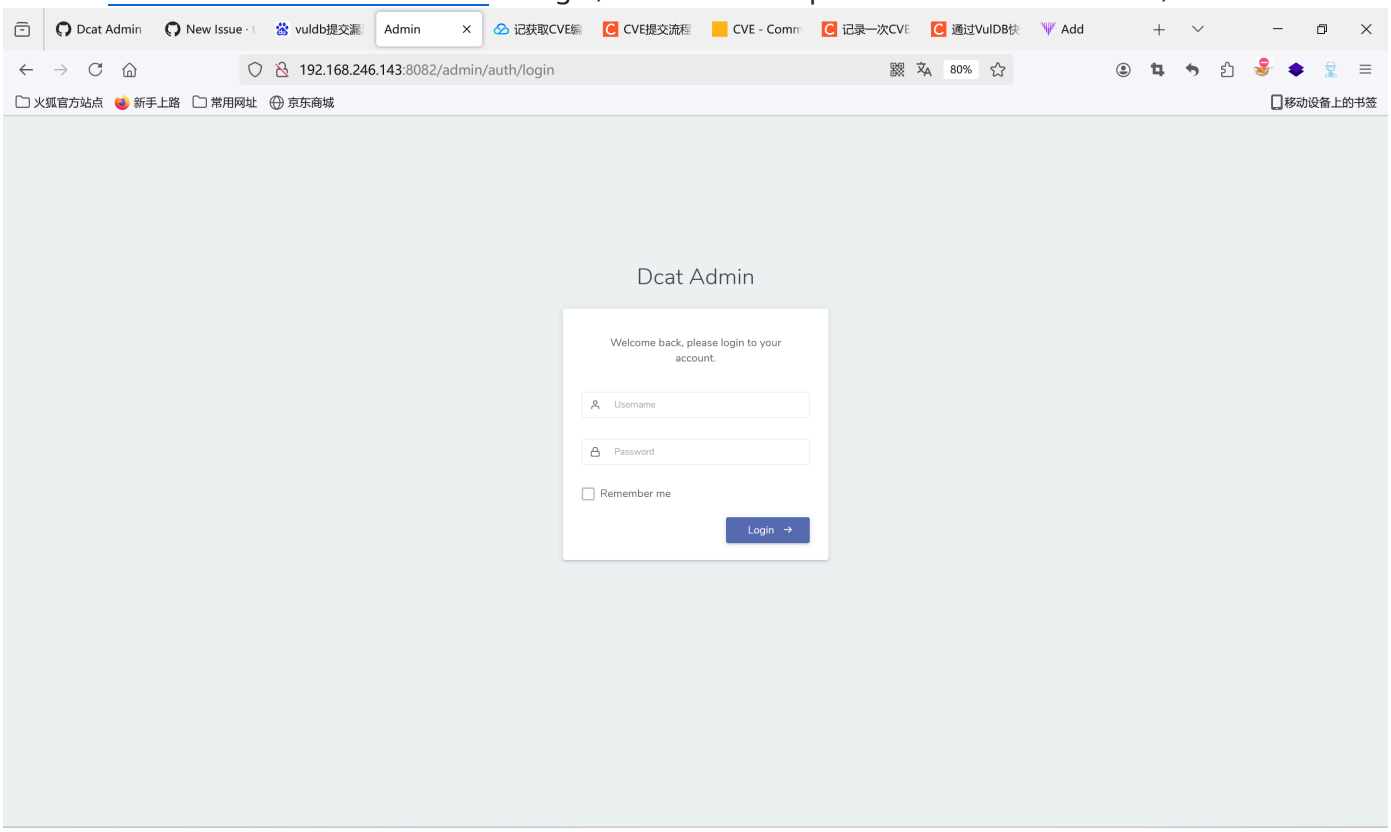
New issue

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

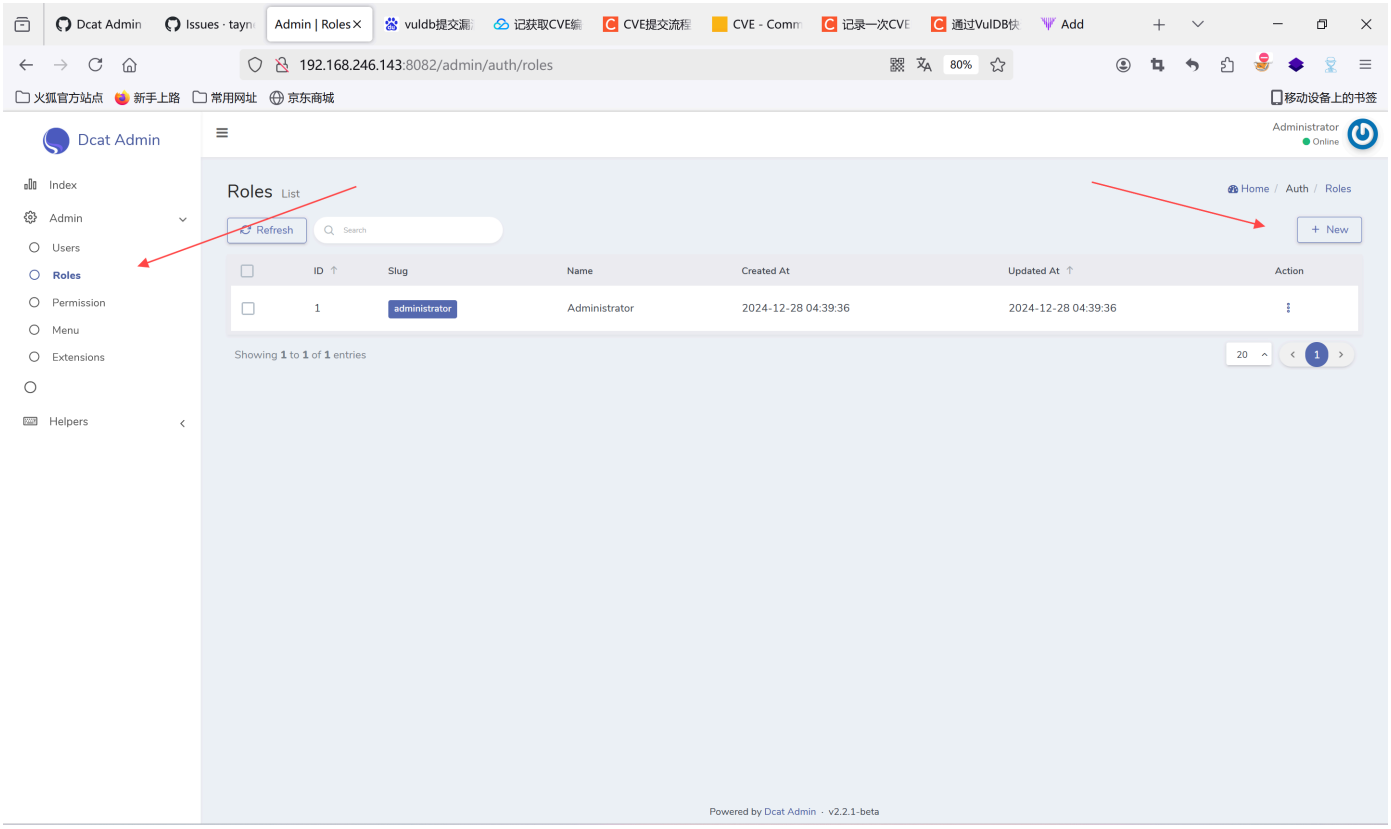
Open

taynes-llllzt opened last week

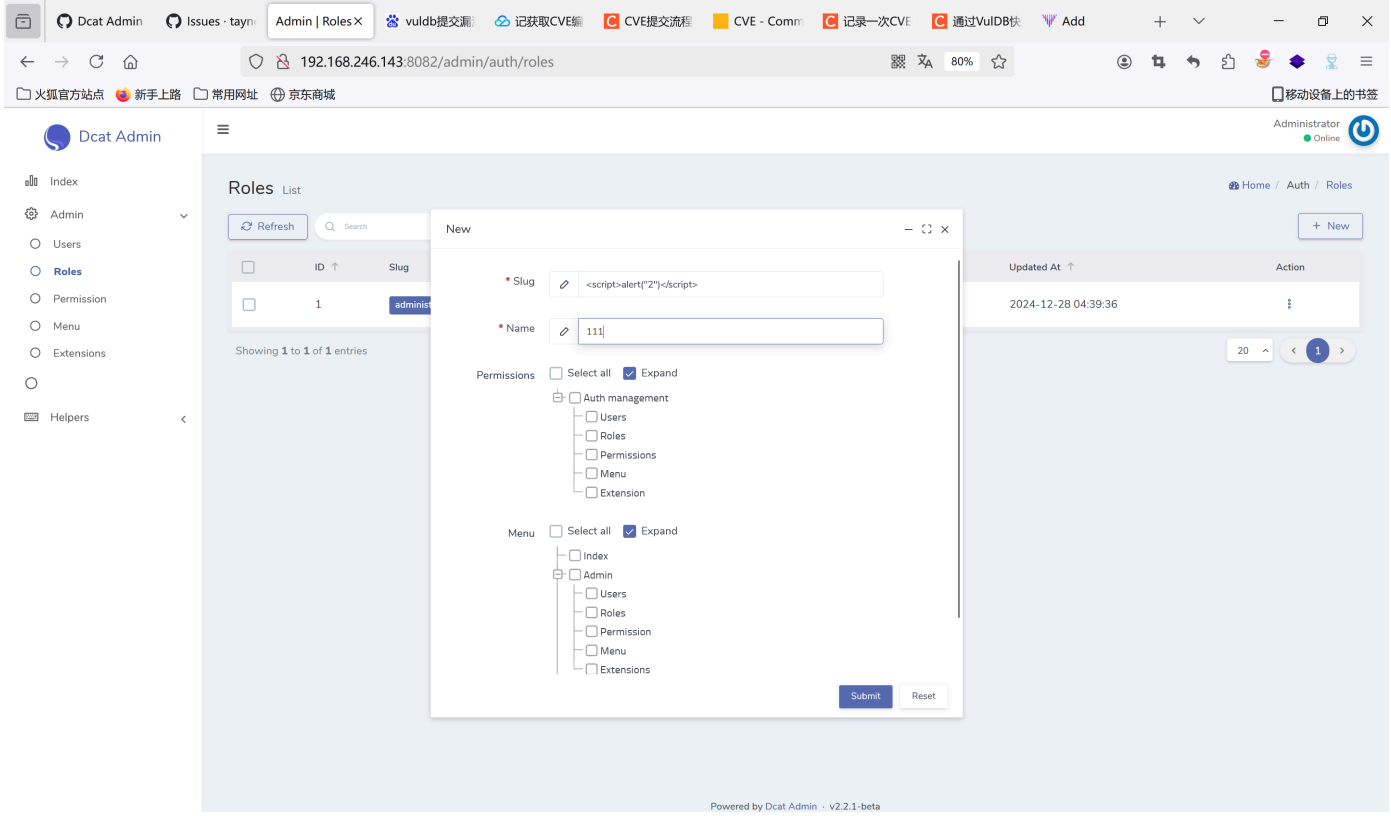
Build the source code locally by downloading
And I deploy the source code in the local environment, set the domain name to 192.168.246.143:8082/admin, equivalent to localhost/admin
The vulnerability exists: 192.168.246.143:8082/admin/auth/roles
Visit url:192.168.246.143:8082/admin to login, username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

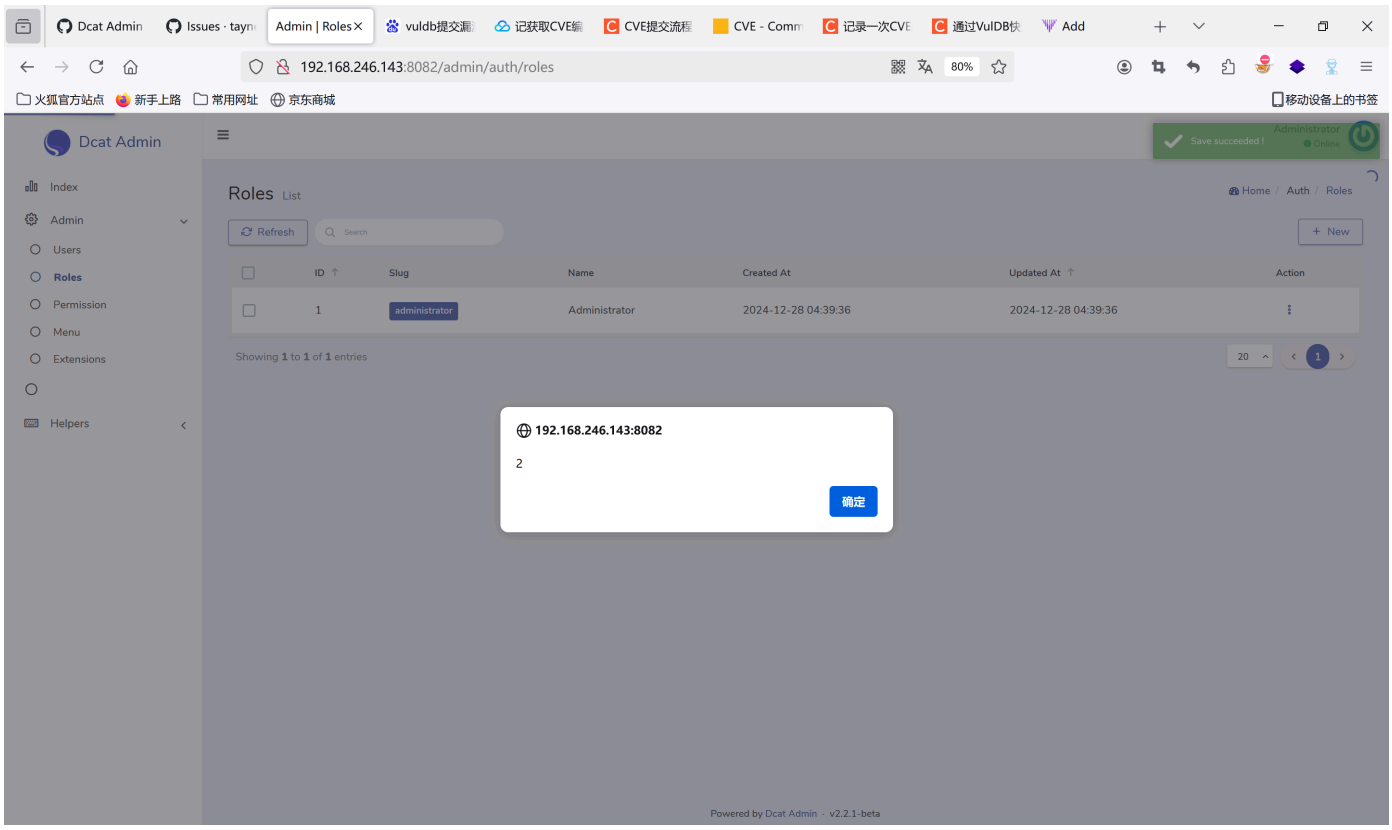


After entering the background, click admin,roles,new



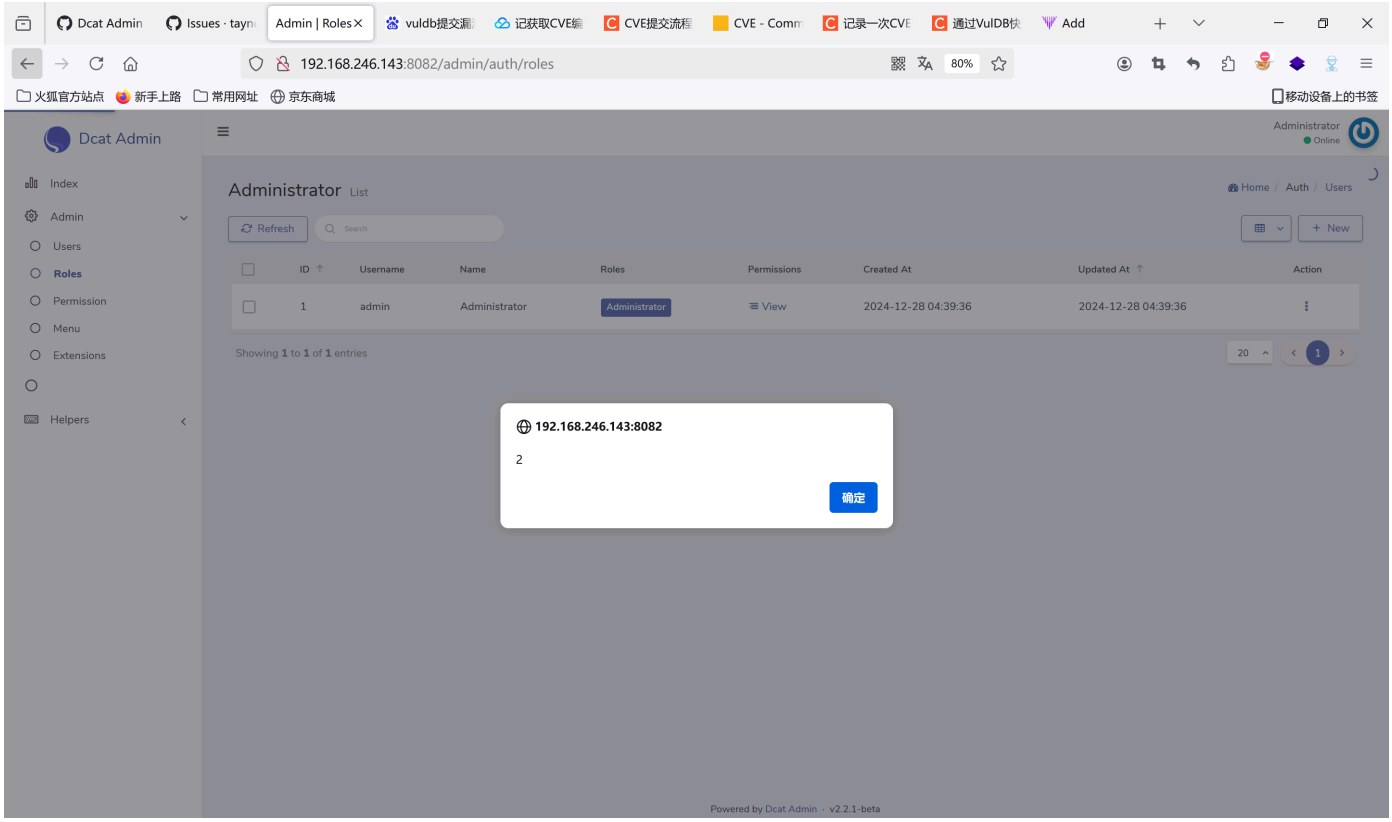
Fill in payload `<script>alert("2")</script>` in slug module; fill in 111 in name, and click Submit, and then pop-ups pop up.





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.



Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants