New issue

Jump to bottom

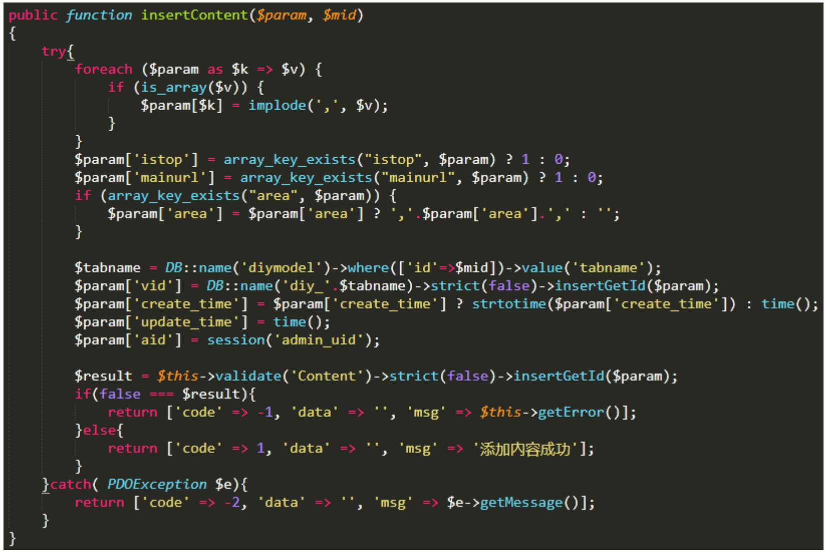
Bug:V1.1.9 Cross Site Scripting Vulnerability #9

⊙ Open Richard1266 opened this issue on Mar 7, 2019 · 0 comments

Richard1266 commented on Mar 7, 2019

There is an Stored Cross Site Scripting vulnerability in your latest version of the CMS v1.1.9
Download link: "http://img.yunucms.com/o_1d1n2lp3h1g0m1rjfvf818epqmua.zip?attname="

In the YUNUCMSv1.1.9\app\admin\model\ContentModel.php,No filtering to param in the insertContent( ) function:

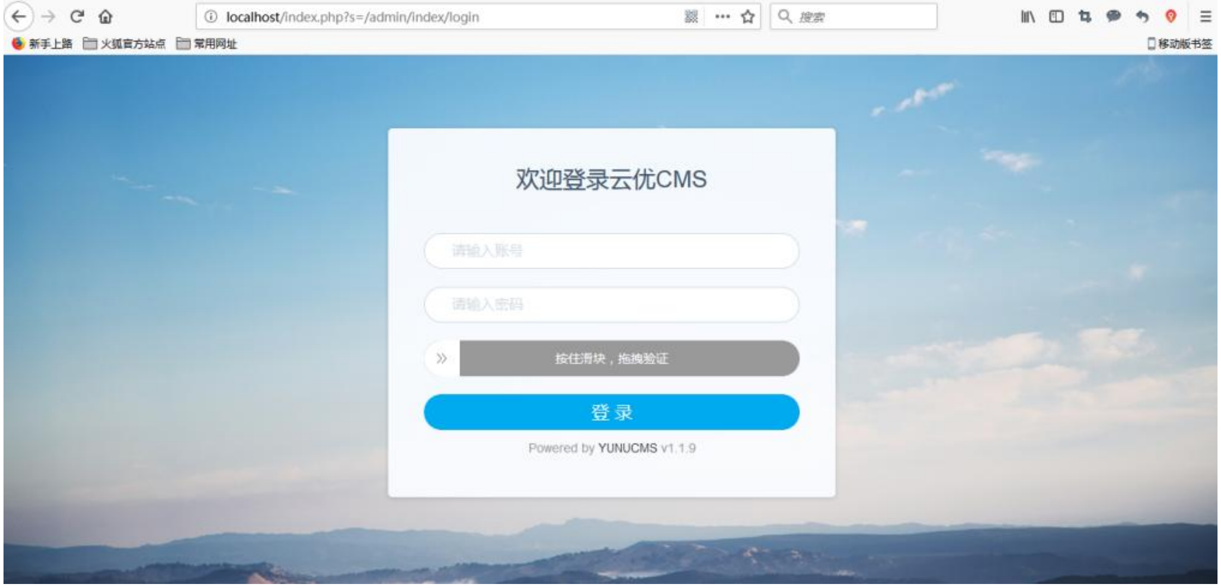


```php
public function insertContent($param, $mid)
{
    try{
        foreach ($param as $k => $v) {
            if (is_array($v)) {
                $param[$k] = implode(',', $v);
            }
        }
        $param['istop'] = array_key_exists("istop", $param) ? 1 : 0;
        $param['mainurl'] = array_key_exists("mainurl", $param) ? 1 : 0;
        if (array_key_exists("area", $param)) {
            $param['area'] = $param['area'] ? ','.$param['area'].',' : '';
        }

        $tabname = DB::name('diymodel')->where(['id'=>$mid])->value('tabname');
        $param['vid'] = DB::name('diy_'.$tabname)->strict(false)->insertGetId($param);
        $param['create_time'] = $param['create_time'] ? strtotime($param['create_time']) : time();
        $param['update_time'] = time();
        $param['aid'] = session('admin_uid');

        $result = $this->validate('Content')->strict(false)->insertGetId($param);
        if(false === $result){
            return ['code' => -1, 'data' => '', 'msg' => $this->getError()];
        }else{
            return ['code' => 1, 'data' => '', 'msg' => '添加内容成功'];
        }
    }catch( PDOException $e){
        return ['code' => -2, 'data' => '', 'msg' => $e->getMessage()];
    }
}
```

Vulnerability trigger point

http://localhost/index.php/index/category/index?id=23&page=3

1、Log in as admin



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

欢迎登录云优CMS

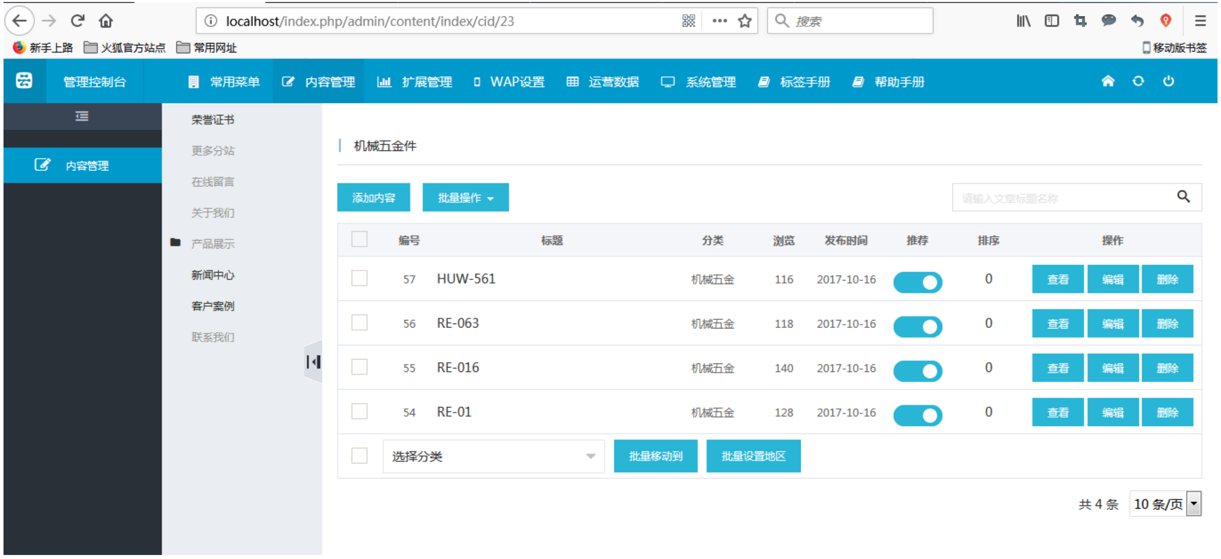
请输入账号

请输入密码

按住滑块，拖拽验证

Powered by YUNUCMS v1.1.9

2、Choose this part



localhost/index.php/admin/content/index/cid/23

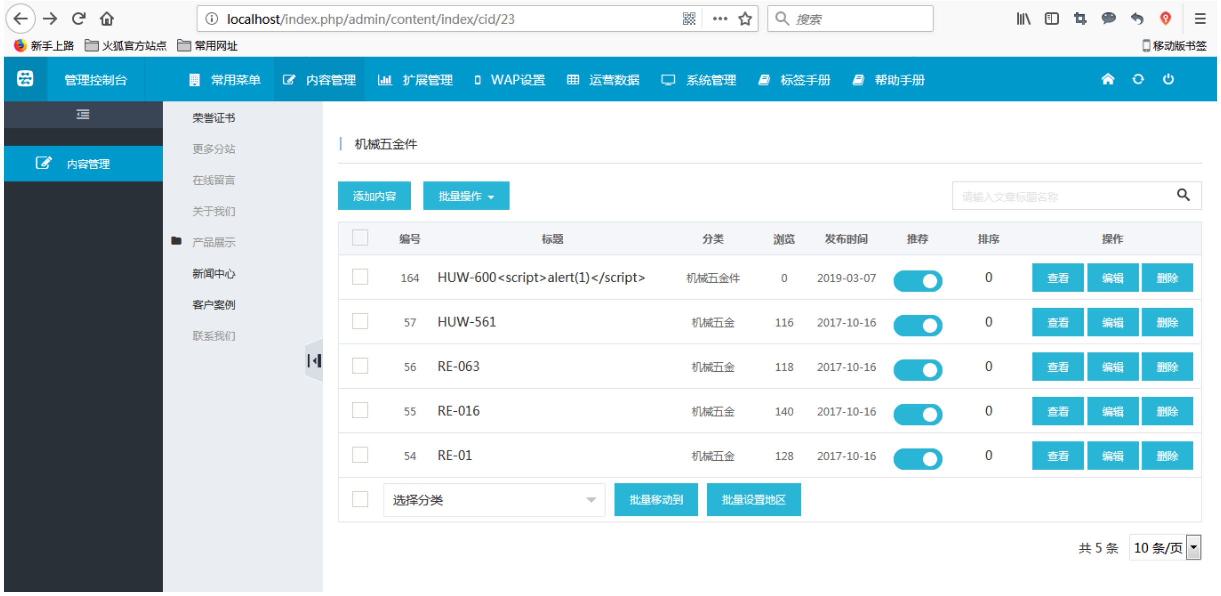
机械五金件

□	编号	标题	分类	浏览	发布时间	推荐	排序	操作
□	57	HUW-561	机械五金	116	2017-10-16		0	查看 编辑 删除
□	56	RE-063	机械五金	118	2017-10-16		0	查看 编辑 删除
□	55	RE-016	机械五金	140	2017-10-16		0	查看 编辑 删除
□	54	RE-01	机械五金	128	2017-10-16		0	查看 编辑 删除

□ 选择分类 批量移动到 批量设置地区

共 4 条 10 条/页

3、Add content



localhost/index.php/admin/content/index/cid/23

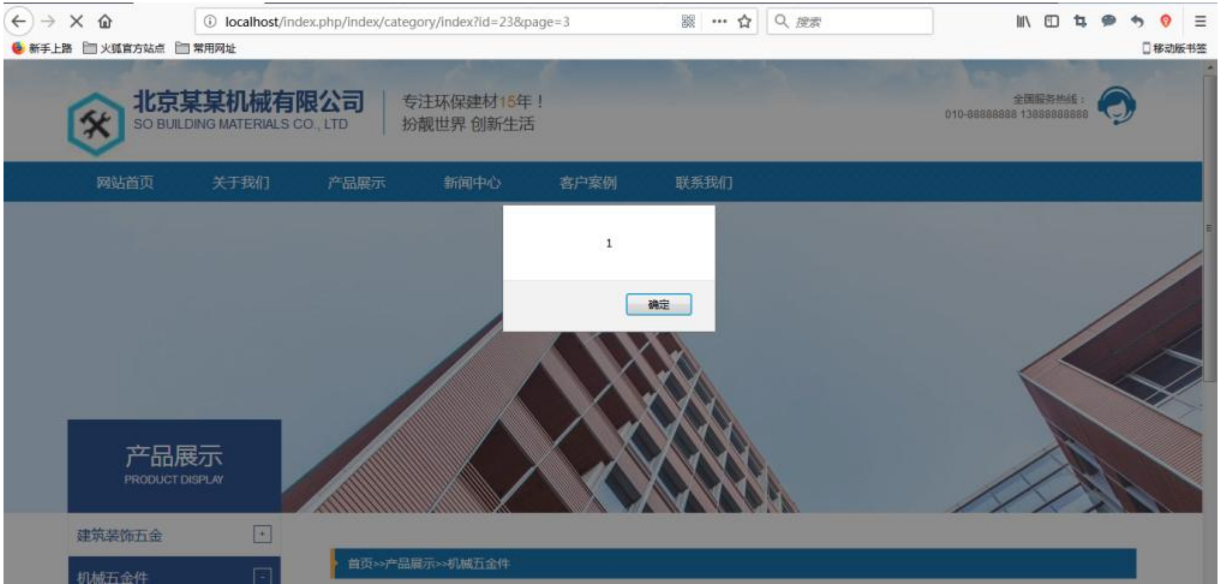
机械五金件

□	编号	标题	分类	浏览	发布时间	推荐	排序	操作
□	164	HUW-600<script>alert(1)</script>	机械五金件	0	2019-03-07		0	查看 编辑 删除
□	57	HUW-561	机械五金	116	2017-10-16		0	查看 编辑 删除
□	56	RE-063	机械五金	118	2017-10-16		0	查看 编辑 删除
□	55	RE-016	机械五金	140	2017-10-16		0	查看 编辑 删除
□	54	RE-01	机械五金	128	2017-10-16		0	查看 编辑 删除

□ 选择分类 批量移动到 批量设置地区

共 5 条 10 条/页

4、Added refresh vulnerability trigger point



localhost/index.php/index/category/index?id=23&page=3

1

Fix:
Filter the param parameter

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant