Challenge

Question 1

What is the flag obtained after winning the lottery?

Analysis

Determine Normal Usage

The site is a lottery system that runs every 12 seconds. Every time the lottery is run, the user has $10,000 dollars. 2000 tickets are available for purchase at $5 per ticket.

Web App Exploit Checklist (for NCL but these are good to check in any web app exploit test)

- [ ] Robots.txt
- [ ] Sitemap.xml
- [ ] Cookies
- [X] Javascript code

Javascript

1. Variable box = number of tickets purchased
2. Variable tickets = value of tickets converted to int
3. If session.money >= session.cost*tickets
    - Send post to /purchase
    - Set cost: session.cost*tickets
4. There is more JS but not relevant to beating this

Exploiting

Now we can move onto the real exploit by looking at all the information we have determined.

Information

- We need to increase the odds of winning but can't afford enough tickets
- The post request to purchase tickets shows us how cost taken from the user is calculated

Using the Information

Using Burpsuite, we can use the Proxy to capture the post request to purchase tickets.

In the request, we see the following JSON information:

`{"cost":50,"tickets":10}`

What happens if we change it to `{"cost":1,"tickets":100000}` and forward that request?

Result

A box appears containing the flag.