Summer Sundae CTF 2023 Walkthrough

Ashley Bilbrey

13 Feb 2024

CYBER SECURITY CLUB AT UC DAVIS

What was it?

Summer Sundae CTF was a competition for beginners I hosted in 2023.

Challenges were released almost every Sunday for the summer.

- 12 Challenges
- 4 Challenge Authors
- 111 Participants
- 209 Solves
- 413 Submissions

CYBER SECURITY CLUB AT UC DAVIS

Today's Goals

Today I hope you get some more experience with:

- Common Linux commands
- Installing packages
- EXIF Data
- Compressed folders
- Find command
- Understanding binary program files
- Docker

Challenge Walkthroughs

All original challenges listed at
https://github.com/AshleyBilbrey/sundae-2023

```
$ git clone https://github.com/AshleyBilbrey/sundae-2023.git
```

Challenges were scored dynamically based on number of solves.
Flags are in the format moo{flag}.

Follow along with your favorite Linux distro!

CYBER SECURITY CLUB AT UC DAVIS

Project Reality

Author: Ashley

10 Points

Misc

Description

bW9ve0gzMUwwX1dPUjFEfQ==

Project Reality Solution

bW9ve0gzMUwwX1dPUjFEfQ==

What is this?

== <- base64 padding?

```
$ echo “bW9ve0gzMUwwX1dPUjFEfQ==” | base64 -d
moo{H31L0_WOR1D}
```

Miki

Author: Ashley
50 Points
Stego & Forensics (Though basically OSINT techniques..)

Description

Miki is so cute! Please give pets.

Files

miki.jpg

Miki Solution

Isn’t she the cutest! ->
Is something hiding under her fur?

Many images can hold data under the surface called EXIF data.
The most interesting is usually GPS data.

```
$ sudo apt install exiftool
...
$ exiftool miki.jpg
...
Copyright: moo{0MG_CUT3_L04F}
```

Chris' Annoyance

Author: Chris
183 Points
Stego & Forensics

Files

normal.file

Chris' Annoyance Solution

What is this? File extensions are kind of suggestions, so how do we figure out file types in Linux?

```
$ file normal.file
normal.file: POSIX tar archive (GNU)
```

That's useful!

```
$ tar -xf normal.file
$ cd ./normal.txt
```

Chris' Annoyance Solution

```
normal.txt$ ls
a b c d e f g h i j k l m n o p q r s t u v w x y z
```

Ugh.... Let's use find. Good skill to know!

```
normal.txt$ find .
...
./h/hello_world
...
```

That one looks interesting!

Chris' Annoyance Solution

```
normal.txt$ cd ./h
normal.txt/h$ file hello_world
hello_world: POSIX tar archive (GNU)
```

Oh we know that one!

```
normal.txt/h$ tar -xvf hello_world
gz.gz
normal.txt/h$ gzip -dv gz.gz
gz.gz:   -0.7% -- replaced with gz
```

Chris’ Annoyance Solution

```
normal.txt/h$ file gz
gz: bzip2 compressed data, block size = 900k
normal.txt/h$ bzip2 -dv gz
gz.out: XZ compressed data, checksum CRC64
normal.txt/h$ xz -dv gz.out
gz.out (1/1)
xz: gz.out: Filename has an unknown suffix, skipping
```

Ughhhh...

```
normal.txt/h$ mv gz.out file.xz
```

Chris' Annoyance Solution

```
normal.txt/h$ xz -dv file.xz
normal.txt/h$ file file
file: gzip compressed data, from Unix
normal.txt/h$ mv file file.gz
nomral.txt/h$ gzip -dv file.gz
file.gz:         95.4% -- replaced with file
normal.txt/h$ file file
file: POSIX tar archive (GNU)
normal.txt/h$ tar -xvf file
hm/
hm/hmmmmmmm/
hm/hmmmmmmm/flag.jpg
```

Chris’ Annoyance Solution

```
normal.txt/h$ cd ./hm/hmmmmmmm
normal.txt/h/hm/hmmmmmmm$ file flag.jpg
flag.jpg: Zip archive data
normal.txt/h/hm/hmmmmmmm$ unzip flag.jpg
Archive:  flag.jpg
  inflating: flag.txt
normal.txt/h/hm/hmmmmmmm$ file flag.txt
flag.txt: ASCII text
```

Could it be???

Chris’ Annoyance Solution

```
           *     ,MMM8&&&.            *
                MMMM88&&&&&    .
               MMMM88&&&&&&&
   *           MMM88&&&&&&&&
               MMM88&&&&&&&&
               'MMM88&&&&&&'
                 'MMM8&&&'      *
        |\___/|
        )     (             .              '
       =\     /=
         )===(       *
        /     \
        |     |        moo{1ns3rt_f1@g_h3r3}
       /       \
       \       /
_/\_/\_/\__  _/_/\_/\_/\_/\_/\_/\_/\_/\_/\_
|  |  |  |( (  |  |  |  |  |  |  |  |  |  |
|  |  |  | ) ) |  |  |  |  |  |  |  |  |  |
|  |  |  |(_(  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
```

Thanks Chris!

WarGames (1983)

Author: Chris
183 Points
Stego & Forensics

Description

I may be addicted to awful hacker movies...

Files

WOPR

WarGames (1983) Solution

```
$ ./WOPR
LOGON: hi
IDENTIFICATION NOT RECOGNIZED BY SYSTEM
--CONNECTION TERMINATED--
```

Let’s see if we can take a shortcut...

```
$ strings ./WOPR | grep moo
moo{GL0B41_TH3RM0NUCL3AR_W4R}
```

ez

Sundae Shop 0

Author: Ashley
229 Points
Web

Description

It's hot today! What a wonderful day to stop by Ashley's Sundae Shop. You can order all different kinds of flavors, but the flag flavor is for cool kids only.

Files

Many, see Dockerfile

Sundae Shop 0 Running

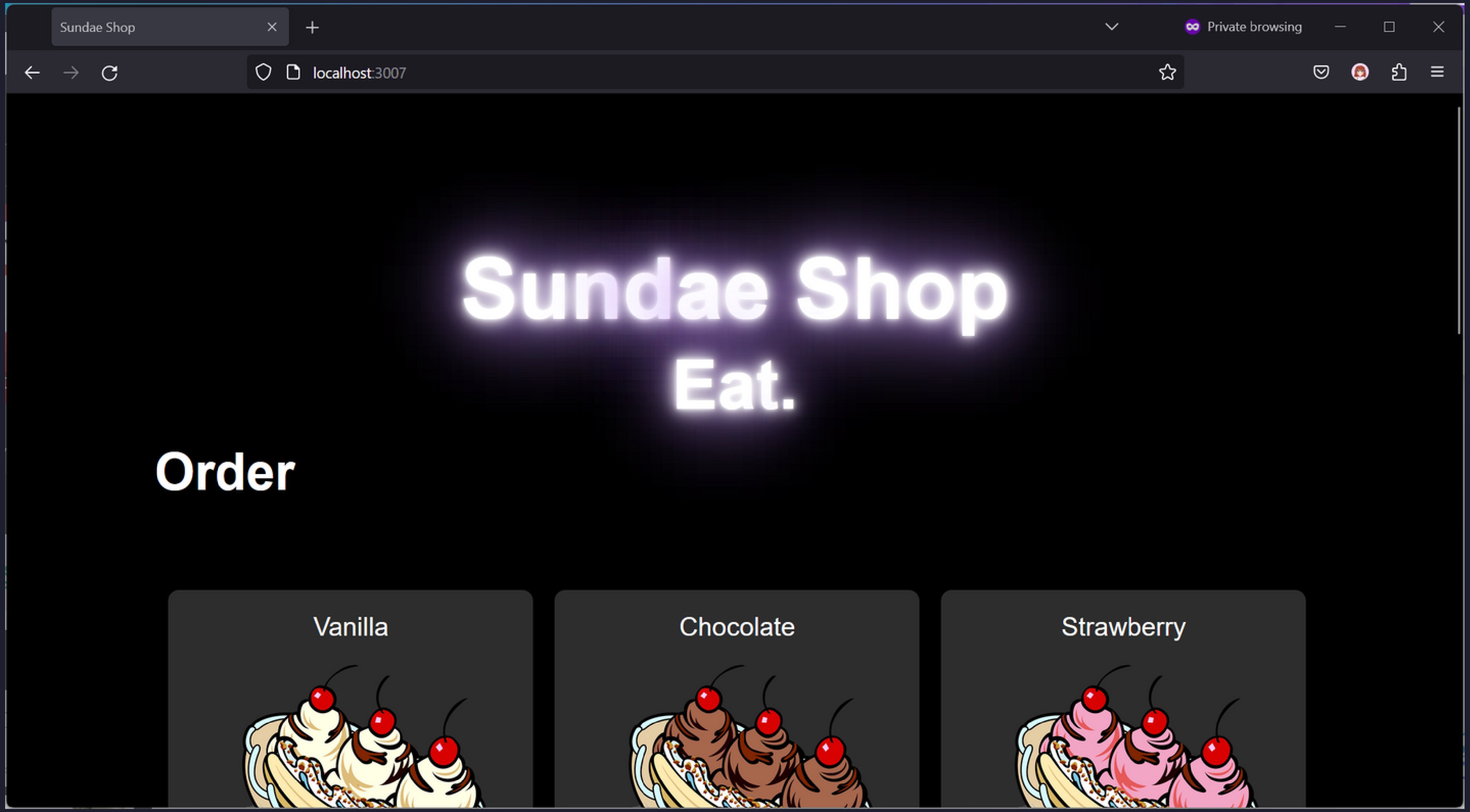
This was hosted during the competition, but today let’s learn how to DIY!

```
$ cat Dockerfile
...
EXPOSE 3007:3007/tcp
$ docker buildx build . -t shop0
...
$ docker run -p 3007:3007 shop0
```

Now we can visit http://localhost:3007.

Sundae Shop 0 Solution

Look at that CSS!



Sundae Shop

Eat.

Order

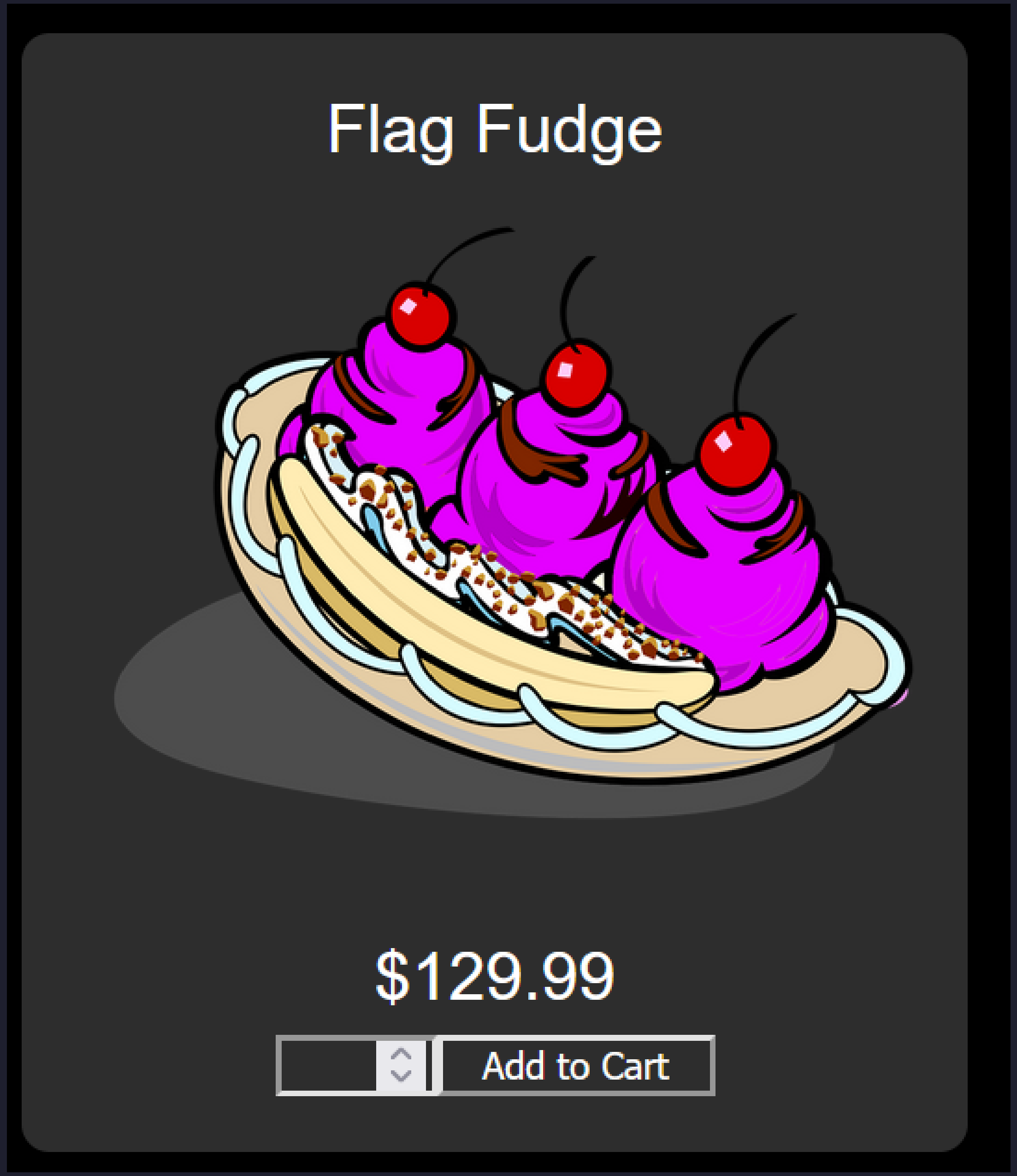
Vanilla

Chocolate

Strawberry

Sundae Shop 0 Solution

Yummy!

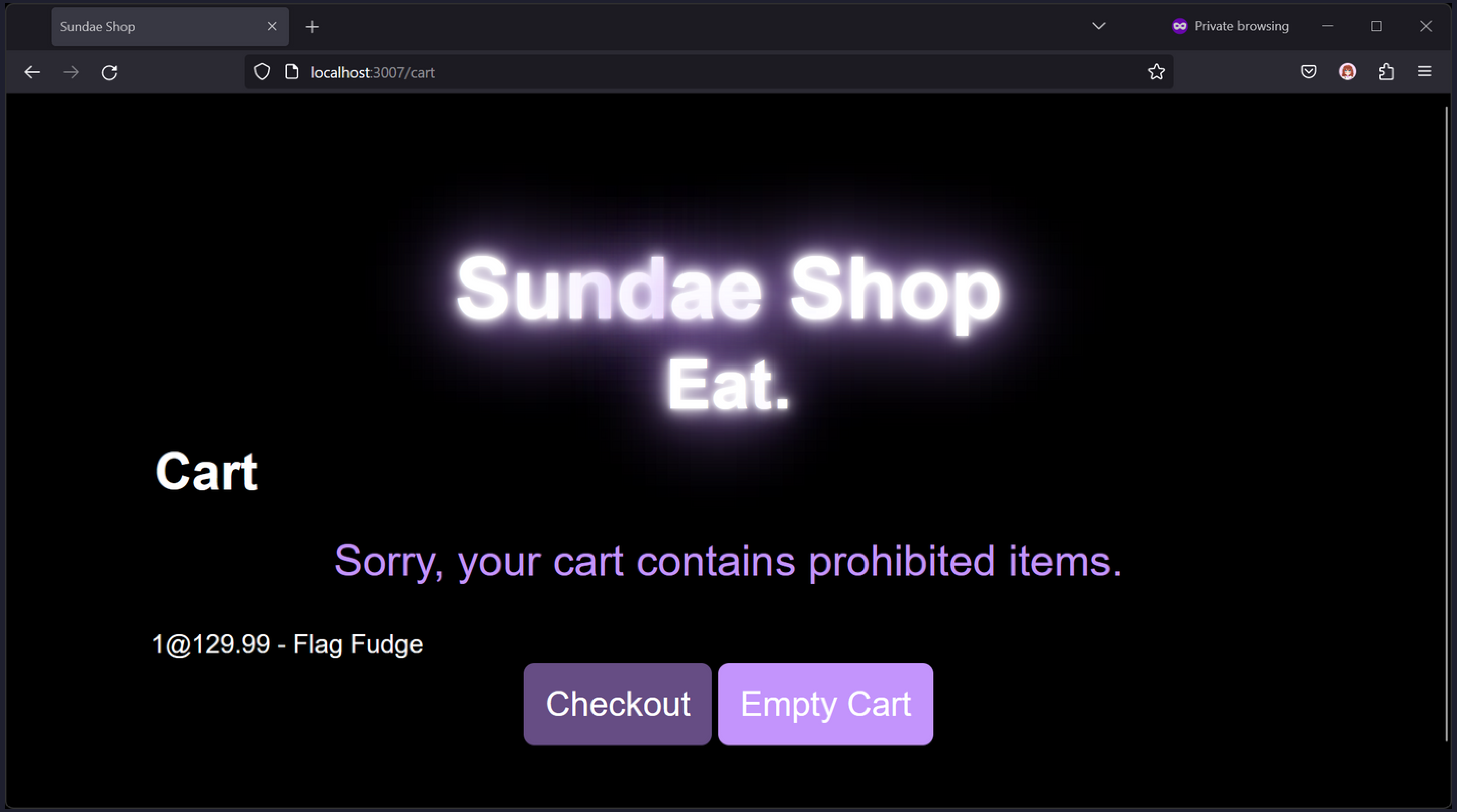


Flag Fudge

$129.99

Sundae Shop 0 Solution

Darn.



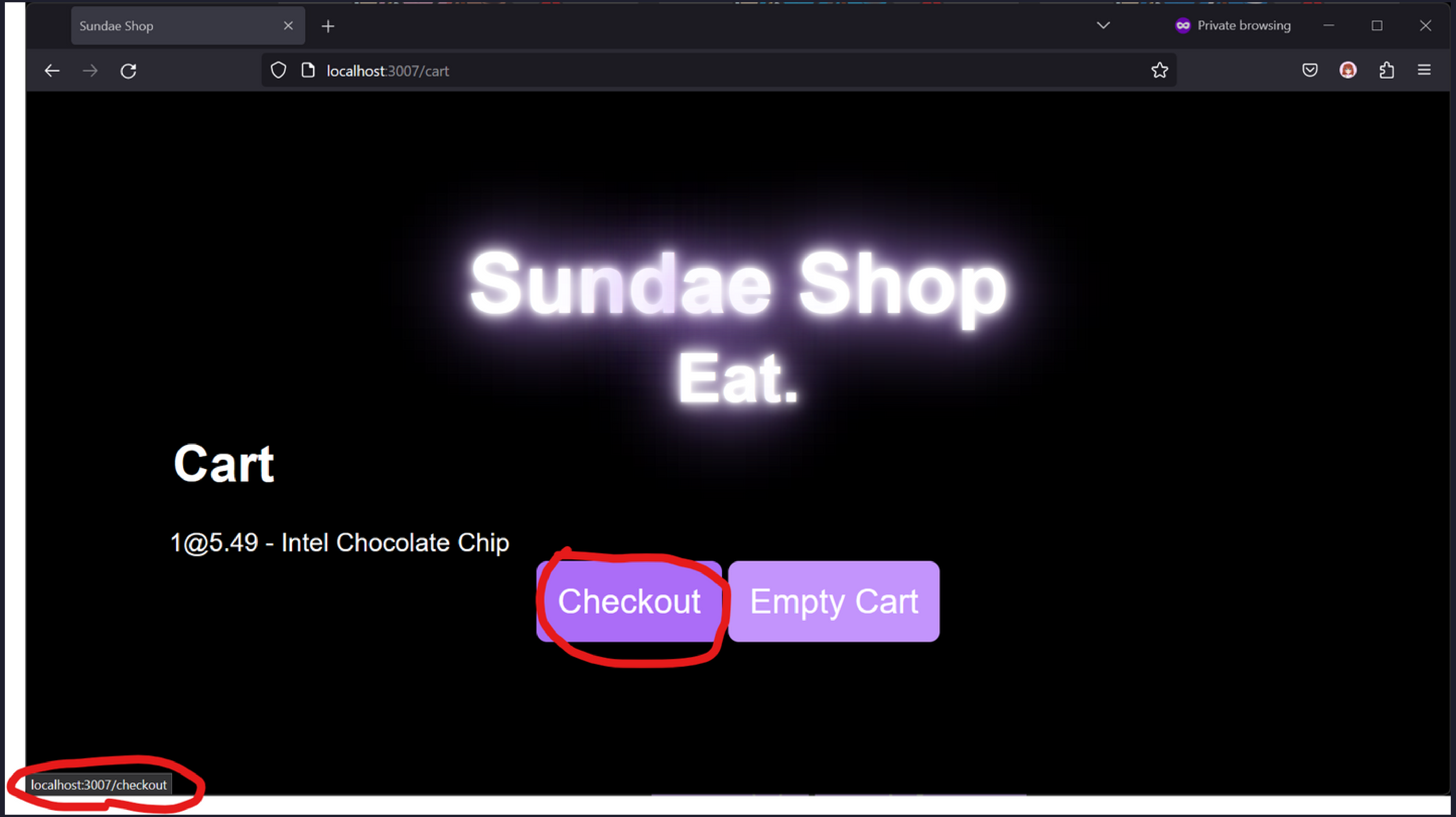
Cart

Sorry, your cart contains prohibited items.

1@129.99 - Flag Fudge

Sundae Shop 0 Solution

Let’s try to order normally. The checkout button goes to /checkout.



Sundae Shop

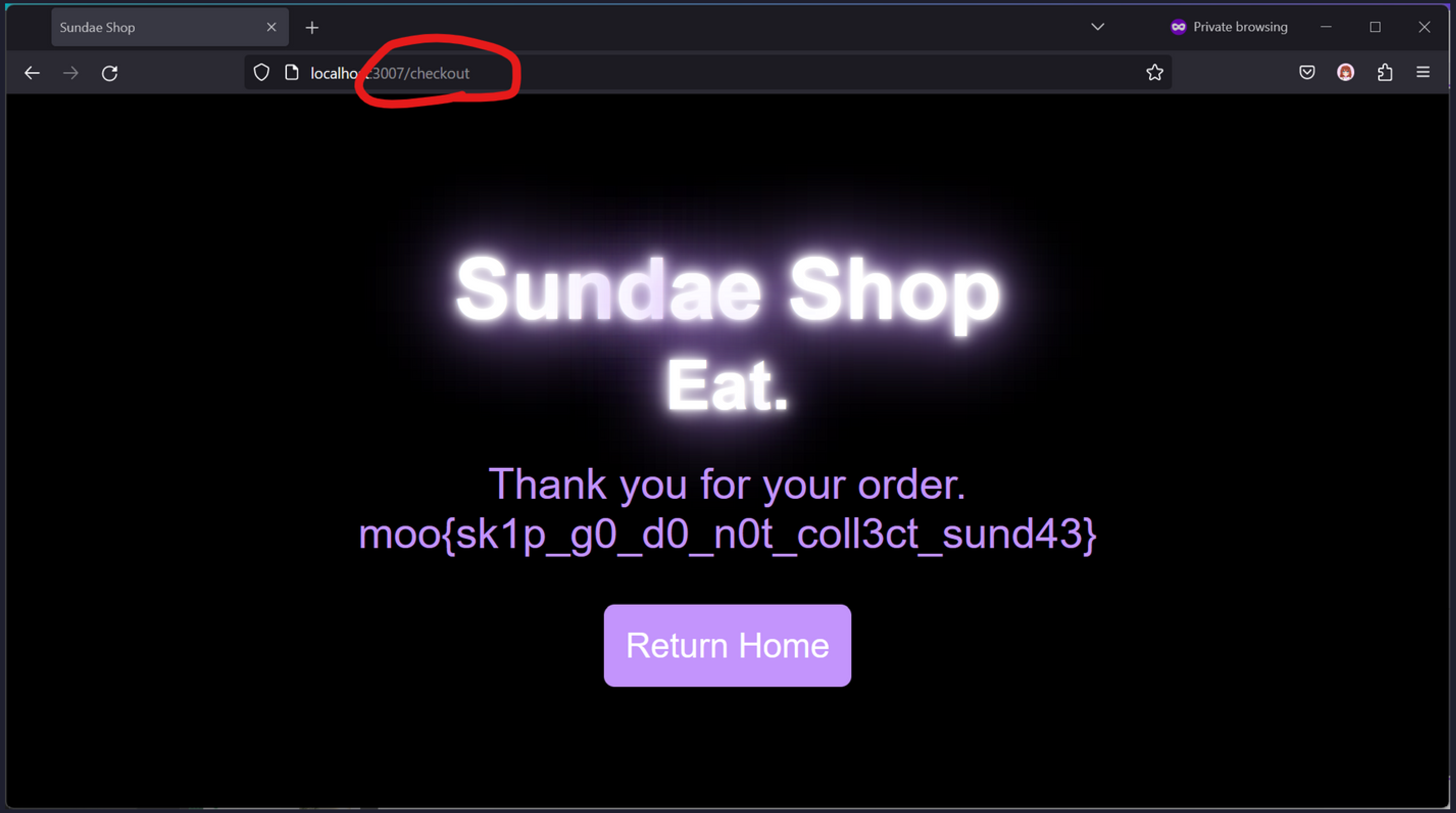
Eat.

Cart

1@5.49 - Intel Chocolate Chip

Sundae Shop 0 Solution

Let’s try to force /checkout with Flag Fudge. Yay!



Sundae Shop

Eat.

Thank you for your order.
moo{sk1p_g0_d0_n0t_coll3ct_sund43}

Thank you.

ashleybilbrey.com