New issue

Jump to bottom

Bug:V6.0.6 Cross Site Scripting Vulnerability #2

Open **Richard1266** opened this issue on Mar 12, 2019 · 0 comments

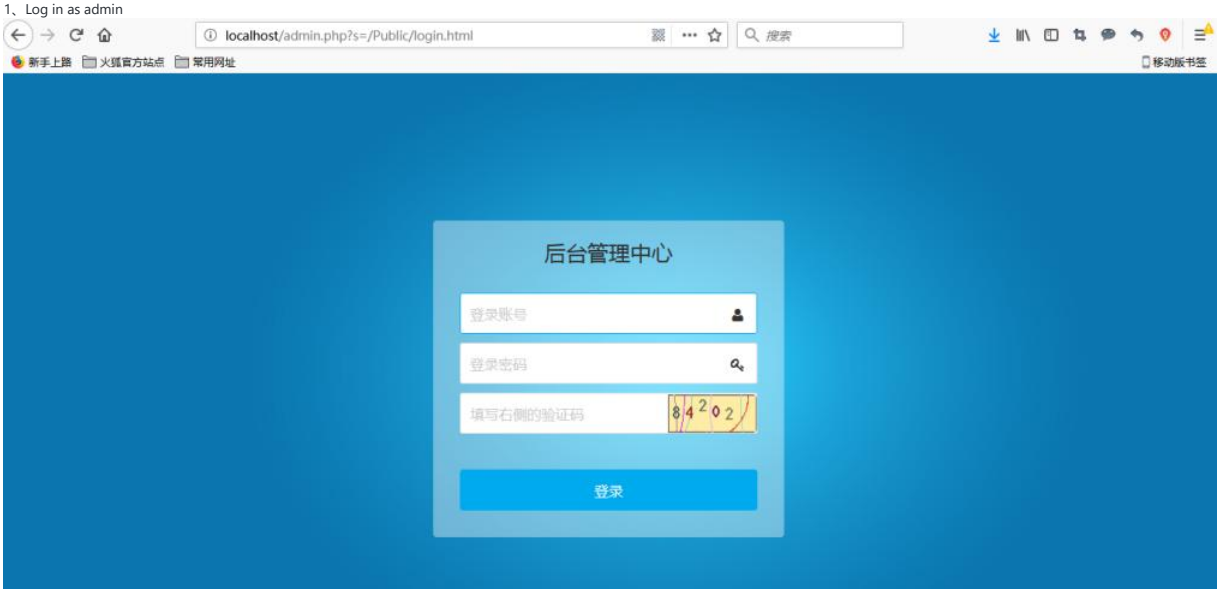
Richard1266 commented on Mar 12, 2019

There is an Stored Cross Site Scripting vulnerability in your latest version of the CMS v6.0.6
Download link: "https://www.damicms.com/downes/dami.rar"
In the DamicmsV6.0.6\Admin\Lib\Action\LabelAction.class.php, No filtering to title in the doadd() function:

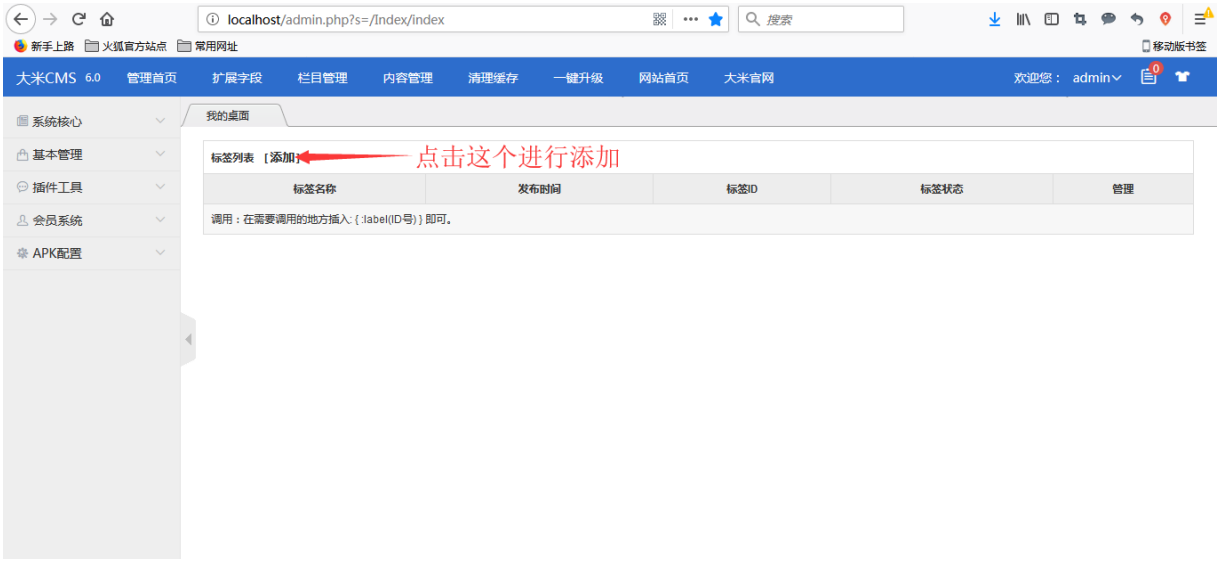
```php
public function doadd()
{
    $label = M('label');
    $data['title'] = $_POST['title'];
//使用stripslashes 反转义,防止服务器开启自动转义
    $data['content'] = stripslashes($_POST['content']);
    $data['addtime'] = date('Y-m-d H:i:s');
    if($label->add($data))
    {
        $this->assign("jumpUrl",U('Label/index'));
        $this->success('操作成功!');
    }
    $this->error('操作失败!');
}
```

没有过滤title参数

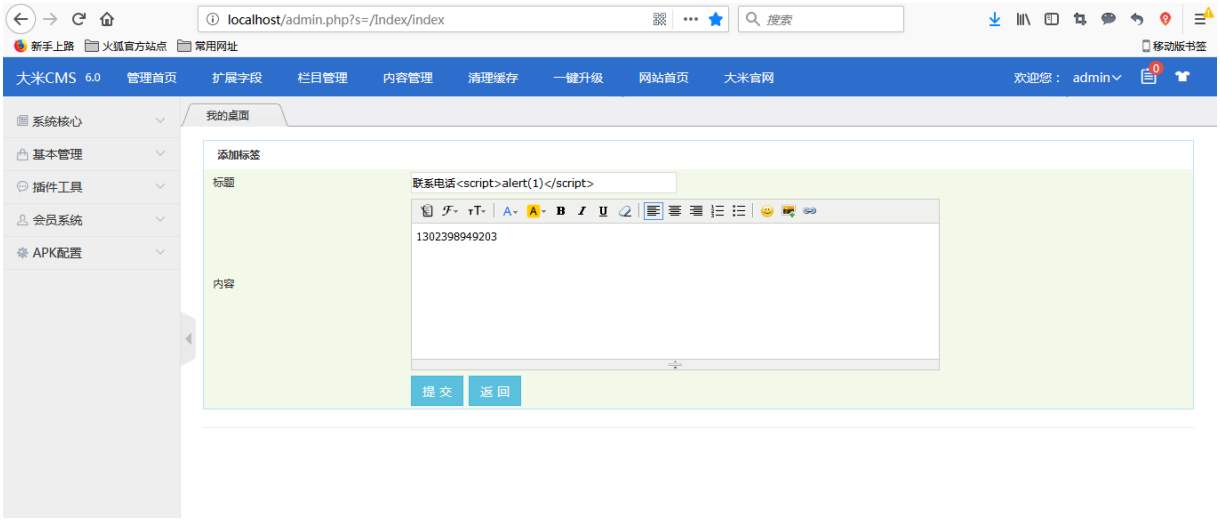
Vulnerability trigger point
http://localhost/admin.php?s=/Index/index
1、Log in as admin

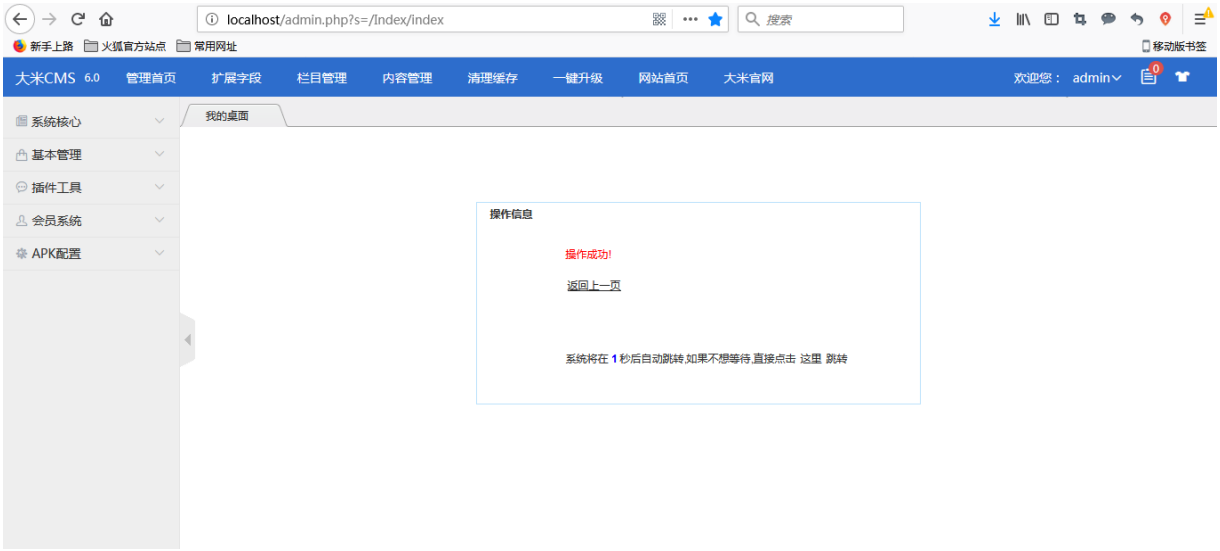


2、Choose this part

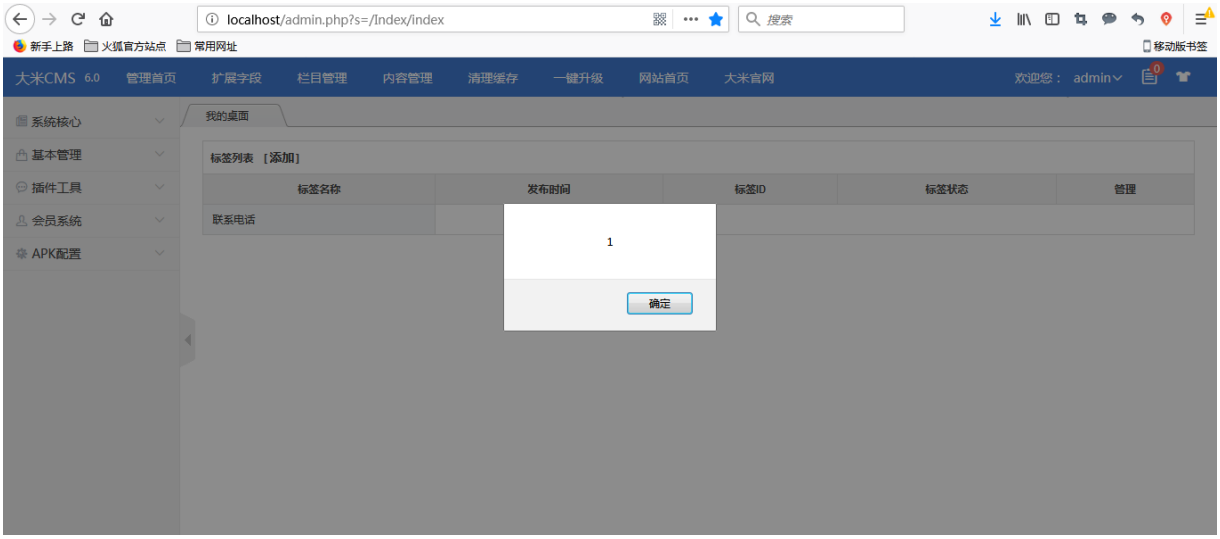


3、Add content





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