



Issues / 详情

Email function has XSS vulnerability in emailbo

Done #1189ZF c0d1M4x Opened this issue 2020-01-12 22:55

Test environment

os: windows

IBOS version: 4.5.4

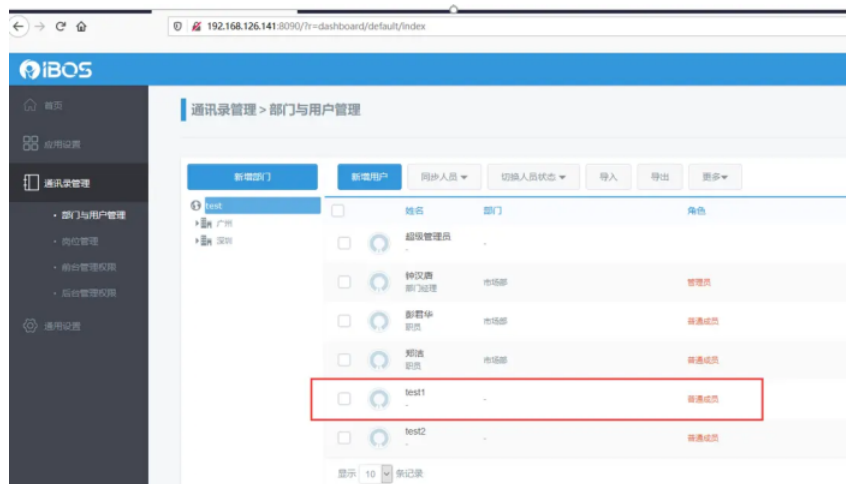
Discovery time: 2020/1/12

download IBOS time: 2020/1/9

Testing process

create new user

Create a new account test1 with normal user permissions

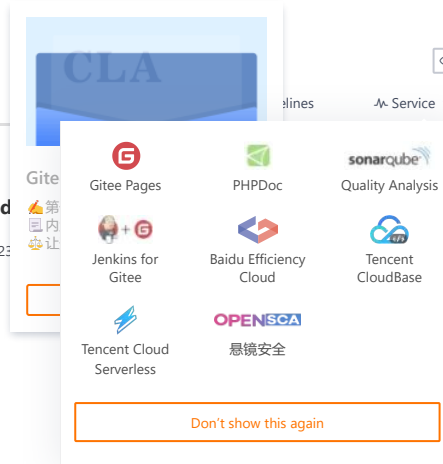


login in the test1 and enter the email.



Send email

Send email to Super Administrator



Status

Done

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull request will close this issue.

Branches

No related branch

Planned to start - Planned to end

Unscheduled - Unscheduled

Top level

Not Top

Priority

Not specified

参与者 (1)







Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

[View Details](#)

Solution

filter or encode special characters like this

```
<
>
"
'
&
%
... ..
```

and filter some keyword like this

```
script
javascript
... ..
```

or filter some label function which can run javascript like this

```
onclick
onerror
onload
... ..
```

👤 c0d1M4x created 任务 3 years ago

[Expand operation logs](#) ▾

[Sign in to comment](#)



©OSCHINA. All rights reserved

[Git Resources](#)
[Learning Git](#)
[CopyCat](#)
[Downloads](#)

[Gitee Reward](#)
[Gitee Stars](#)
[Featured Projects](#)
[Blog](#)
[Nonprofit](#)
[Gitee Go](#)

[OpenAPI](#)
[Help Center](#)
[Self-services](#)
[Updates](#)

[About Us](#)
[Join us](#)
[Terms of use](#)
[Feedback](#)
[Partners](#)

📞 777320883
✉ git@oschina.cn
📌 Gitee
☎ +86 400-606-0201



Mini Program



WeChat

