

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

收藏

打印

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

I am test01.

表情

提交

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on

Raw Params Headers Hex

Pretty Raw In Actions

```
1 POST /yzmcms/comment/index/init.html HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4660.53 Safari/537.36
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 143
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/yzmcms//qitax
12 Cookie: PHPSESSID=h5k08v2g1rplrlp2psvf0; yzmphp_username=ac88dHNONhrcr-E4H6AV8944o1VwD6_1gECeEFwLReImtLd_vqdIT010rNV6d0ei1LsrkV3aXe2C6ambZNCnQvySJ9HV8V6YIf
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
```

Send to Decoder
Request in browser
captcha-killer
HopLa
从乌云搜索类似漏洞
Send to turbo intruder
burpFakeIP
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
Do intercept
Convert selection
URL-encode as you type
Cut

Find references
Discover content
Schedule task
Generate CSRF PoC

Comment this item

F7SI ID: 376 317

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

收藏

打印

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~

表情

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

