

New issue

[Jump to bottom](#)

74cmsSE Storage cross site scripting vulnerability(XSS) #1

Open YLoiK opened this issue on Sep 23 · 0 comments

YLoiK commented on Sep 23 • edited ▼

Owner

Vulnerability Name: Storage cross site scripting vulnerability(XSS)

Date of Discovery: 23/9/2022

Product version: 74cmsSEv3.12.0 DownloadLink : <https://www.74cms.com/download/detail/89.html>

Author: xxhzz

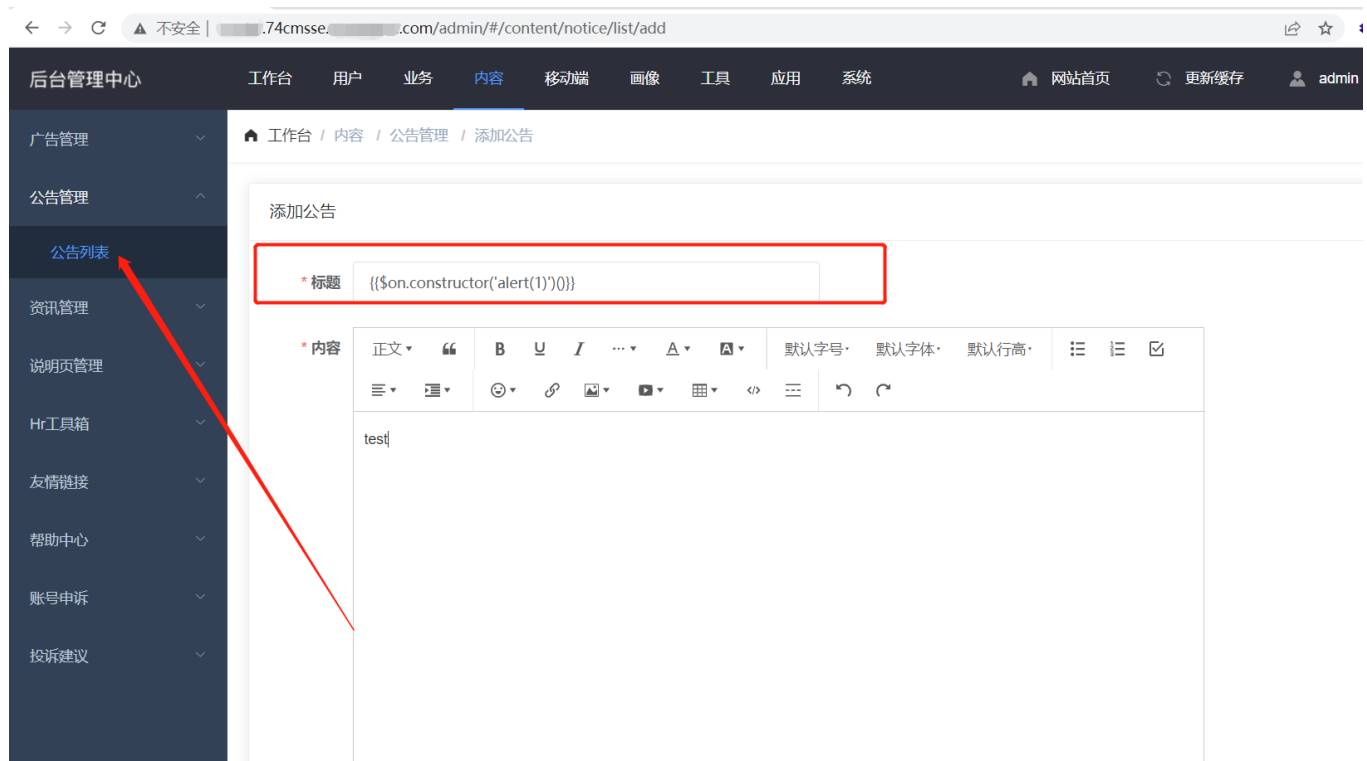
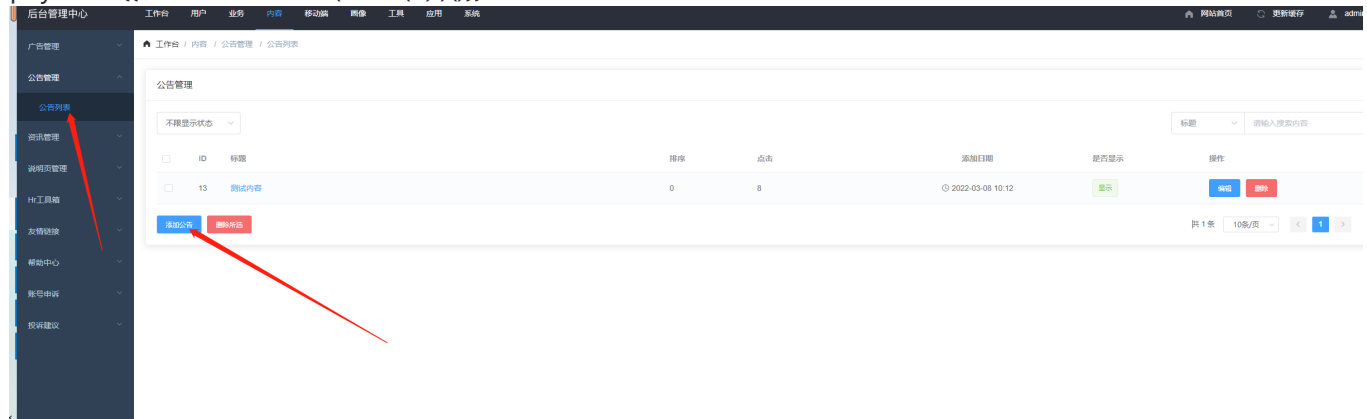
Vulnerability Description:

Add a bulletin to the background of 74cmSSE V3.12.0. Insert the XSS Payload into the header to store and trigger the XSS

Prove:

1.In the background of the website, add a bulletin and insert payload in the header

payload: `{{${on.constructor('alert(1)')()}}`



2.Check the parameter and find title



3.Save success

← → ↻ 不安全 | .74cmsse. .com/admin/#/content/notice/list

后台管理中心 工作台 用户 业务 内容 移动端 画像 工具 应用 系统 网站首页 更新缓存 admin (超级管理)

广告管理 公告管理 公告列表 资讯管理 说明页管理 Hr工具箱 友情链接 帮助中心 账号申诉 投诉建议

公告管理

不限显示状态 标题 请输入搜索内容

<input type="checkbox"/>	ID	标题	排序	点击	添加日期	是否显示	操作
<input type="checkbox"/>	20	{{\$.constructor("alert(1)");}}	0	6	2022-09-23 11:42	显示	编辑 删除
<input type="checkbox"/>	13	测试内容	0	8	2022-03-08 10:12	显示	编辑 删除

添加公告 删除所选 共 2 条 10条/页 1 前往 1

4.Click the title to trigger the XSS successfully

公告列表 - 网站后台中心 - Powe x {{\$.constructor("alert(1)");}} x

← → × 不安全 | .74cmsse. .com/notice/20.html

.74cmsse. .com 显示 1

确定

code:

Position: \74cmsSEv3.12.0\upload\application\apiadmin\controller\Notice.php

```
27 <?php
28
29 use Illuminate\Http\Request;
30 use Illuminate\Support\Facades\Validator;
31 use Illuminate\Support\Facades\Gate;
32 use App\Models\Notice;
33 use App\Models\User;
34 use App\Models\Article;
35
36 class NoticeController extends Controller
37 {
38     // 公告
39     public function index()
40     {
41         // 获取公告列表
42         $notices = Notice::paginate(10);
43         return view('notice.index', compact('notices'));
44     }
45
46     // 公告详情
47     public function show($id)
48     {
49         // 获取公告详情
50         $notice = Notice::findOrFail($id);
51         return view('notice.show', compact('notice'));
52     }
53
54     // 公告编辑
55     public function edit($id)
56     {
57         // 获取公告详情
58         $notice = Notice::findOrFail($id);
59
60         // 验证数据
61         $validator = Validator::make(request()->input(), [
62             'content' => 'required|string|max:200',
63             'title' => 'required|string|max:50',
64         ]);
65
66         if ($validator->fails()) {
67             return redirect()->back()->withErrors($validator);
68         }
69
70         // 更新公告
71         $notice->update(request()->input());
72
73         // 记录日志
74         $adminLog = new AdminLog();
75         $adminLog->record(
76             '添加公告: 公告ID【' .
77                 $notice->id .
78                 '】; 公告标题【' .
79                 $notice->title .
80                 '】',
81             $this->admininfo
82         );
83
84         return redirect()->back()->with('success', '保存成功');
85     }
86
87     public function update($id)
88     {
89         // 获取公告详情
90         $notice = Notice::findOrFail($id);
91
92         // 验证数据
93         $validator = Validator::make(request()->input(), [
94             'content' => 'required|string|max:200',
95             'title' => 'required|string|max:50',
96         ]);
97
98         if ($validator->fails()) {
99             return redirect()->back()->withErrors($validator);
100         }
101
102         // 更新公告
103         $notice->update(request()->input());
104
105         // 记录日志
106         $adminLog = new AdminLog();
107         $adminLog->record(
108             '更新公告: 公告ID【' .
109                 $notice->id .
110                 '】; 公告标题【' .
111                 $notice->title .
112                 '】',
113             $this->admininfo
114         );
115
116         return redirect()->back()->with('success', '保存成功');
117     }
118
119     // 公告删除
120     public function destroy($id)
121     {
122         // 获取公告详情
123         $notice = Notice::findOrFail($id);
124
125         // 删除公告
126         $notice->delete();
127
128         // 记录日志
129         $adminLog = new AdminLog();
130         $adminLog->record(
131             '删除公告: 公告ID【' .
132                 $notice->id .
133                 '】',
134             $this->admininfo
135         );
136
137         return redirect()->back()->with('success', '删除成功');
138     }
139 }
```

Check the xss parameter filtering mechanism and escape only the angle brackets

The screenshot shows a code editor with a sidebar containing a file explorer listing numerous PHP files such as Entrust.php, Explain.php, Export.php, Feedback.php, Link.php, Help.php, HelpCategory.php, Howford.php, Httos.php, HttpoolCategory.php, ImChatmanage.php, Inforbid.php, InQuikemng.php, Intubule.php, Index.php, Job.php, JobApply.php, JobInfo.php, JobInfoOleport.php, LinkSubmitt.php, Login.php, Market.php, Marketing.php, Member.php, MemberCancelApply.php, Newer.php, Notice.php, Order.php, Page.php, PageMobile.php, Personal.php, PersonalServiceStick.php, PersonalServiceTag.php, Poster.php, PromotioinJob.php, PromotionResume.php, OrCode.php, Resume.php, Resumelink.php, SceneOrCode.php, ServiceOl.php, Statmeal.php, ShortUrl.php, ShortVideo.php, Smallacklist.php, StatBusiness.php, StatCompanyOverview.php, StatIntention.php, Statlobhot.php, StatlobOverview.php, StatOrder.php, StatOverview.php, StatPersonal.php, StatResumeHot.php, StatResumeOverview.php, Subsite.php, SynTool.php, Task.php, Tpicof.php, Tipale.php, TweetsLabel.php, TweetsTemplate.php, Upgrade.php.

The main editor window displays the source code of AppController.php. The code includes several comments in Chinese and defines two public static functions: run() and logo(). A red rectangular box highlights the run() function.

```
// 控制器类  
// 开启跨站请求伪造机制  
set(C('URL_PARAMS_SAFE')){  
    $filters = C('URL_PARAMS_FILTER')?C('DEFAULT_FILTER');  
    if($filters){  
        $filters = explode('.', $filters);  
        foreach($filters as $filter){  
            $args = array_map_recursive($filter,$args); // 参数过滤  
        }  
    }  
    array_walk_recursive($args,'think_filter');  
    $method->invokeArgs($module,$args);  
}else{  
    $method->invoke($module);  
}  
// 检查版本  
if($class->hasMethod('__after_'.$_action)) {  
    $after = $class->getMethod('__after_'.$_action);  
    if($after->isPublic()) {  
        $after->invoke($module);  
    }  
}  
}else{  
    // 保存方法不是Public 抛出异常  
    throw new \ReflectionException();  
}  
}  
/**  
 * 该应用在实例、入口文件使用的快捷方法  
 * @access public  
 * @return void  
 */  
static public function run() {  
    // 应用初始化标签  
    Hook::listen('app_init');  
    App::init(),  
    // Session的初始化  
    if(!IS_CLI){  
        session(C('SESSION_OPTIONS'));  
    }  
    // 应用开始标签  
    Hook::listen('app_begin');  
    // 记录应用初始化时间  
    G('initTime');  
    App::exec()  
    // 应用结束标签  
    Hook::listen('app_end');  
    return ;  
}  
  
static public function logo(){
```

I am using AngularJS sandbox escapes reflected. Therefore, the storage xss vulnerability was successfully triggered.

Assignees

No one assigned

no one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

