New issue

Jump to bottom

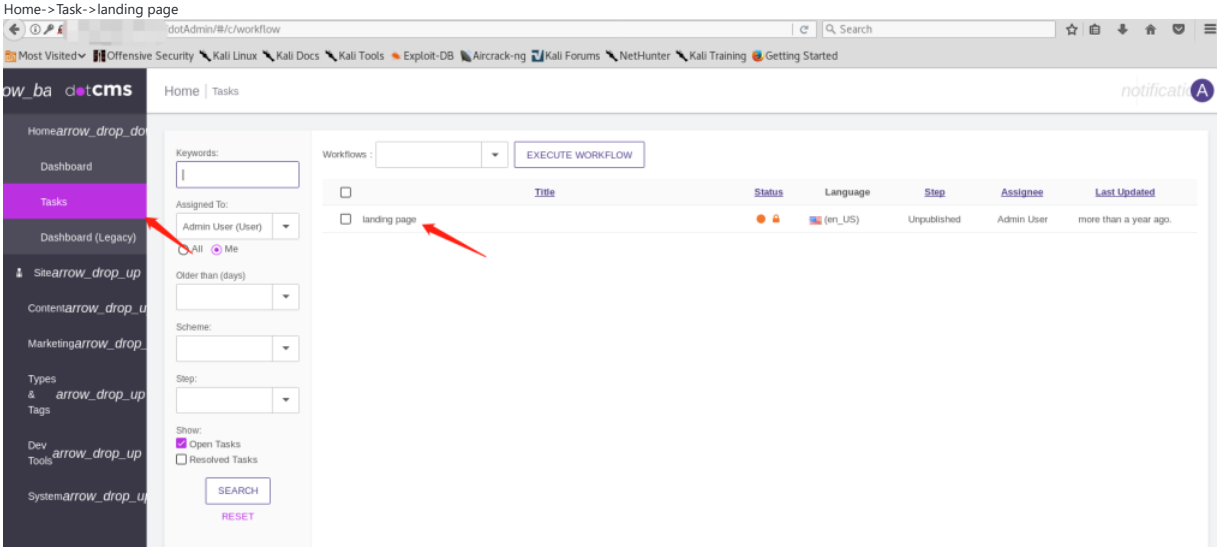
DotCMS v5.1.5 stored xss vul. #16890

Closed graySava opened this issue on Jul 18, 2019 · 1 comment

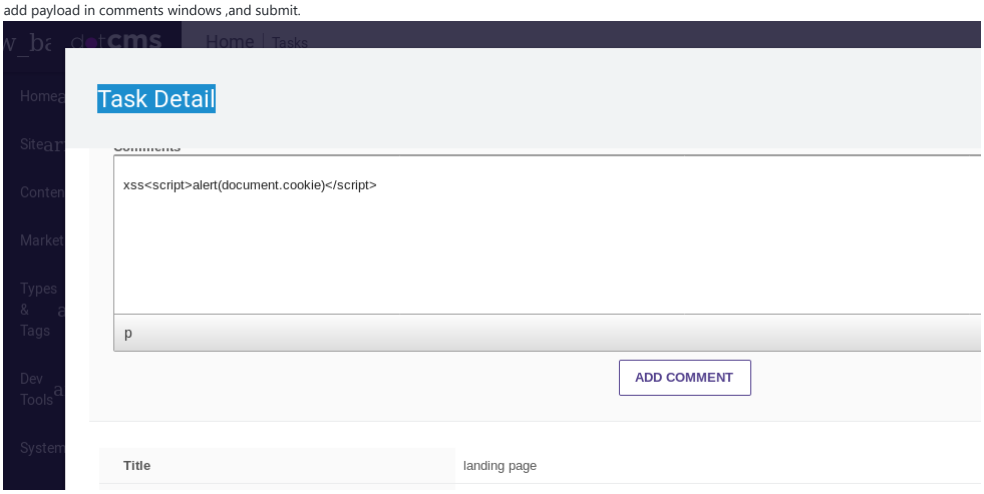
Labels Type : Bug Won't Fix

graySava commented on Jul 18, 2019 • edited

hi,
I've found a xss vul on DotCMS v5.1.5,it allows remote attackers to insert js code
and print cookie.Some screenshots below.
1.url: http://...*:8088/dotAdmin/#/c/workflow
Home->Task->landing page

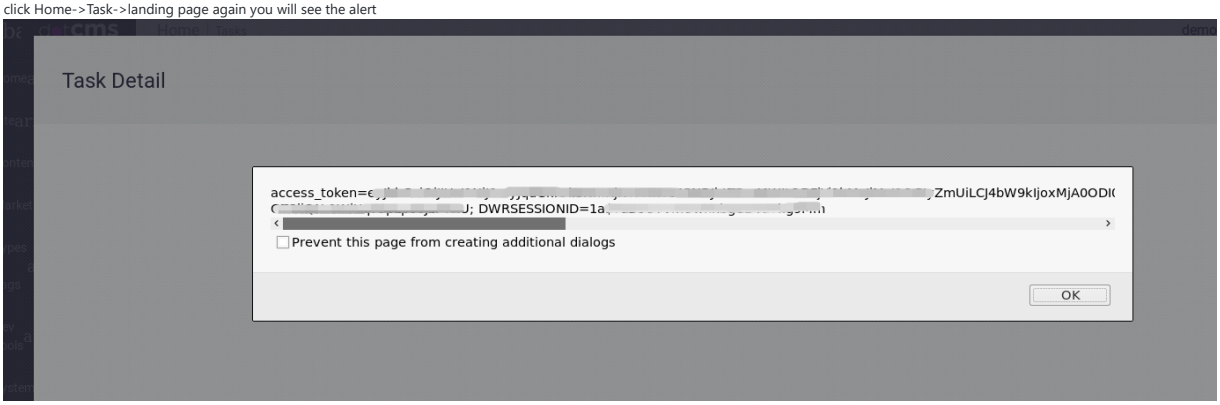


add payload in comments windows ,and submit.



use burpsuite to intercept this request

click Home->Task->landing page again you will see the alert



graySava added the Type : Bug label on Jul 18, 2019

jdotcms added a commit that referenced this issue on Aug 16, 2019

#16890 renaming the content_type_workflow_action_mapping to workflow_… ··· 782c342

jdotcms added a commit that referenced this issue on Aug 16, 2019

#16890 reformatting the oracle creates table f8e3a41

jdotcms added a commit that referenced this issue on Aug 16, 2019

#16890 removing for oracle the ; on the sql statements 96b70fa

jdotcms added a commit that referenced this issue on Aug 16, 2019

#16890 removing for oracle the ; on the sql statements 6e8ad77

jgambarios pushed a commit that referenced this issue on Aug 19, 2019

#16890 3b1632e

jgambarios pushed a commit that referenced this issue on Aug 19, 2019

#16890 renaming the content_type_workflow_action_mapping to workflow_… (··· a41cd2d

stale bot commented on Oct 22, 2019

This issue has been automatically marked as stale because it has not had activity within the past 90 days. It will be closed in 30 days no further activity occurs. Thank you.

stale bot added the Won't Fix label on Oct 22, 2019

stale bot closed this as completed on Nov 21, 2019

Assignees

No one assigned

Labels

Type : Bug Won't Fix

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant