

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

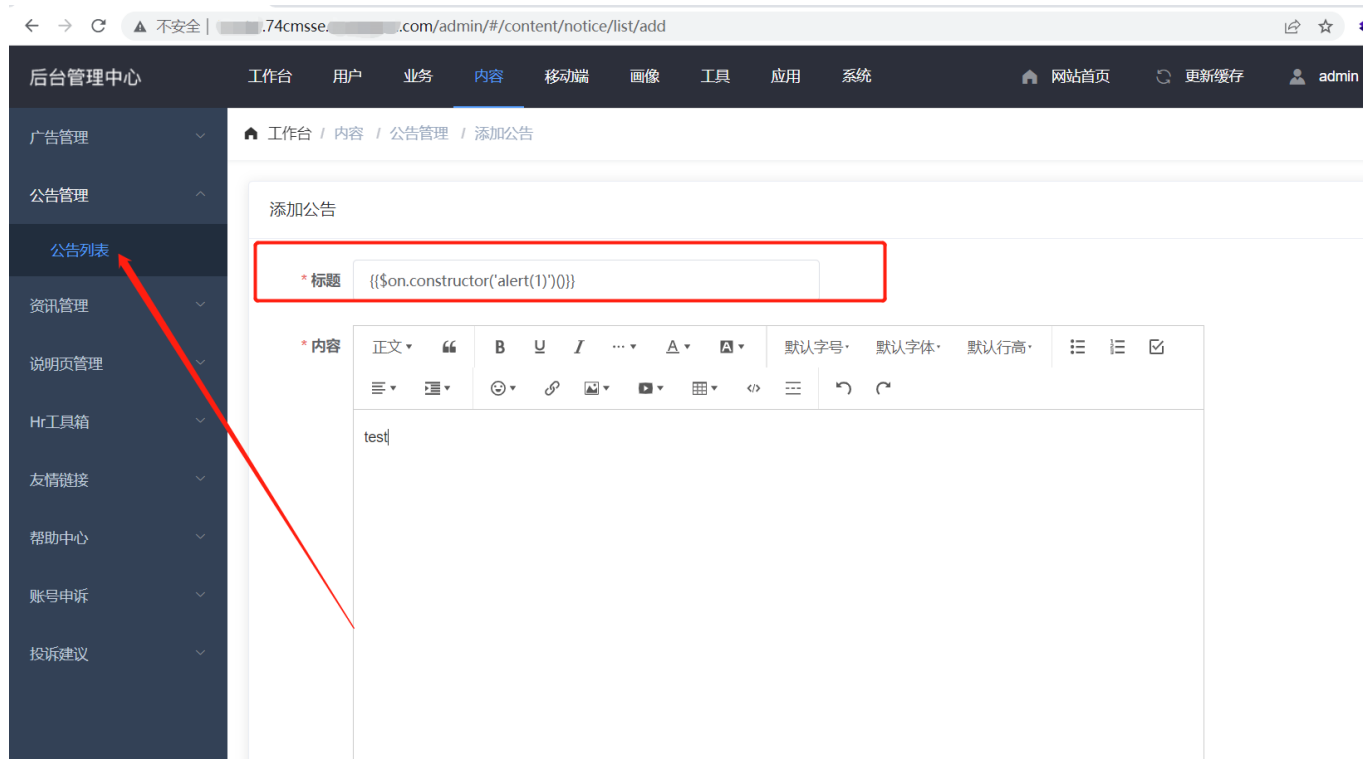
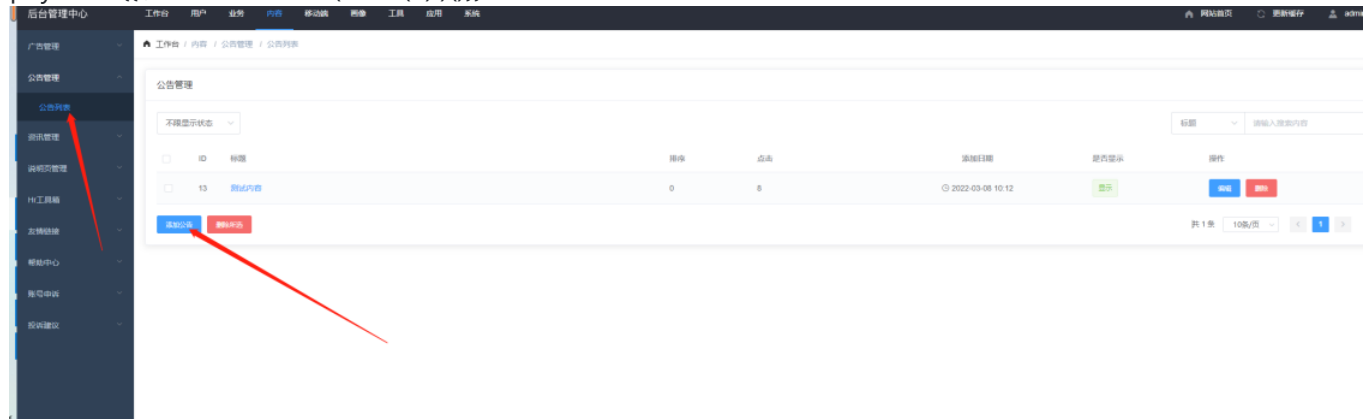
Vulnerability Description:

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

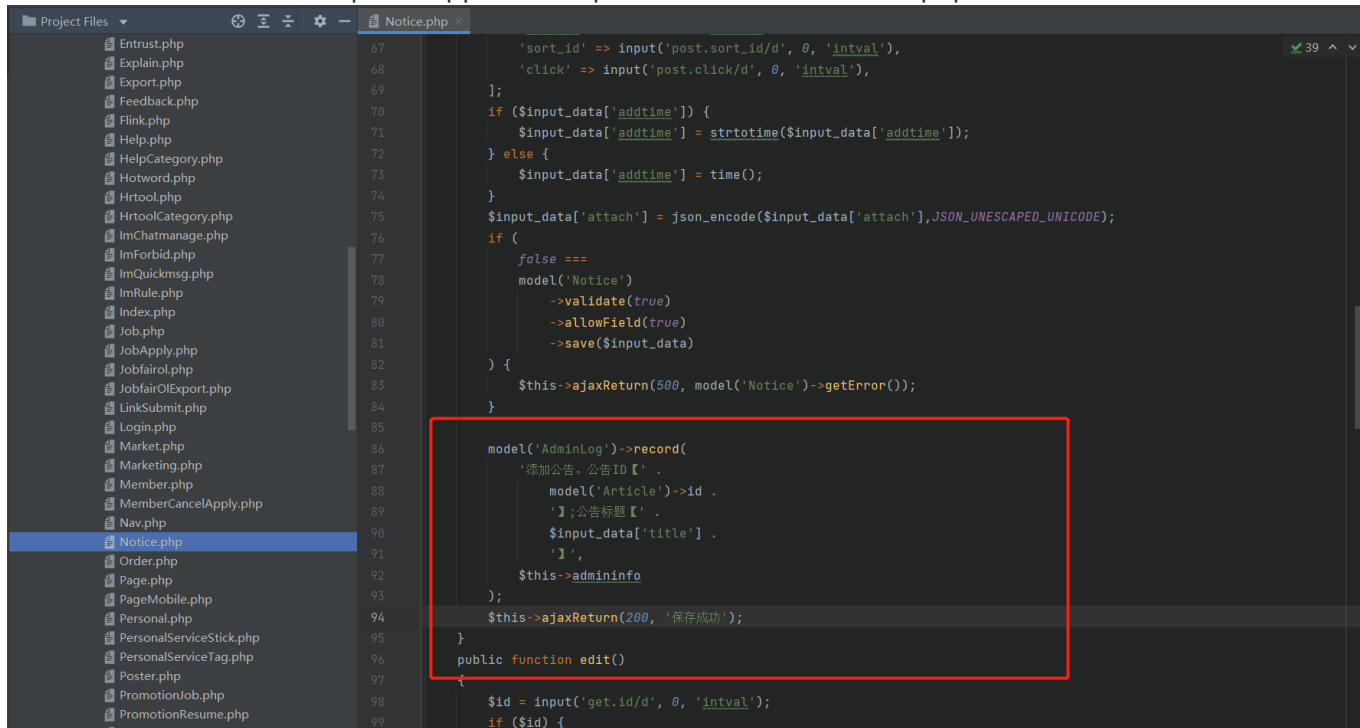
← → × 不安全 | .74cmsse. .com/notice/20.html

.74cmsse. .com 显示 1

确定

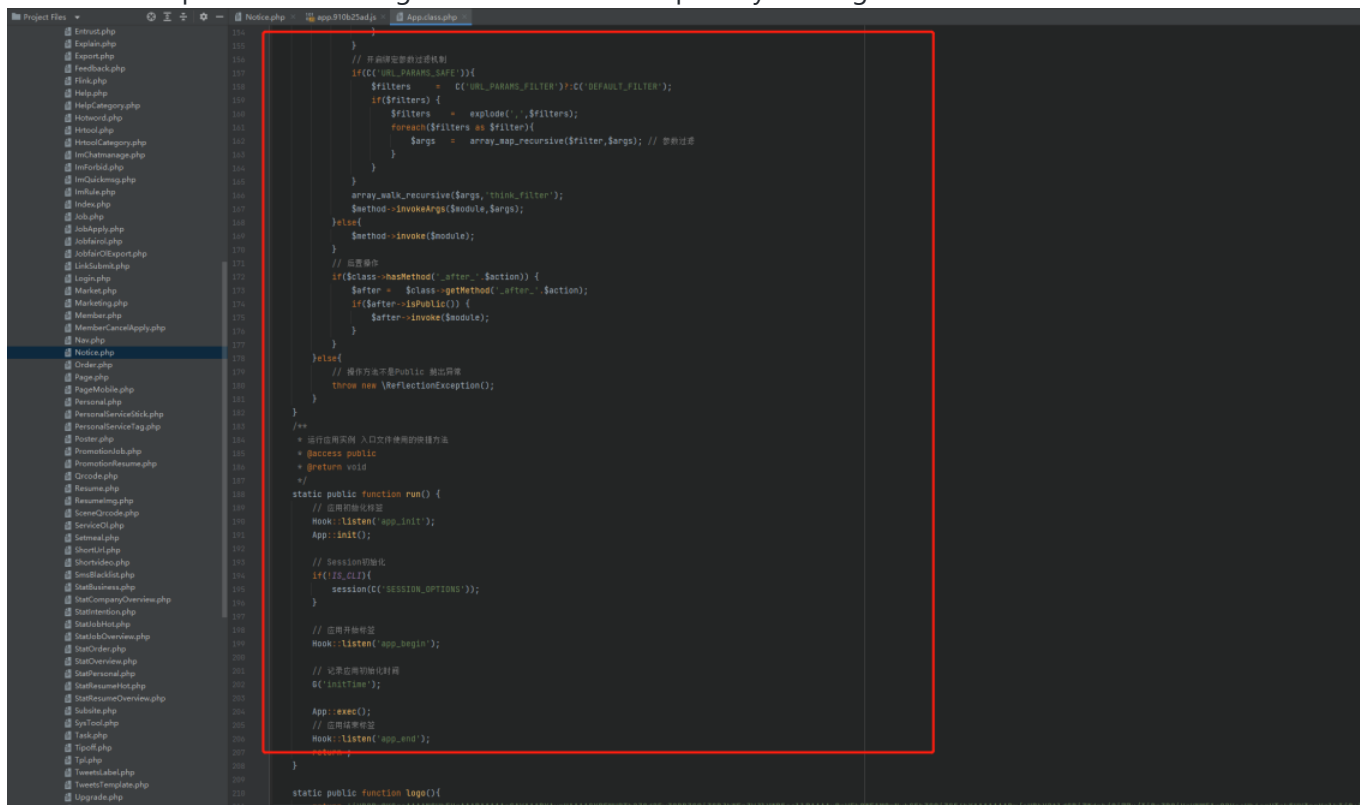
code:

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



```
67         'sort_id' => input('post.sort_id/d', 0, 'intval'),
68         'click' => input('post.click/d', 0, 'intval'),
69     ];
70     if ($input_data['addtime']) {
71         $input_data['addtime'] = strtotime($input_data['addtime']);
72     } else {
73         $input_data['addtime'] = time();
74     }
75     $input_data['attach'] = json_encode($input_data['attach'], JSON_UNESCAPED_UNICODE);
76     if (
77         false ===
78         model('Notice')
79             ->validate(true)
80             ->allowField(true)
81             ->save($input_data)
82     ) {
83         $this->ajaxReturn(500, model('Notice')->getError());
84     }
85
86     model('AdminLog')->record(
87         '添加公告. 公告ID【' .
88         model('Article')->id .
89         '】;公告标题【' .
90         $input_data['title'] .
91         '】',
92         $this->admininfo
93     );
94     $this->ajaxReturn(200, '保存成功');
95 }
96 public function edit()
97 {
98     $id = input('get.id/d', 0, 'intval');
99     if ($id) {
```

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



```
171 // 参数过滤
172 // 参数过滤函数过滤机制
173 if (C('URL_PARAMS_SAFE')) {
174     $filters = C('URL_PARAMS_FILTER'); // C('DEFAULT_FILTER');
175     if ($filters) {
176         $filters = explode(':', $filters);
177         foreach ($filters as $filter) {
178             $args = array_map_recursive($filter, $args); // 参数过滤
179         }
180     }
181     array_walk_recursive($args, 'think::filter');
182     $method->invokeArgs($module, $args);
183 } else {
184     $method->invoke($module);
185 }
186 // 异常捕获
187 if ($class->hasMethod('_after_.' . $action)) {
188     $after = $class->getMethod('_after_.' . $action);
189     if ($after->isPublic()) {
190         $after->invoke($module);
191     }
192 }
193 } elseif (
194     // 操作方法不是Public 抛出异常
195     throw new \ReflectionException();
196 ) {
197 }
198 /**
199  * 运行应用实例 入口文件使用的方法
200  * @access public
201  * @return void
202  */
203 static public function run() {
204     // 应用初始化设置
205     Hook::listen('app_init');
206     App::init();
207
208     // Session初始化
209     if (isset($_SESSION)) {
210         session(C('SESSION_OPTIONS'));
211     }
212
213     // 应用开始标记
214     Hook::listen('app_begin');
215
216     // 记录应用初始化时间
217     G('initTime');
218
219     App::exec();
220     // 应用结束标记
221     Hook::listen('app_end');
222     return;
223 }
224
225 static public function logon() {
226     return;
227 }
```

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

