New issue

Jump to bottom

file inclusion vulnerability #36

Closed **cilan2** opened this issue on Aug 23, 2019 · 0 comments

cilan2 commented on Aug 23, 2019

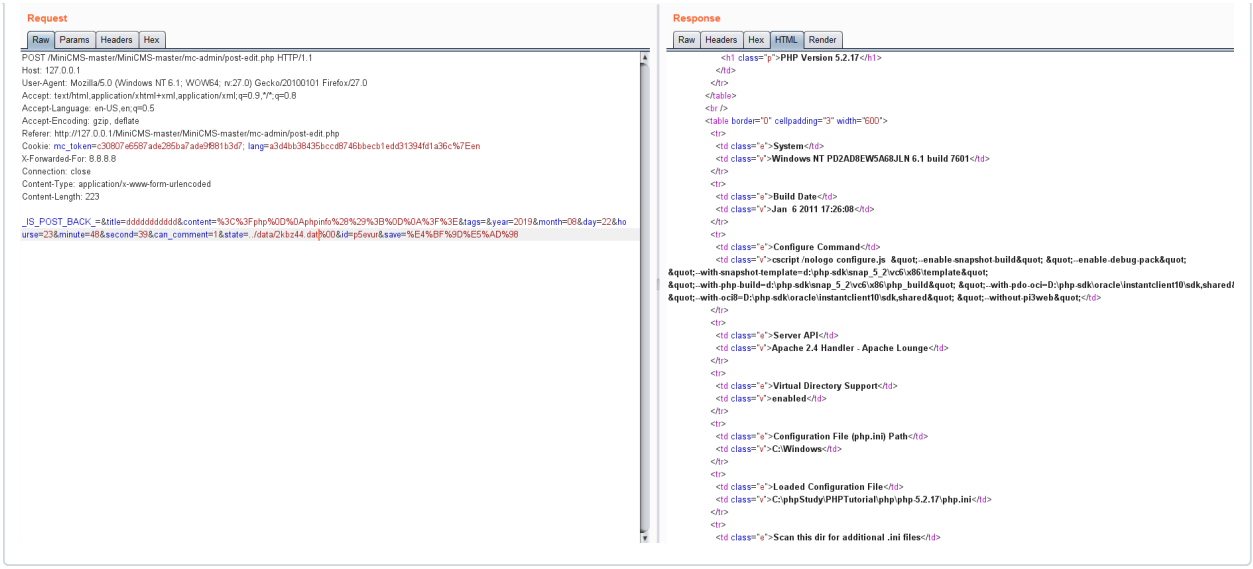
Require:
PHP Version <5.3.4
magic_quotes_gpc=off
1.
require $index_file
$index_file = '../mc-files/posts/index/'.$post_old_state.'.php'
$post_old_state = $data['state']

```
  }
  else {
    if ($post_id == '') {
      $file_names = shorturl($post_title);

      foreach ($file_names as $file_name) {
        $file_path = '../mc-files/posts/data/'.$file_name.'.dat';

        if (!is_file($file_path)) {
          $post_id = $file_name;
          break;
        }
      }
    }
    else {
      $file_path = '../mc-files/posts/data/'.$post_id.'.dat';

      $data = unserialize(file_get_contents($file_path));

      $post_old_state = $data['state'];

      if ($post_old_state != $post_state) {
        $index_file = '../mc-files/posts/index/'.$post_old_state.'.php';

        require $index_file;

        unset($mc_posts[$post_id]);

        file_put_contents($index_file,
          "<?php\n\$mc_posts=".var_export($mc_posts, true).";\n?>"
        );
      }
    }

    $data = array(
      'id'          => $post_id,
      'state'       => $post_state,
      'title'       => $post_title,
      'tags'        => $post_tags,
      'date'        => $post_date,
      'time'        => $post_time,
      'can_comment'  => $post_can_comment,
    );

    $index_file = '../mc-files/posts/index/'.$post_state.'.php';

    require $index_file;

    $mc_posts[$post_id] = $data;

    uasort($mc_posts, "post_sort");

    file_put_contents($index_file,
      "<?php\n\$mc_posts=".var_export($mc_posts, true).";\n?>"
```

2.
write a page or article with content

3.
can see url is
127.0.0.1/MiniCMS-master/MiniCMS-master/mc-admin/post-edit.php?id=2kbz44

so filename is 2kbz44.bat
4.use burppsuite,we can find phpinfo in response



bg5sbk closed this as completed in `f8fc729` on Jul 19, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant