hillerlin / bycms Public

Code Issues 3 Pull requests Actions Projects Security ···

New issue

Jump to bottom

Bug:V1.3.0 Cross Site Scripting Vulnerability #2

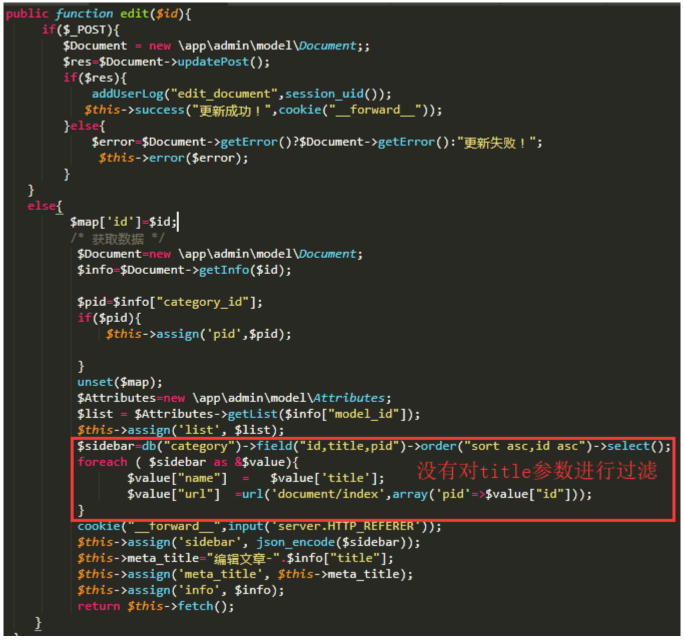
Open **Richard1266** opened this issue on Mar 21, 2019 · 0 comments

Richard1266 commented on Mar 21, 2019 • edited

There is an Stored Cross Site Scripting vulnerability in your latest version of the CMS v1.3.0

Download link: "http://ahdx.down.chinaz.com/201901/bycms_v1.3.zip"

In the BYCMSv1.3.0\application\admin\controller\Document.php, No filtering to title in the edit( ) function:



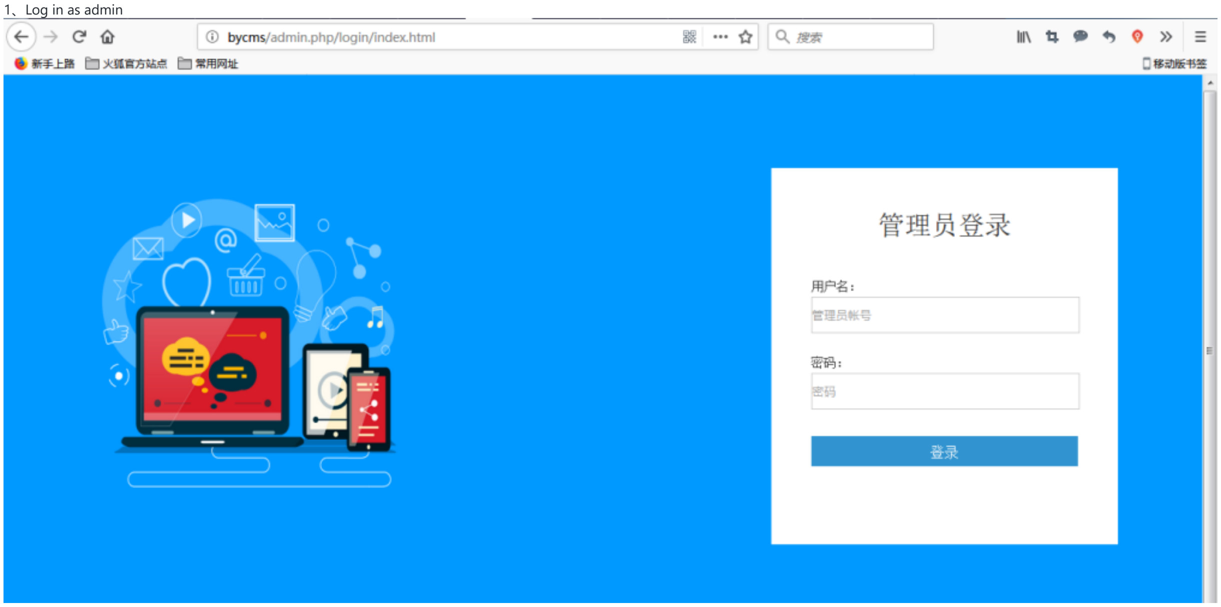
```php
public function edit($id){
     if($_POST){
        $Document = new \app\admin\model\Document;;
        $res=$Document->updatePost();
        if($res){
            addUserLog("edit_document",session_uid());
           $this->success("更新成功！",cookie("__forward__"));
        }else{
            $error=$Document->getError()?$Document->getError():"更新失败！";
             $this->error($error);
        }
    }
    else{
         $map['id']=$id;
         /* 获取数据 */
          $Document=new \app\admin\model\Document;
          $info=$Document->getInfo($id);

          $pid=$info["category_id"];
          if($pid){
              $this->assign('pid',$pid);

          }
          unset($map);
          $Attributes=new \app\admin\model\Attributes;
          $list = $Attributes->getList($info["model_id"]);
          $this->assign('list', $list);
          $sidebar=db("category")->field("id,title,pid")->order("sort asc,id asc")->select();
          foreach ( $sidebar as &$value){
                 $value["name"]  =   $value['title'];
                 $value["url"]  =url('document/index',array('pid'=>$value["id"]));
          }
          cookie("__forward__",input('server.HTTP_REFERER'));
          $this->assign('sidebar', json_encode($sidebar));
          $this->meta_title="编辑文章-".$info["title"];
          $this->assign('meta_title', $this->meta_title);
          $this->assign('info', $info);
          return $this->fetch();
     }
```

没有对title参数进行过滤

Vulnerability trigger point

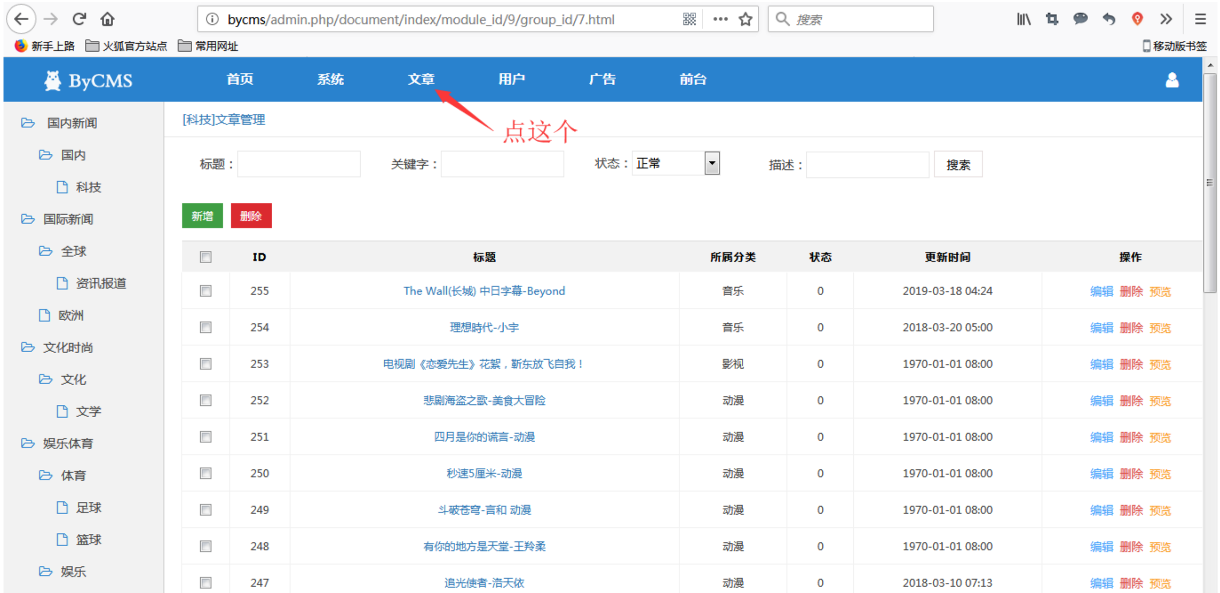
http://bycms/admin.php/document/index/module_id/9/group_id/7.html

1、Log in as admin



bycms/admin.php/login/index.html

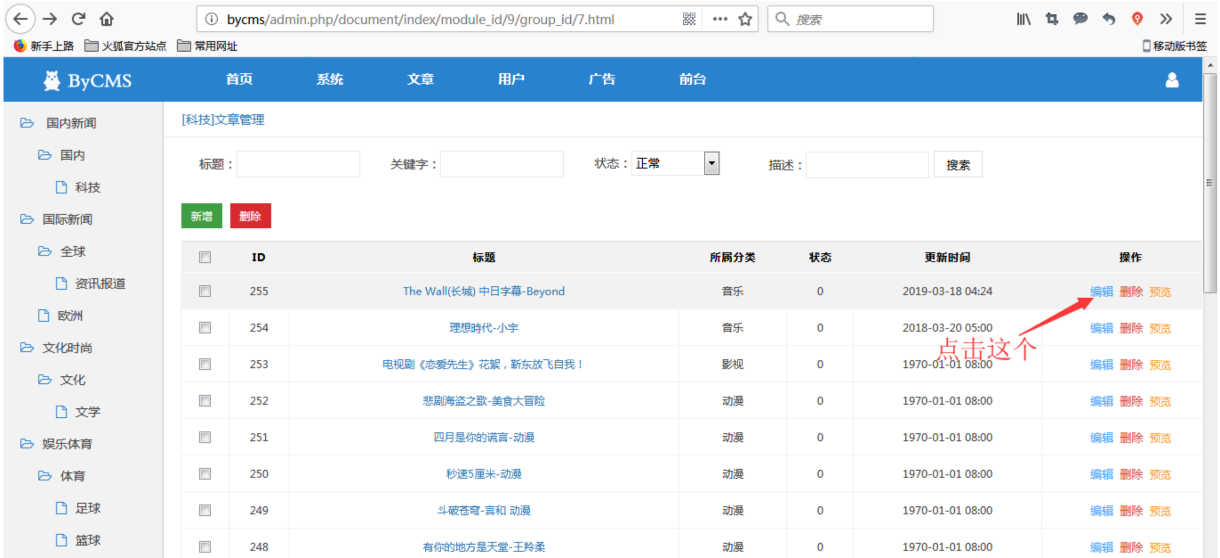
2、Choose this part



[科技]文章管理

标题： 关键字： 状态： 正常 描述：

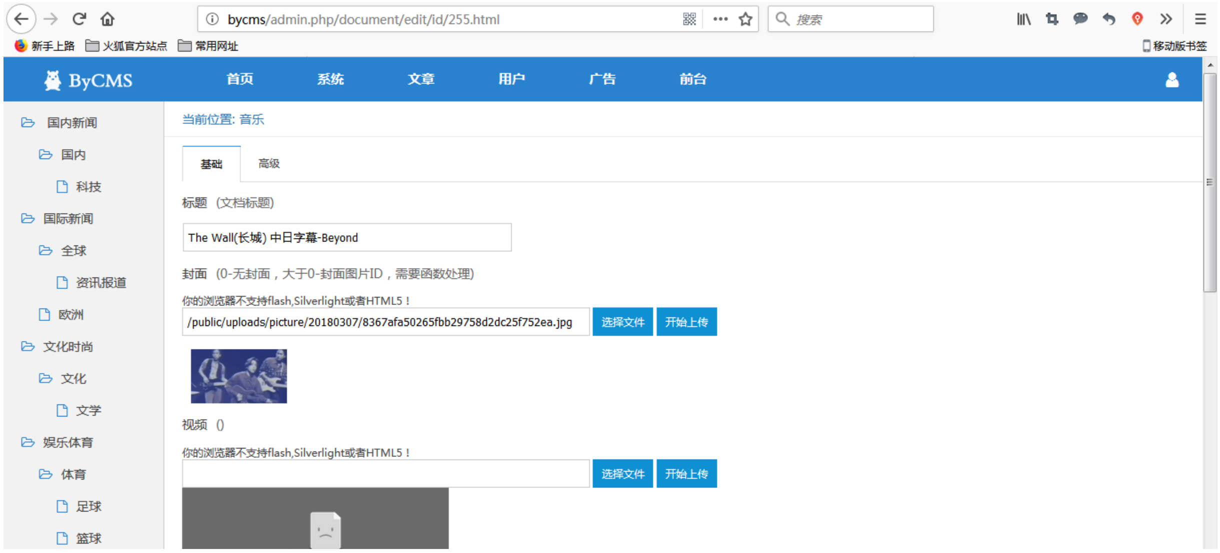
□	ID	标题	所属分类	状态	更新时间	操作
□	255	The Wall(长城) 中日字幕-Beyond	音乐	0	2019-03-18 04:24	编辑 删除 预览
□	254	理想时代-小宇	音乐	0	2018-03-20 05:00	编辑 删除 预览
□	253	电视剧《恋爱先生》花絮，靳东放飞自我！	影视	0	1970-01-01 08:00	编辑 删除 预览
□	252	悲剧海盗之歌-美食大冒险	动漫	0	1970-01-01 08:00	编辑 删除 预览
□	251	四月是你的谎言-动漫	动漫	0	1970-01-01 08:00	编辑 删除 预览
□	250	秒速5厘米-动漫	动漫	0	1970-01-01 08:00	编辑 删除 预览
□	249	斗破苍穹-言和 动漫	动漫	0	1970-01-01 08:00	编辑 删除 预览
□	248	有你的地方是天堂-王羚柔	动漫	0	1970-01-01 08:00	编辑 删除 预览
□	247	追光使者-洛天依	动漫	0	2018-03-10 07:13	编辑 删除 预览



[科技]文章管理

标题： 关键字： 状态： 正常 描述：

□	ID	标题	所属分类	状态	更新时间	操作
□	255	The Wall(长城) 中日字幕-Beyond	音乐	0	2019-03-18 04:24	编辑 删除 预览
□	254	理想时代-小宇	音乐	0	2018-03-20 05:00	编辑 删除 预览
□	253	电视剧《恋爱先生》花絮，靳东放飞自我！	影视	0	1970-01-01 08:00	编辑 删除 预览
□	252	悲剧海盗之歌-美食大冒险	动漫	0	1970-01-01 08:00	编辑 删除 预览
□	251	四月是你的谎言-动漫	动漫	0	1970-01-01 08:00	编辑 删除 预览
□	250	秒速5厘米-动漫	动漫	0	1970-01-01 08:00	编辑 删除 预览
□	249	斗破苍穹-言和 动漫	动漫	0	1970-01-01 08:00	编辑 删除 预览
□	248	有你的地方是天堂-王羚柔	动漫	0	1970-01-01 08:00	编辑 删除 预览



当前位置: 音乐

标题（文档标题）

The Wall(长城) 中日字幕-Beyond

封面（0-无封面，大于0-封面图片ID，需要函数处理）

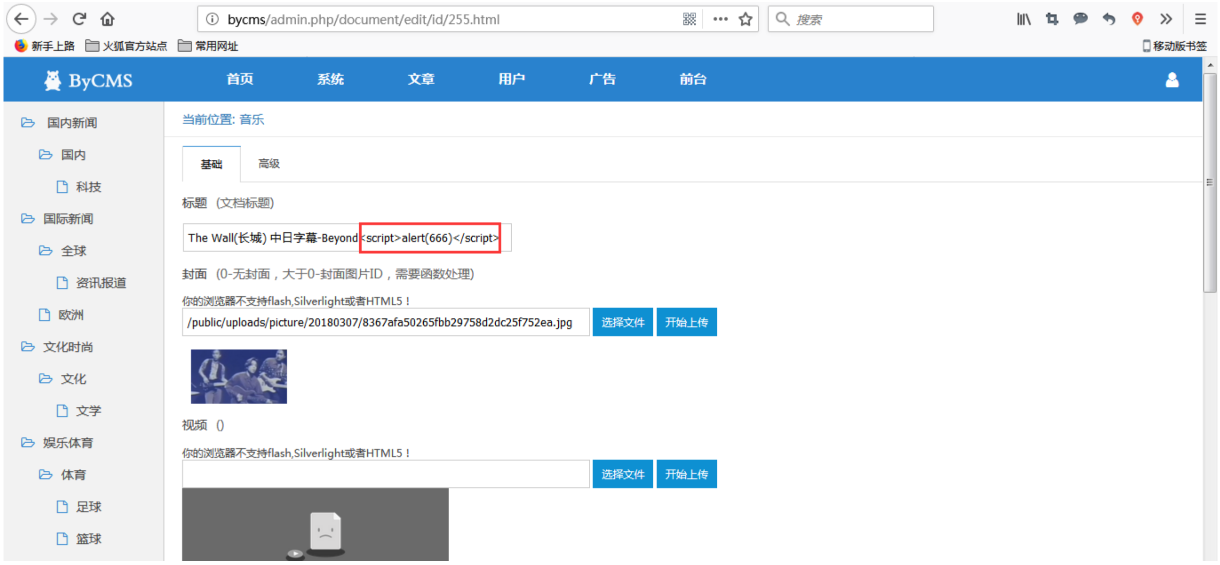
你的浏览器不支持flash,Silverlight或者HTML5！

/public/uploads/picture/20180307/8367afa50265fbb29758d2dc25f752ea.jpg

视频（）

你的浏览器不支持flash,Silverlight或者HTML5！

3、Modify content



bycms/admin.php/document/edit/id/255.html

当前位置: 音乐

标题（文档标题）

The Wall(长城) 中日字幕-Beyond<script>alert(666)</script>

封面（0-无封面，大于0-封面图片ID，需要函数处理）

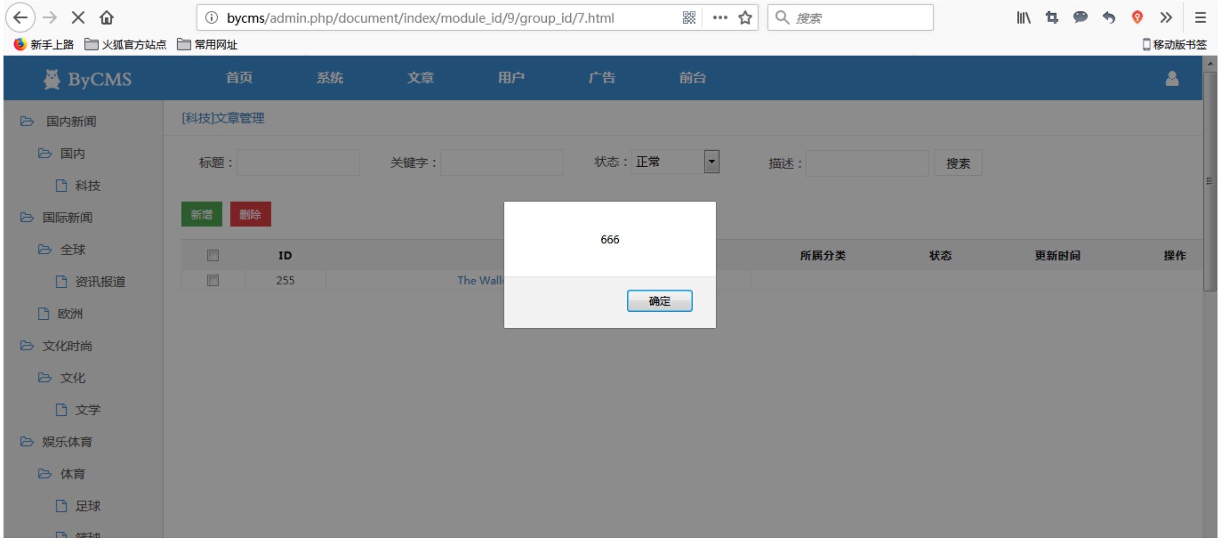
你的浏览器不支持flash,Silverlight或者HTML5！

/public/uploads/picture/20180307/8367afa50265fbb29758d2dc25f752ea.jpg

视频（）

你的浏览器不支持flash,Silverlight或者HTML5！

4、Edited the refresh vulnerability trigger point



bycms/admin.php/document/index/module_id/9/group_id/7.html

[科技]文章管理

标题： 关键字： 状态：正常 描述：

☐	ID		所属分类	状态	更新时间	操作
☐	255	The Wall				

666

Fix:
Filter the title parameter

Richard1266 changed the title ~~Bug:V3.0.4 Cross Site Scripting Vulnerability~~ Bug:V1.3.0 Cross Site Scripting Vulnerability on Apr 8, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant