

[New issue](#)[Jump to bottom](#)

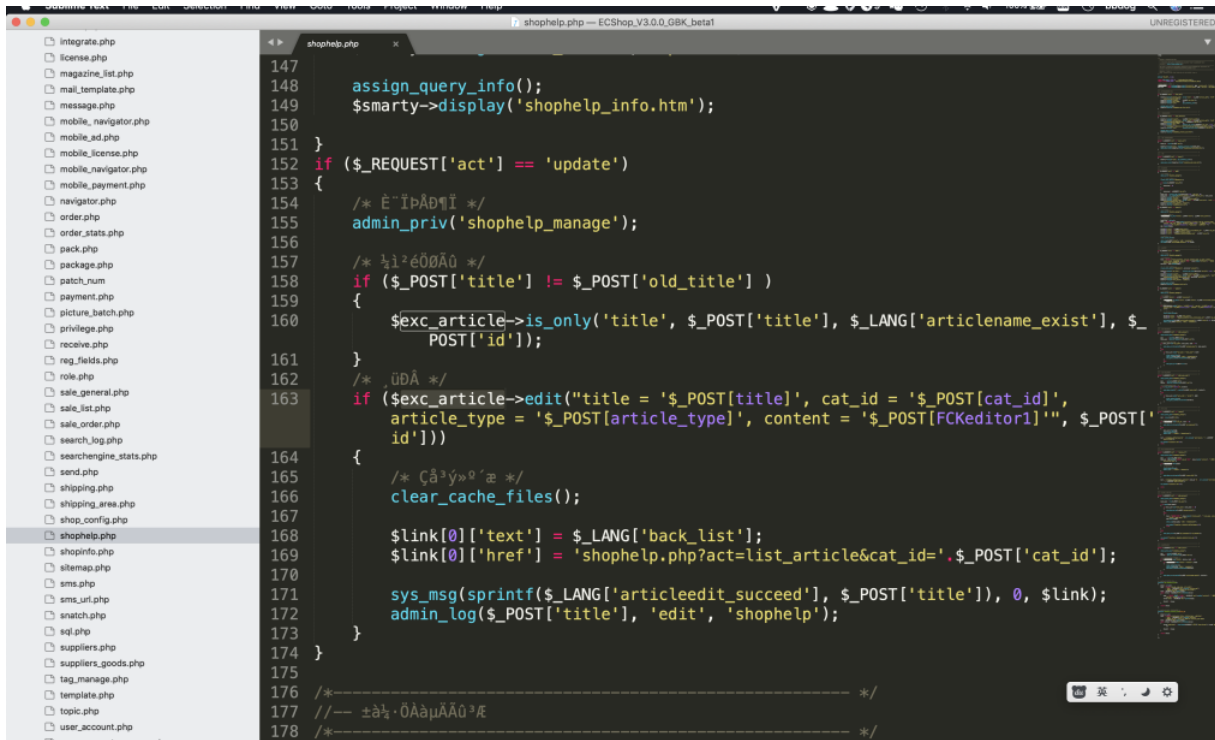
## ecshop 3.0 /admin/shophelp.php id SQLinject #8

[Open](#) blindkey opened this issue on Feb 18, 2020 · 0 comments

blindkey commented on Feb 18, 2020

[Owner](#)

ecshop 3.0 /admin/shophelp.php



```
147
148 assign_query_info();
149 $smarty->display('shophelp_info.htm');
150
151 }
152 if ($REQUEST['act'] == 'update')
153 {
154     /* 验证权限 */
155     admin_priv('shophelp_manage');
156
157     /* 验证标题 */
158     if ($POST['title'] != $POST['old_title'] )
159     {
160         $exc_article->is_only('title', $POST['title'], $LANG['articlename_exist'], $POST['id']);
161     }
162     /* 更新 */
163     if ($exc_article->edit("title = '$POST[title]', cat_id = '$POST[cat_id]',
164         article_type = '$POST[article_type]', content = '$POST[FCKeditor1'", $POST['id']))
165     {
166         /* 清除缓存 */
167         clear_cache_files();
168
169         $link[0]['text'] = $LANG['back_list'];
170         $link[0]['href'] = 'shophelp.php?act=list_article&cat_id='.$POST['cat_id'];
171
172         sys_msg(sprintf($LANG['articleedit_succeed'], $POST['title']), 0, $link);
173         admin_log($POST['title'], 'edit', 'shophelp');
174     }
175 }
176 /*-----*/
177 /*----- 标题修改成功 -----*/
178 /*-----*/
```

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

