

[New issue](#)

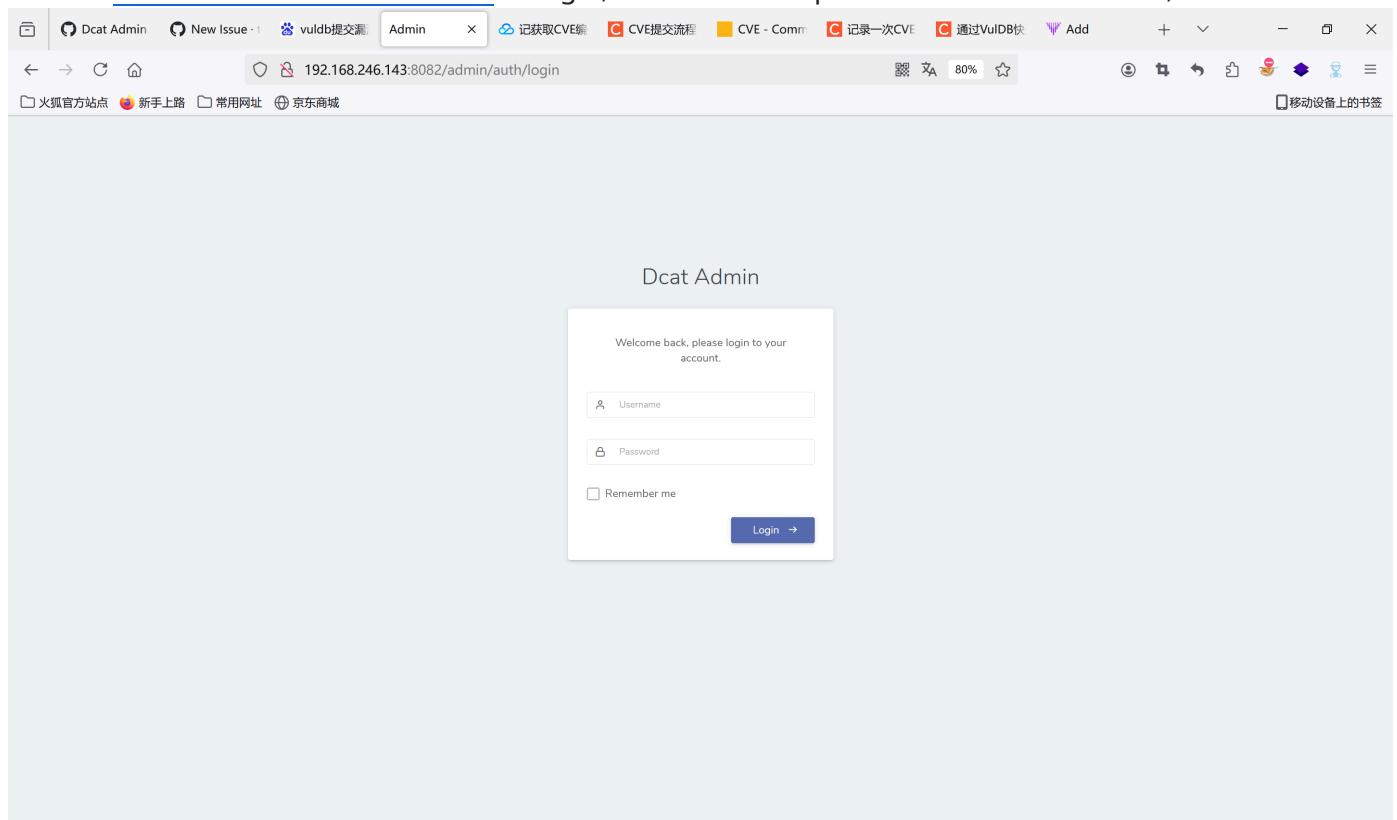
Dcat Admin v2.2.1-beta There is a stored XSS cross-site scripting vulnerability exists /admin/auth/roles #7

[Open](#)

taynes-lllzt opened last week

...

Build the source code locally by downloading
And I deploy the source code in the local environment, set the domain name to
192.168.246.143:8082/admin, equivalent to localhost/admin
The vulnerability exists: 192.168.246.143:8082/admin/auth/roles
Visit url:192.168.246.143:8082/admin to login, username and password default to admin,admin



After entering the background, click admin,roles,new

Fill in payload <script>alert("2")</script> in slug module; fill in 111 in name, and click Submit, and then pop-ups pop up.

Dcat Admin

Roles List

New

Slug: <script>alert('2')</script>

Name: 111

Permissions: Select all Expand

Auth management

- Users
- Roles
- Permissions
- Menu
- Extension

Menu: Select all Expand

- Index
- Admin
 - Users
 - Roles
 - Permission
 - Menu
 - Extensions

Submit Reset

Save succeeded!

Administrator Online

192.168.246.143:8082

2

确定

Then I found that every time I click role, this module will appear pop-up window, indicating that it is a

stored xss cross-site scripting vulnerability.

The screenshot shows a web application interface for managing users and roles. On the left, there is a sidebar with navigation links: Index, Admin (selected), Users, Roles (highlighted in blue), Permission, Menu, Extensions, and Helpers. The main content area displays a table titled "Administrator List" with one entry:

ID	Username	Name	Roles	Permissions	Created At	Updated At	Action
1	admin	Administrator	Administrator	View	2024-12-28 04:39:36	2024-12-28 04:39:36	<button>⋮</button>

Below the table, a message says "Showing 1 to 1 of 1 entries". A modal dialog is open in the center, displaying the IP address "192.168.246.143:8082" and the number "2". A blue button labeled "确定" (Confirm) is visible at the bottom right of the modal.

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

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants

