yzmcms / yzmcms Public

Code Issues 11 Pull requests 1 Actions Projects Security ···

New issue

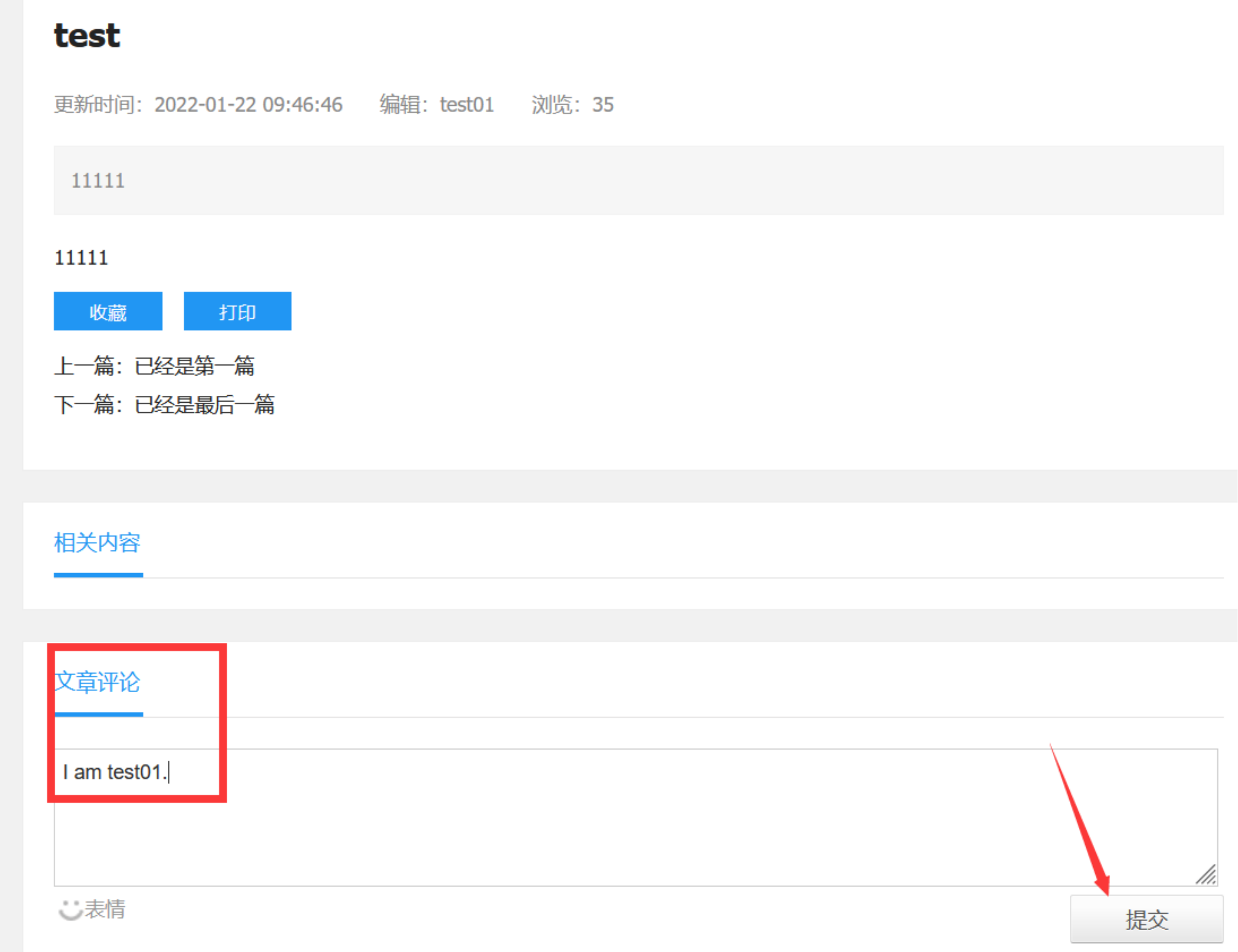
Jump to bottom

YzmCMSV6. 3. There is a CSRF vulnerability in the foreground in the official version(YzmCMS V6.3 正式版前台存在csrf漏洞) #60

Closed zpxlz opened this issue on Jan 21 · 1 comment

zpxlz commented on Jan 21 • edited

Prepare two accounts: test01 and test02, background settings allow users to contribute,
Generate POC of CSRF with test01, First log in to test01 and comment on an article, and grab the request packet,



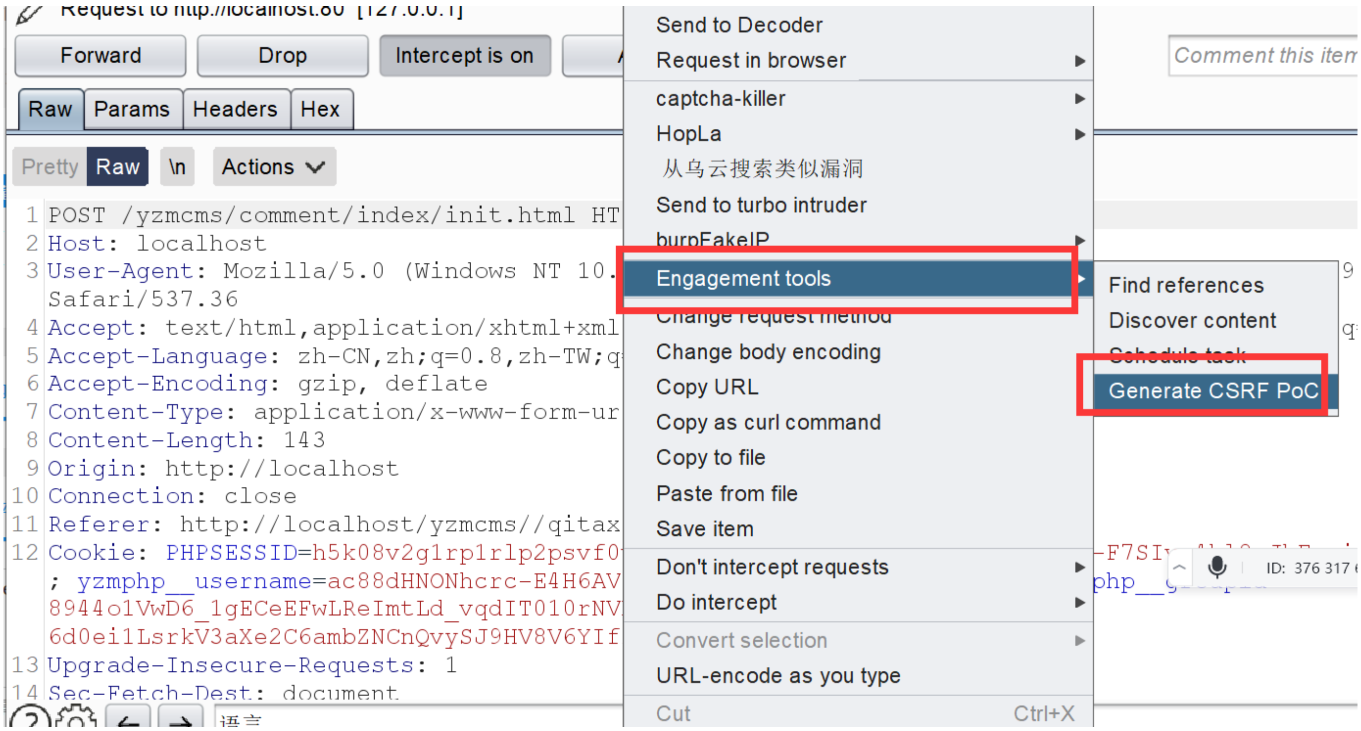
test

更新时间：2022-01-22 09:46:46 编辑：test01 浏览：35

11111

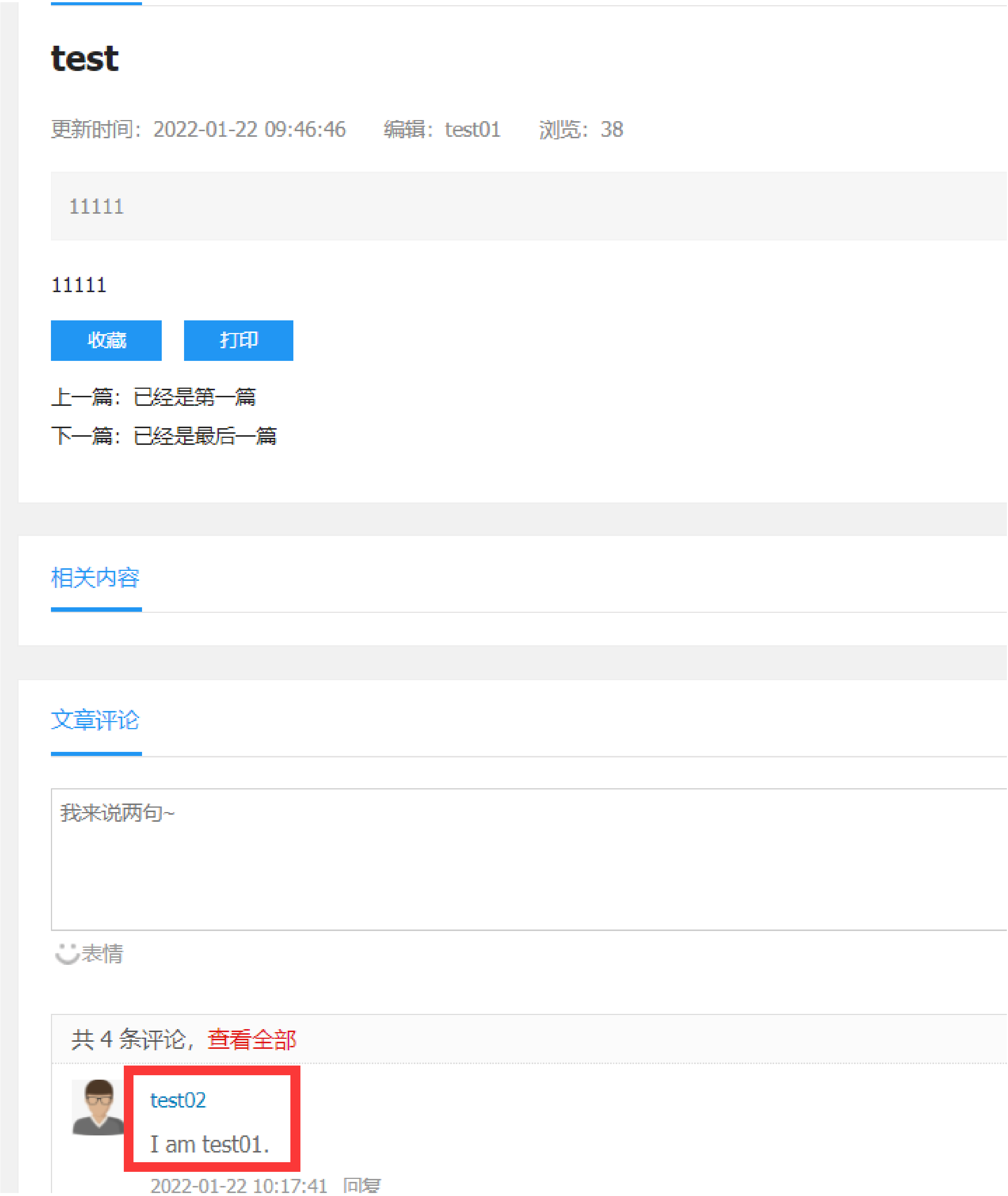
11111

I am test01.



```
POST /yzmcms/comment/index/init.html HT
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.
Safari/537.36
Accept: text/html,application/xhtml+xml
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-ur
Content-Length: 143
Origin: http://localhost
Connection: close
Referer: http://localhost/yzmcms//qitax
Cookie: PHPSESSID=h5k08v2g1rp1rlp2psvf0
; yzmphp__username=ac88dHNONhcrc-E4H6AV
8944o1VwD6_1gECeEFwLReImtLd_vqdIT010rNV
6d0ei1LsrkV3aXe2C6ambZNCnQvySJ9HV8V6YIf
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
```

Log in to TEST02 with another browser and open the web page of the generated POC,
Triggered CSRF and successfully commented as TEST02.



test

更新时间：2022-01-22 09:46:46　编辑：test01　浏览：38

11111

11111

上一篇：已经是第一篇

下一篇：已经是最后一篇

相关内容

文章评论

我来说两句~

共 4 条评论，查看全部

test02

I am test01.

2022-01-22 10:17:41　回复

yzmcms commented on Feb 13 Owner

非安全漏洞，无需修复

yzmcms closed this as completed on Feb 13

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants