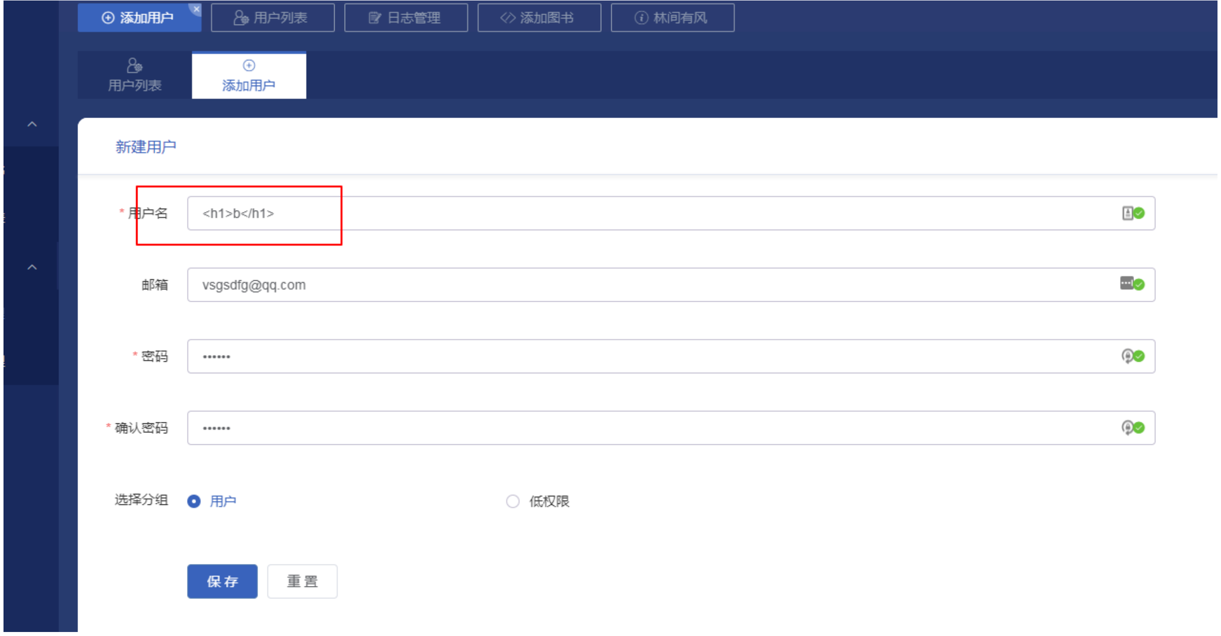
Cross Site Scripting Vulnerability in Latest Release #28

Open HatBoy opened this issue on Mar 14, 2019 · 2 comments

HatBoy commented on Mar 14, 2019

Hi, I would like to report Cross Site Scripting vulnerability in latest release.

Description:
Cross-site scripting (XSS) vulnerability in app/api/cms/user.py 12 line register() function and app/api/cms/log.py 23 line get_logs() function.
User name usage XSS payload will be executed in the log when registering users
Steps To Reproduce:
1.Add a user, the username is xss payload.



新建用户

* 用户名 <h1>b</h1>

邮箱 vsgsdfg@qq.com

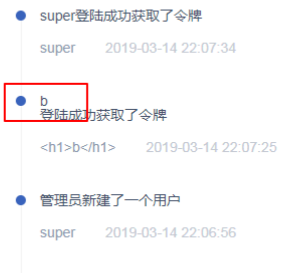
* 密码 ••••••

* 确认密码 ••••••

选择分组 ● 用户 ○ 低权限

保 存 重 置

2.Then use the username login, see the log manager find the xss payload already executed, the super user also can find.



super登陆成功获取了令牌
super 2019-03-14 22:07:34

b
登陆成功获取了令牌
<h1>b</h1> 2019-03-14 22:07:25

管理员新建了一个用户
super 2019-03-14 22:06:56

author by jin.dong@dbappsecurity.com.cn

7insummer commented on Mar 14, 2019

Thanks for these suggestions, as we have just started, including SQL injection and CSRF prevention has been put on the agenda but has not yet been achieved. We will improve these security issues in the near future. Thanks again.

OS-WS commented on Aug 17, 2021

Hi @7insummer @HatBoy ,
Was this issue fixed?
if so, in what commit and what tag/version?
thanks!

Assignees
No one assigned

Labels
None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants