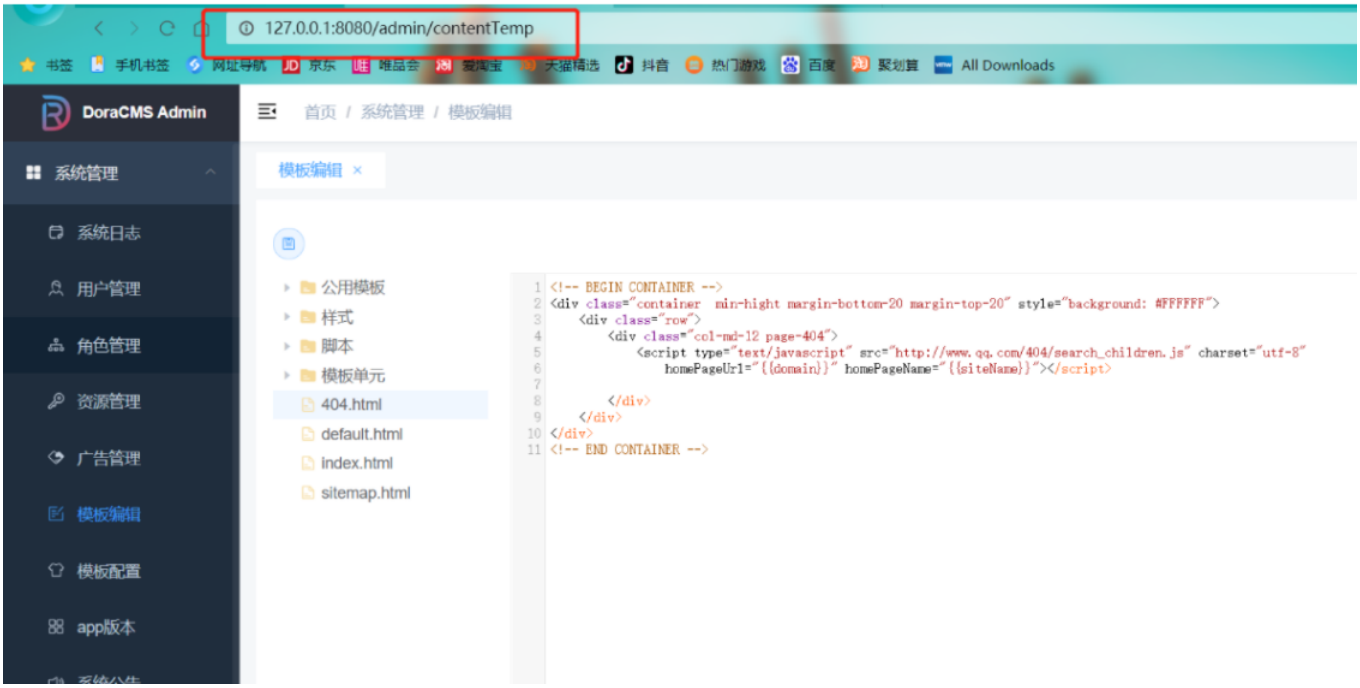
[Affected Product Code Base]
DoraCMS v2.1.8

[Attack Type]
Remote

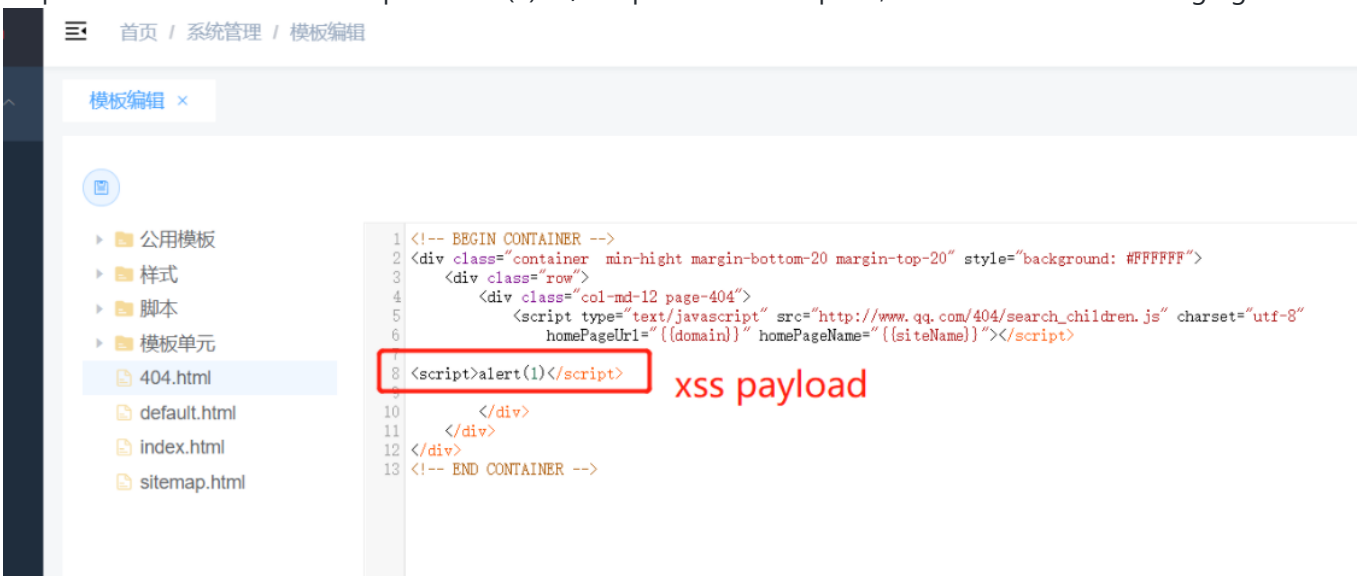
[Impact Code execution]
true

[Vulnerability proof]

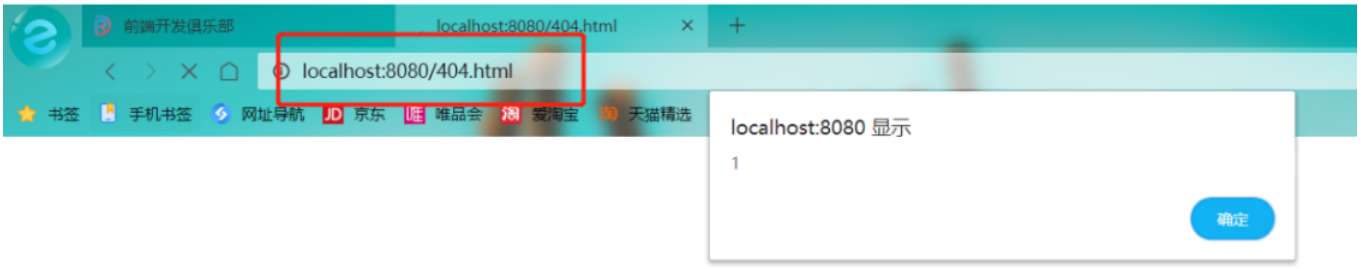
Step 1: log in to doracms and visit the admin / contenttemp page at URL: http://127.0.0.1:8080/admin/contentTemp。As can be seen from the figure below, the template is a page frequently visited by users, such as 404 html、index. html。

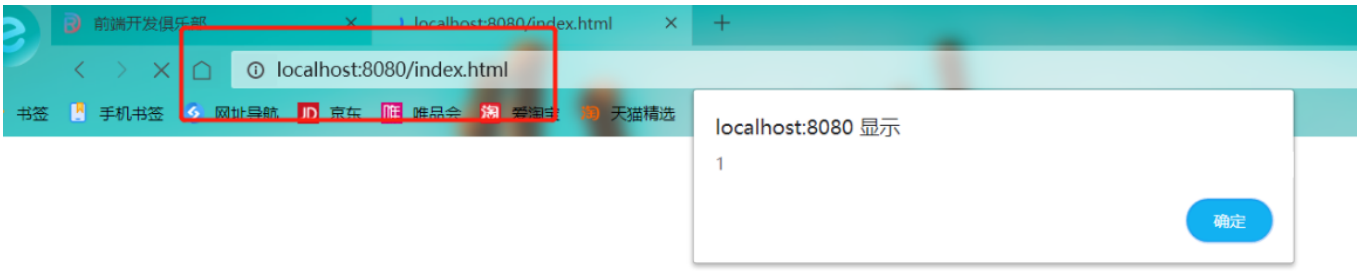


Step 2: enter the JS code < script > alert (1) < / script > in the template, as shown in the following figure.



Step 3: after saving the changes, visit 404 HTML and index HTML, trigger JS code execution pop-up window.





Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant