Write Up

PicoCTF 2019

Institut Teknologi Sepuluh Nopember

Aaron Christopher Tanhar

07211940000055

Dibuat menggunakan LaTeX

Daftar Isi

1. plumbing(200 points)

Soal: Sometimes you need to handle process data outside of a file. Can you find a way to keep the output from this program and search for the flag? Connect to 2019shell1.picoctf.com 57911.
Solusi:
nc 2019shell1.picoctf.com 57911 — grep ”picoCTF{.*}”
EZ PZ

2. picobrowser(200 points)

Soal: This website can be rendered only by picobrowser, go and catch the flag!
https://2019shell1.picoctf.com/problem/32205/ (link) or http://2019shell1.picoctf.com:32205
Solusi: Dari soalnya sendiri sudah memberi hint bahwa hanya user agent ’picobrowser’ yang akan memberi flagnya.
curl -s -H ”User-Agent: picobrowser” https://2019shell1.picoctf.com/problem/32205/flag — grep -oE ”picoCTF{.*}”

3. like1000(250 points)

Soal: This .tar file got tarred alot.
Solusi: Ketika kita mendownload file yang diberikan, akan didapati file berekstensi tar bernama 1000.tar
Ketika kita mengekstrak 1000.tar, akan didapati 999.tar. Maka hal ini akan sangat mudah apabila menggunakan script.

Gambar 1: Script yang digunakan

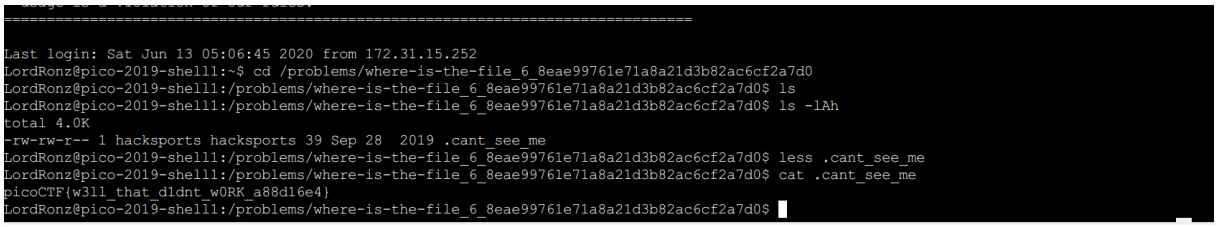
Ketika sudah mencapai 1.tar, ketika diekstrak akan muncul file png bernama flag.png

picoCTF{l0t5_0f_TAR5}

Gambar 2: Flagnyaa

4. where-is-the-file(200 points)

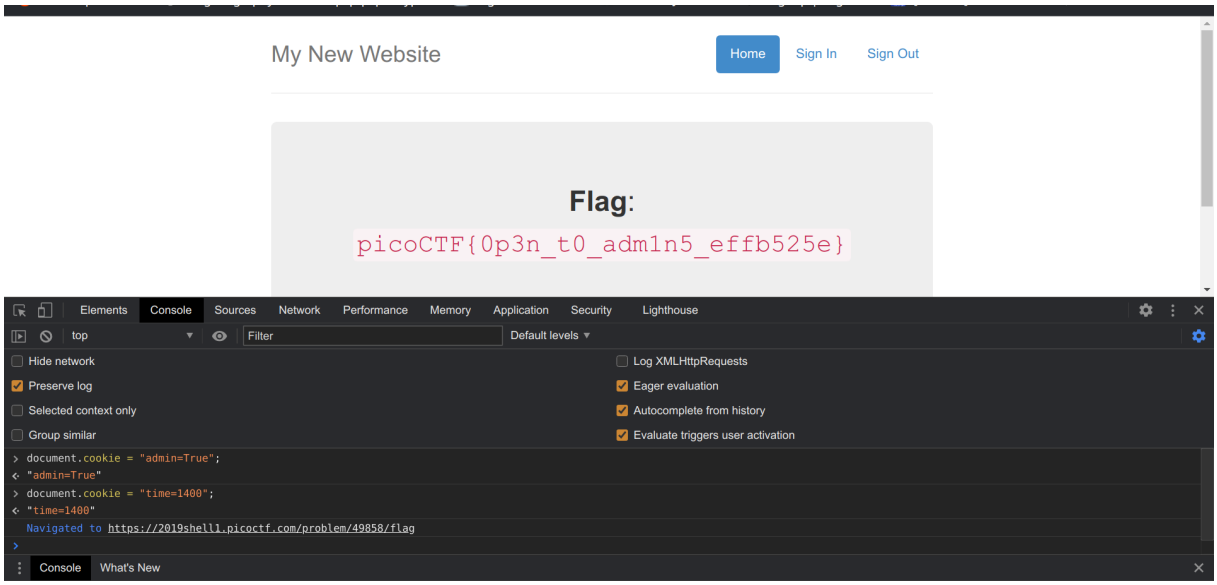
Soal: I've used a super secret mind trick to hide this file. Maybe something lies in /problems/where-is-the-file_6_8eae99761e71a8a21d3b82ac6cf2a7d0. Solusi: Login ke shell picoCTF, lalu cd ke direktori yang ada di soal Mudah sebenarnya, tinggal ls -a lalu cat saja



Gambar 3: Flagnyaa

5. open-to-admins(200 points)

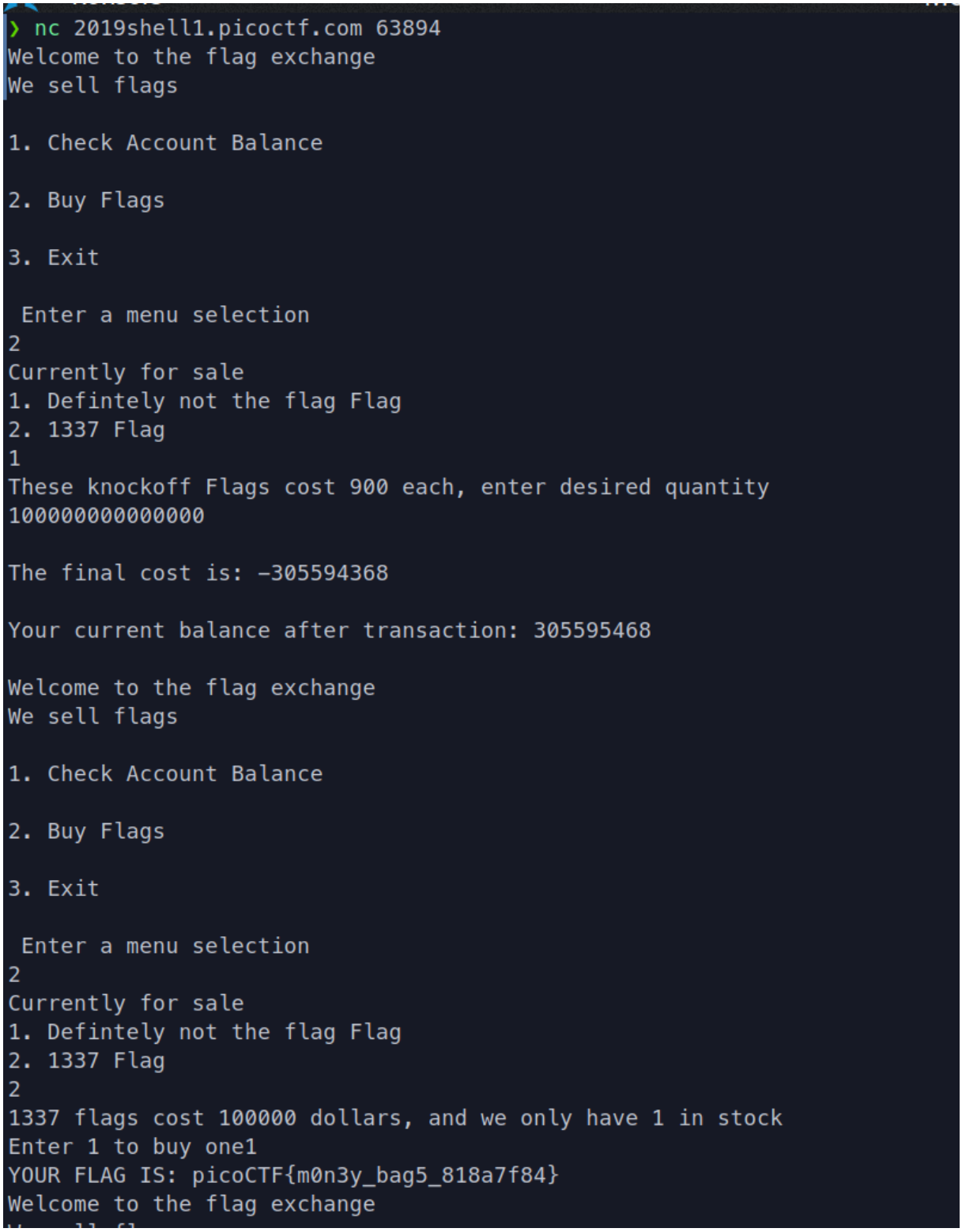
Soal: This secure website allows users to access the flag only if they are admin and if the time is exactly 1400.
https:2019shell1.picoctf.comproblem49858 (link) or http:2019shell1.picoctf.com:49858 Solusi: Dari soalnya dan hintnya bisa disimpulkan bahwa akan ada manipulasi cookie disini. Kita dapat mengganti cookie dengan console dan memberi value cookie ke variable document.cookie



Gambar 4: Flagnyaa

6. flag_shop(300 points)

Soal: There's a flag shop selling stuff, can you buy a flag? Source. Connect with nc 2019shell1.picoctf.com 63894. Solusi: sebenarnya ini merupakan soal yang cukup mudah, karena kita diberi source codenya. Tipe int pada C maksimal menampung 2 pangkat 32 sehingga jika overflow maka nilainya akan minus.



Gambar 5: Flagnyaa