New issue

Jump to bottom

Bind email address in user's function lead to XSS #18

⊙ Open **H4niz** opened this issue on Aug 21, 2021 · 0 comments

H4niz commented on Aug 21, 2021

I and **@KietNA-HPT** found a XSS vulnerability on a user function called `bind_email()` when we audit your source code. The vulnerability occurs when we input new email with injecting some trick to trigger XSS in `title` param like:

```
index.php?m=user&c=Users&a=bind_email&title=123%27;+window.open("www.google.com.vn");//
```

To trigger this bug, we did following below:

1. Access url: http://example-host.com/index.php?m=user&c=Users&a=bind_email&title=triggerxss%27;+window.open("www.google.com.vn");//
2. Enter a valid email
3. Click to `Send` (点击发送 in your language) button. And then the XSS is triggered.

Solution: To fix this vulnerability, please validate input from user into `title` param

H4niz changed the title ~~Change email address in user's function lead to XSS~~ **Bind email address in user's function lead to XSS** on Aug 21, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant