

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

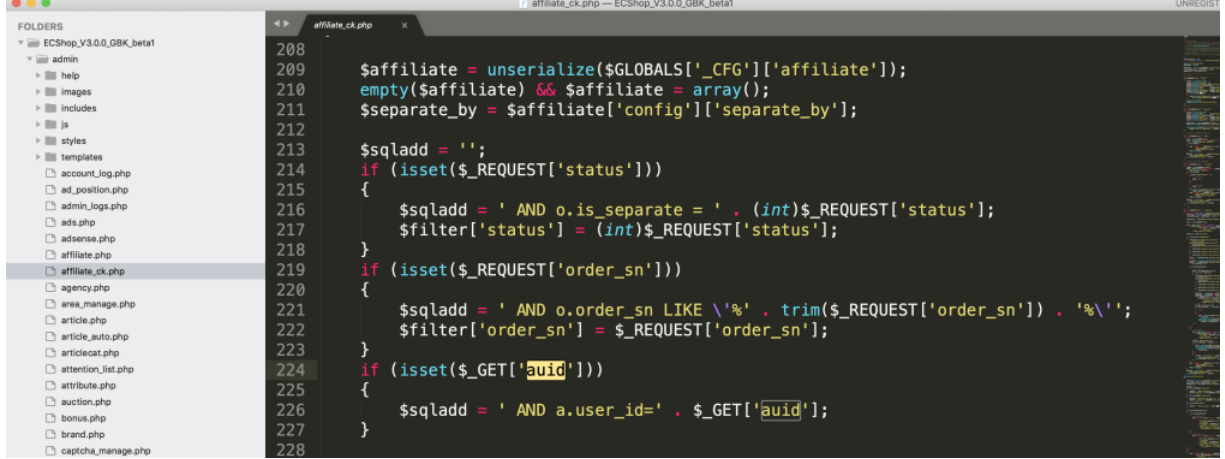
ecshop3.0 /admin/affiliate_ck.php aid SQL inject #9

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

blindkey commented on Feb 18, 2020

Owner

/admin/affiliate_ck.php



```
208
209 $affiliate = unserialize($GLOBALS['_CFG']['affiliate']);
210 empty($affiliate) && $affiliate = array();
211 $separate_by = $affiliate['config']['separate_by'];
212
213 $sqladd = '';
214 if (isset($_REQUEST['status']))
215 {
216     $sqladd = ' AND o.is_separate = ' . (int)$_REQUEST['status'];
217     $filter['status'] = (int)$_REQUEST['status'];
218 }
219 if (isset($_REQUEST['order_sn']))
220 {
221     $sqladd = ' AND o.order_sn LIKE \'' . trim($_REQUEST['order_sn']) . '%\'';
222     $filter['order_sn'] = $_REQUEST['order_sn'];
223 }
224 if (isset($_GET['aid']))
225 {
226     $sqladd = ' AND a.user_id=' . $_GET['aid'];
227 }
228
```

aid parameters pass to sqladd without filter 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

