New issue

Jump to bottom

wuzhicms v4.1.0 statcode reflected xss vulnerability #183

Open **feixuezhi** opened this issue on Aug 1, 2019 · 0 comments

feixuezhi commented on Aug 1, 2019 • edited

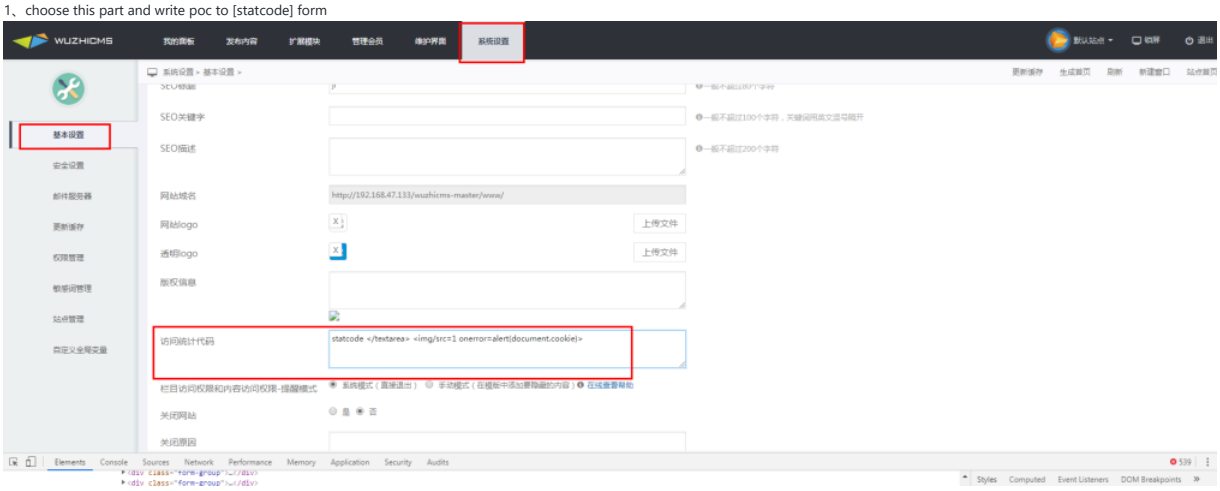
A xss vulnerability was discovered in WUZHI CMS 4.1.0

There is a reflected XSS vulnerability which allows remote attackers to inject arbitrary web script or HTML via the imgurl parameter of /index.php?m=core&f=index&_su=wuzhicms.

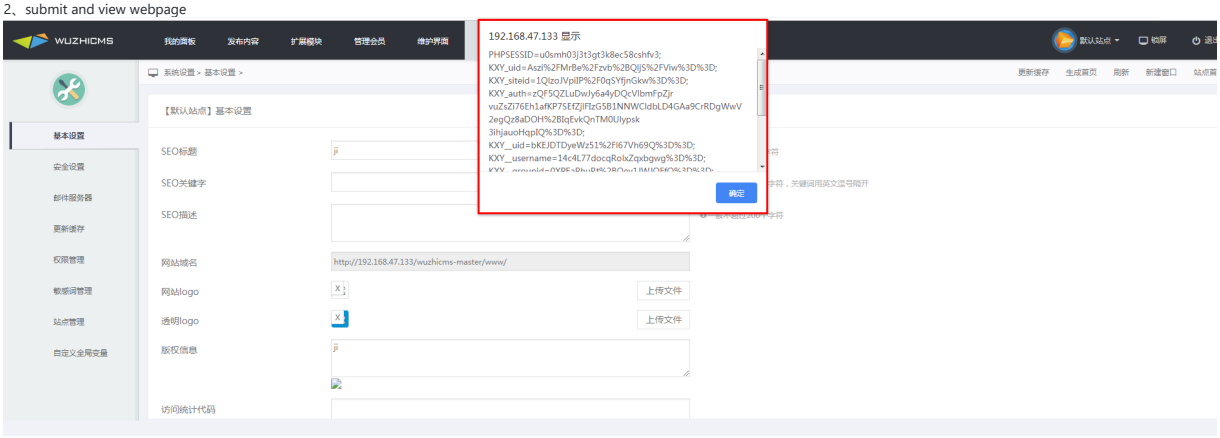
POC
ji</textarea> <img/src=1 onerror=alert(document.cookie)>

Vulnerability trigger point
http://localhost/index.php?m=core&f=index&_su=wuzhicms. When attacker access -system settings - basic settings, Write poc in the statcode form , then XSS vulnerability is triggered successfully.

1、choose this part and write poc to [statcode] form



2、submit and view webpage



Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant