New issue

Bug:V2.0.0 Cross-site request forgery #2

Open Richard1266 opened this issue on Apr 29, 2019 · 0 comments

Richard1266 commented on Apr 29, 2019

Owner

There is an Cross-site request forgery vulnerability in your latest version of the CMS v2.0.0
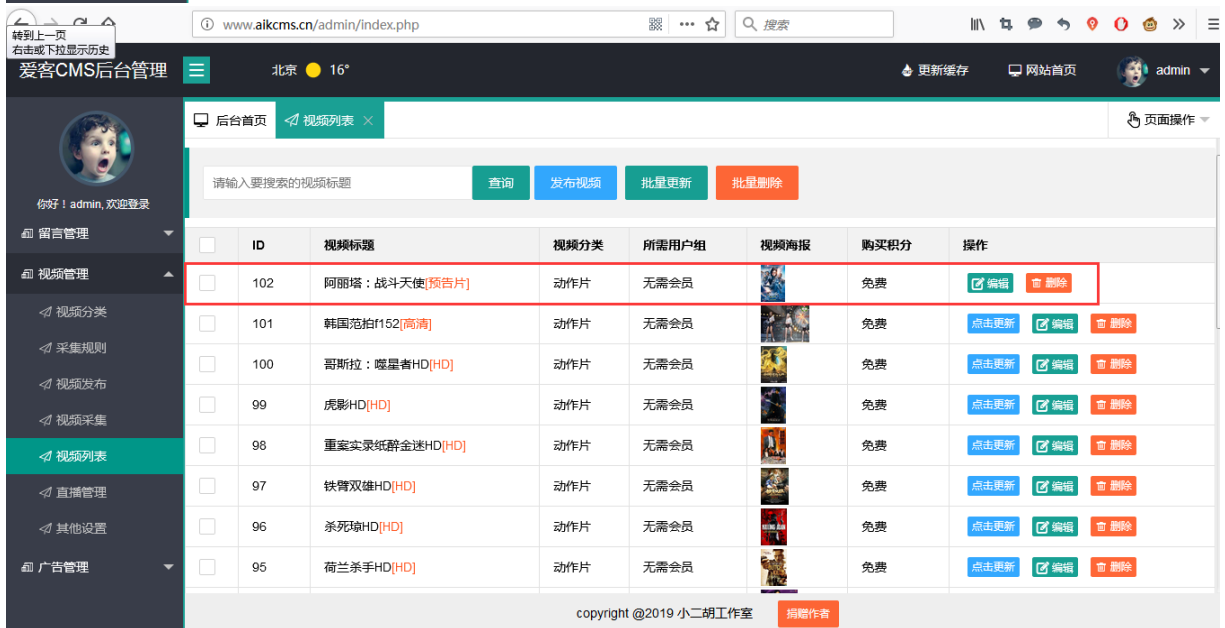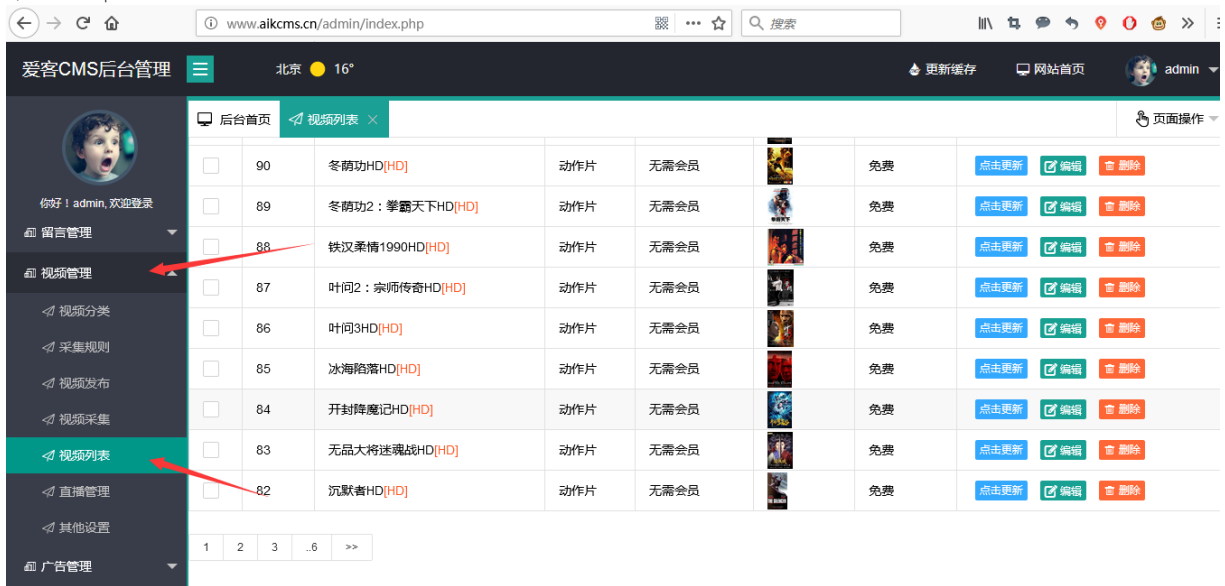
Download link: "http://www.aikcms.com/download/%E7%88%B1%E5%AE%A2CMS2.0.zip"

Vulnerability trigger point:

http://www.aikcms.cn/admin/page/video/video_list.php

1、Log in as admin

2、Choose this part

3、Capture the package to generate a POC file and run it

csrf.txt

Submit request

file:///C:/Users/orange@2/Desktop/csrf.html

www.aikcms.cn/admin/page/video/video_list.php?del=102

搜索

删除成功!

确定
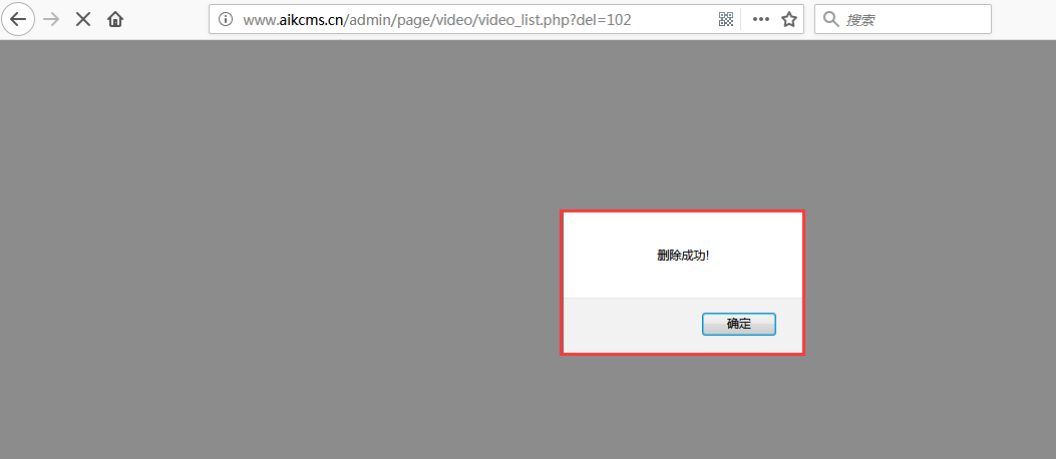
4、Refresh page has changed

www.aikcms.cn/admin/index.php

搜索

爱客CMS后台管理

北京 ☀ 16°

更新缓存　　网站首页　　admin

后台首页　　视频列表

页面操作

你好！admin,欢迎登录

留言管理

视频管理

　视频分类

　采集规则

　视频发布

　视频采集

　视频列表

　直播管理

　其他设置

广告管理

请输入要搜索的视频标题

查询　　发布视频　　批量更新　　批量删除

	ID	视频标题	视频分类	所需用户组	视频海报	购买积分	操作
☐	101	韩国范拍f152[高清]	动作片	无需会员		免费	点击更新 编辑 删除
☐	100	哥斯拉：噬星者HD[HD]	动作片	无需会员		免费	点击更新 编辑 删除
☐	99	虎影HD[HD]	动作片	无需会员		免费	点击更新 编辑 删除
☐	98	重案实录纸醉金迷HD[HD]	动作片	无需会员		免费	点击更新 编辑 删除
☐	97	铁臂双雄HD[HD]	动作片	无需会员		免费	点击更新 编辑 删除
☐	96	杀死琼HD[HD]	动作片	无需会员		免费	点击更新 编辑 删除
☐	95	荷兰杀手HD[HD]	动作片	无需会员		免费	点击更新 编辑 删除
☐	94	太子爷出差HD[HD]	动作片	无需会员		免费	点击更新 编辑 删除

javascript:;

copyright @2019 小二胡工作室　捐赠作者

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant