New issue Jump to bottom

ecshop 3.0 /admin/shophelp.php id SQLinject #8

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

```
Owner
blindkey commented on Feb 18, 2020
ecshop 3.0 /admin/shophelp.php
        integrate.php license.php
       icense.php
magazine_list.php
mall_template.php
mobile_navigator.php
mobile_ad.php
mobile_schpp
mobile_icense.php
mobile_navigator.php
mobile_navigator.php
                                                     147
148
149
                                                                      assign_query_info();
$smarty->display('shophelp_info.htm');
                                                    153 { 154
                                                                    ($_REQUEST['act'] == 'update')
       navigator.php
order.php
order_stats.php
                                                                      admin_priv('shophelp_manage');
        pack.php
package.php
patch_num
                                                                           ($_POST['title'] != $_POST['old_title'] )
        payment.php
picture_batch.php
privilege.php
receive.php
                                                                              $exc_article->is_only('title', $_POST['title'], $_LANG['articlename_exist'], $_
                                                                                      POST['id']);
       reg_fields.php
role.php
sale_general.php
sale_list.php
                                                                           ($exc_article->edit("title = '$_POST[title]', cat_id = '$_POST[cat_id]',
article_type = '$_POST[article_type]', content = '$_POST[FCKeditor1]'", $_POST['
id']))
        sale_order.php
        send.php
        shipping.php
shipping.area.php
shop_config.php
                                                                              clear_cache_files();
                                                                              $\link[0]['text'] = $\_LANG['back_list'];
$\link[0]['href'] = 'shophelp.php?act=list_article&cat_id='.$_POST['cat_id'];

☐ shophelp.php

       shopinfo.php
sitemap.php
sms.php
sms.php
sms_url.php
                                                                              sys_msg(sprintf($_LANG['articleedit_succeed'], $_POST['title']), 0, $link);
admin_log($_POST['title'], 'edit', 'shophelp');
        snatch.php
        suppliers.php suppliers_goods.php
       tag_manage.php
template.php
topic.php
                                                                                                                                                                                                                       間 英 、 ) ☆
        user_account.php
at line 160,$id was passe to execute without filter and leads to sql inject
```

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone
Development
No branches or pull requests

1 participant

