```
☐ jsjbcyber / bug_report (Public)
<> Code
           Issues
                       ! Pull requests
                                         Actions
                                                      Security
                                                                                 ✓ Insights
  ٢º main ◄
bug_report / bug_o
     jsjbcyber Update bug_o
                                                                                     (1) History
  ৪ 1 contributor
  70 lines (69 sloc) | 3.28 KB
        Build environment with PHP5.
    1
    2
    3
        affected source code file: /admin/news/sort_add.php and /inc/function.php
```

```
4
5
    affected source code:
6
      /admin/news/sort_mod.php:
7
           <?php
8
             . . . . .
9
             栏目名称: <
10
              <div style=</pre>
11
                  <input type="hidden" value="" name="title_color" id="title_color" />
12
                  <input type="hidden" value="" name="title_bold" id="title_bold" />
13
                  <input type="hidden" value="" name="title_em" id="title_em" />
14
                  <input type="hidden" value="" name="title_u" id="title_u" />
15
                  <input name="name" type="text" id="name" size="50" value="" />
16
                </div>
17
                <div class="color">
18
19
                  <?php include '../../inc/choose_color.php'; ?>
                </div>
20
21
            22
23
           ?>
24
     /inc/function.php:
25
     <?php
26
     . . . . . .
        function getCategoryList($id = 0, $level = 0) {
27
28
         global $db;
         $category_arr = $db->getList (get_sql( "SELECT * FROM {pre}class WHERE fid = " . $id . " ord
29
```

```
30
        for($lev = 0; $lev < $level * 2 - 1; $lev ++) {
31
          $level_nbsp .= "  ";
32
        }
        $level++;
33
        $level nbsp .= "\right";
34
35
        foreach ( $category arr as $category ) {
36
          $id = $category ['id'];
37
         $fid = $category ['fid'];
38
          $name = $category ['name'];
39
         $son = $category ['son'];
40
         $sons = $category ['sons'];
41
         $count = $category['count'];
42
         $depth = $category['depth'];
43
         $rank = $category['rank'];
          echo "
44
       45
46
        " . $id . " 
47
        " . $level nbsp . " <a href='sort mod.php?act=mod&id=" . $id . "&fid=" .
        " . $son . " 
48
49
        " . $count . " 
50
        " . $depth . " 
        " . $fid . " 
51
52
        " . $rank . " 
53
        54
          <a href='sort add.php?act=add&fid=" . $id . "'>添加子栏目</a> |
55
          <a href='news_add.php?act=add&cid=" . $id . "'>添加文章</a> |
56
          <a href='sort_mod.php?act=mod&id=" . $id . "&fid=" . $fid . "'>修改</a> |
57
          <a href='sort_ok.php?id=" . $id . "&act=del' onClick=\"javascript:return confirm('确实要删队
        ";
58
59
          getCategoryList ( $id, $level );
60
        }
61
       }
62
       . . . . . .
63
64
    affected executable:
65
66
     After Signing in to the background in advance. Then we can visit the following URL:
67
     http://xx.xx.com/admin/news/sort_mod.php?act=mod&id=2&fid=0
68
69
     And we edit the "栏目名称" with "<script>alert(/xss/)</script>"
70
     Then we can see a pop-up window with an XSS prompt.
```