New issue

Jump to bottom

Bug:V1.3.7 Cross Site Scripting Vulnerability #4

Open **Richard1266** opened this issue on Apr 8, 2019 · 0 comments

Richard1266 commented on Apr 8, 2019

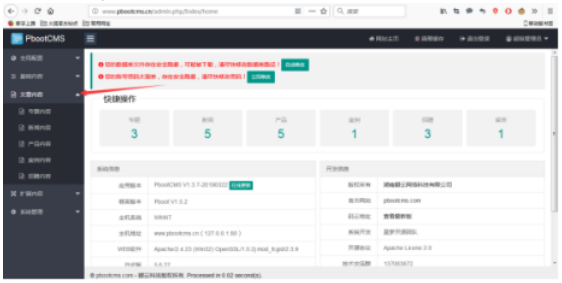
There is an Stored Cross Site Scripting vulnerability in your latest version of the CMS v1.3.7
Download link: "https://codeload.github.com/hnaoyun/PbootCMS/zip/V1.3.7"
In the Pbootcmsv1.3.7\apps\admin\controller\content\SingleController.php, No filtering to title in the mod( ) function:

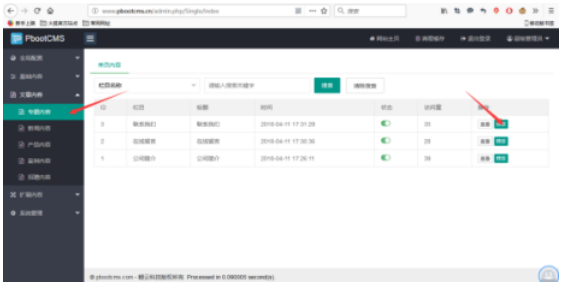
```
if ($_POST) {

    // 获取数据
    $title = post('title');
    $author = post('author');
    $source = post('source');
    $ico = post('ico');
    $pics = post('pics');
    $content = post('content');
    $tags = str_replace('，', ',', post('tags'));
    $titlecolor = post('titlecolor');
    $subtitle = post('subtitle');
    $outlink = post('outlink');
    $date = post('date');
    $enclosure = post('enclosure');
    $keywords = post('keywords');
    $description = post('description');
    $status = post('status', 'int');

    if (! $title) {
        alert_back('单页内容标题不能为空！');
    }

    // 自动提起前一百个字符为描述
    if (! $description && isset($_POST['content'])) {
        $description = escape_string(clear_html_blank(substr_both(strip_tags($_POST['content']), 0, 150)));
    }

    // 缩放缩略图
    if ($ico) {
        resize_img(ROOT_PATH . $ico, '', $this->config('ico.max_width'), $this->config('ico.max_height'));
    }
```

```
    // 执行添加
    if ($this->model->modSingle($id, $data)) {

        // 扩展内容修改
        foreach ($_POST as $key => $value) {
            if (preg_match('/^ext_[\w\-]+$/', $key)) {
                $temp = post($key);
                if (is_array($temp)) {
                    $data2[$key] = implode(',', $temp);
                } else {
                    $data2[$key] = str_replace("\r\n", '<br>', $temp);
                }
            }
        }
        if (isset($data2)) {
            if ($this->model->findContentExt($id)) {
                $this->model->modContentExt($id, $data2);
            } else {
                $data2['contentid'] = $id;
                $this->model->addContentExt($data2);
            }
        }

        $this->log('修改单页内容' . $id . '成功！');
        if (! ! $backurl = get('backurl')) {
            success('修改成功！', base64_decode($backurl));
        } else {
            success('修改成功！', url('/admin/Single/index'));
        }
    } else {
        location(- 1);
    }
} else {
    // 调取修改内容
    $this->assign('mod', true);
    if (! $result = $this->model->getSingle($id)) {
        error('编辑的内容已经不存在！', - 1);
    }
    $this->assign('content', $result);

    // 扩展字段
    if (! $mcode = get('mcode', 'var')) {
        error('传递的模型编码参数有误，请核对后重试！');
    }
    $this->assign('extfield', model('admin.content.ExtField')->getModelField($mcode));

    $this->display('content/single.html');
}
```

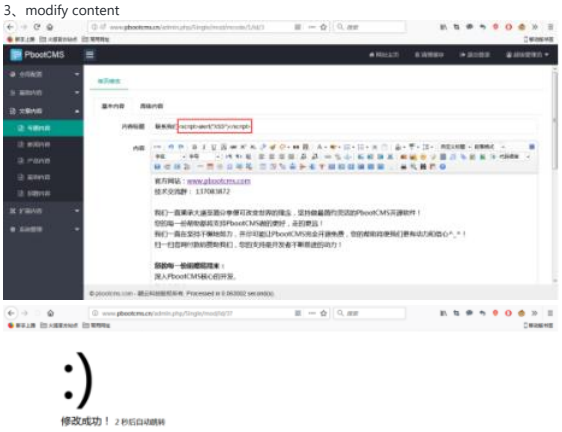
Vulnerability trigger point:
http://www.pbootcms.cn/index.php/about/11
1、Log in as admin

2、Choose this part





3、modify content



4、Added refresh vulnerability trigger point

Fix:
Filter the title parameter

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant