

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:

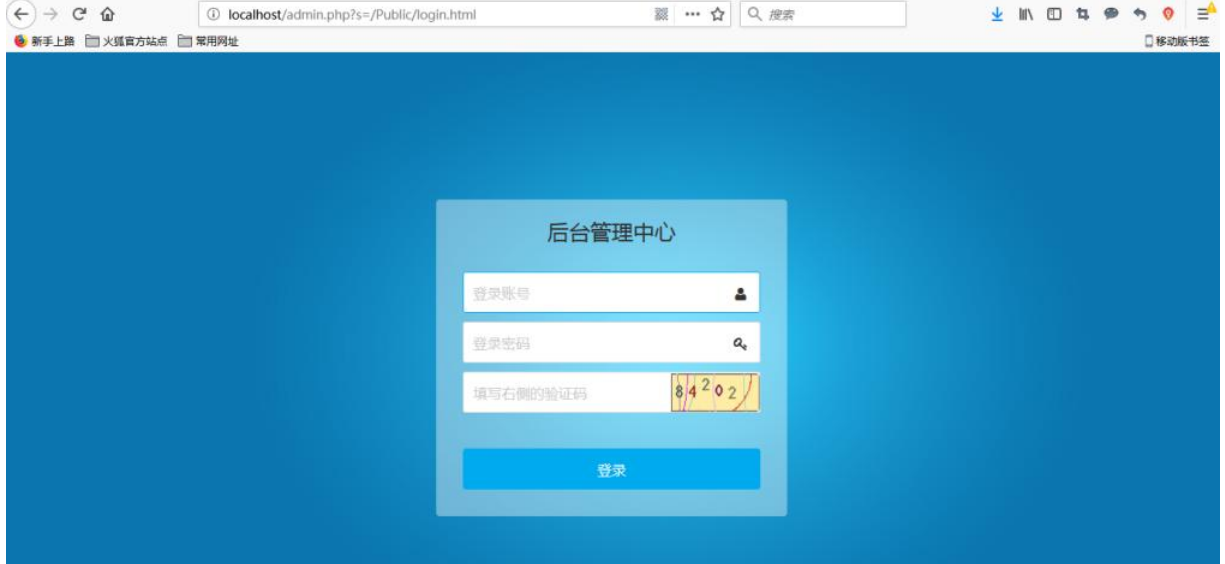
```
public function doadd()  
{  
    $label = M('label');  
    $data['title'] = $_POST['title'];  
    //使用stripslashes 反转义,防止服务器开启自动转义  
    $data['content'] = stripslashes($_POST['content']);  
    $data['addtime'] = date('Y-m-d H:i:s');  
    if($label->add($data))  
    {  
        $this->assign("jumpUrl",U('Label/index'));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

没有过滤
title参数

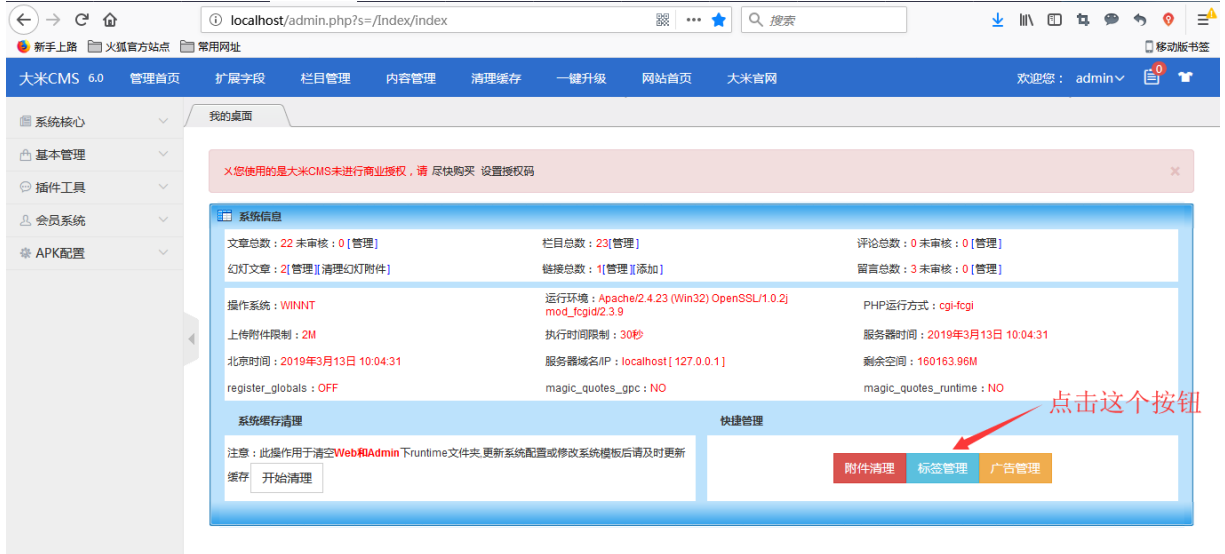
Vulnerability trigger point

http://localhost/admin.php?s=/Index/index

1、Log in as admin



2、Choose this part



localhost/admin.php?s=/Index/index

新手上路 火狐官方网站 常用网址

大米CMS 6.0 管理首页 扩展字段 栏目管理 内容管理 清理缓存 一键升级 网站首页 大米官网 欢迎您: admin

系统核心 基本管理 插件工具 会员系统 APK配置

我的桌面

标签列表 [添加] 点击这个进行添加

标签名称	发布时间	标签ID	标签状态	管理
调用: 在需要调用的地方插入: {label(ID号)} 即可。				

3、Add content

localhost/admin.php?s=/Index/index

新手上路 火狐官方网站 常用网址

大米CMS 6.0 管理首页 扩展字段 栏目管理 内容管理 清理缓存 一键升级 网站首页 大米官网 欢迎您: admin

系统核心 基本管理 插件工具 会员系统 APK配置

我的桌面

添加标签

标题 联系电话 <script>alert(1)</script>

内容 1302398949203

提交 返回

localhost/admin.php?s=/Index/index

新手上路 火狐官方网站 常用网址

大米CMS 6.0 管理首页 扩展字段 栏目管理 内容管理 清理缓存 一键升级 网站首页 大米官网 欢迎您: admin

系统核心 基本管理 插件工具 会员系统 APK配置

我的桌面

操作信息

操作成功!

返回上一页

系统将在 1 秒后自动跳转,如果不想等待,直接点击 这里 跳转

4、Added refresh vulnerability trigger point

←

→

🏠

localhost/admin.php?s=/Index/index

🔍 搜索

📖 新手上路

📁 火狐官方网站

📁 常用网址

📱 移动版书签

大米CMS 6.0

管理首页

扩展字段

栏目管理

内容管理

清理缓存

一键升级

网站首页

大米官网

欢迎您: admin

🔔

📁 系统核心

📁 基本管理

📁 插件工具

📁 会员系统

📁 APK配置

我的桌面

标签列表 【添加】

标签名称	发布时间	标签ID	标签状态	管理
联系电话				

1

确定

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

