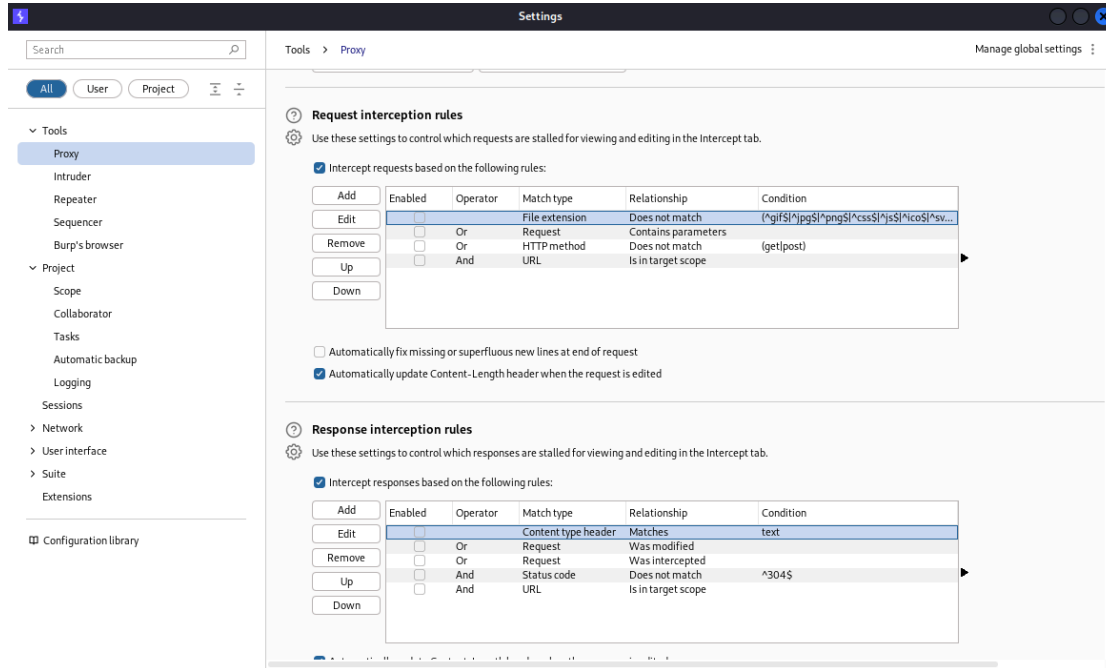
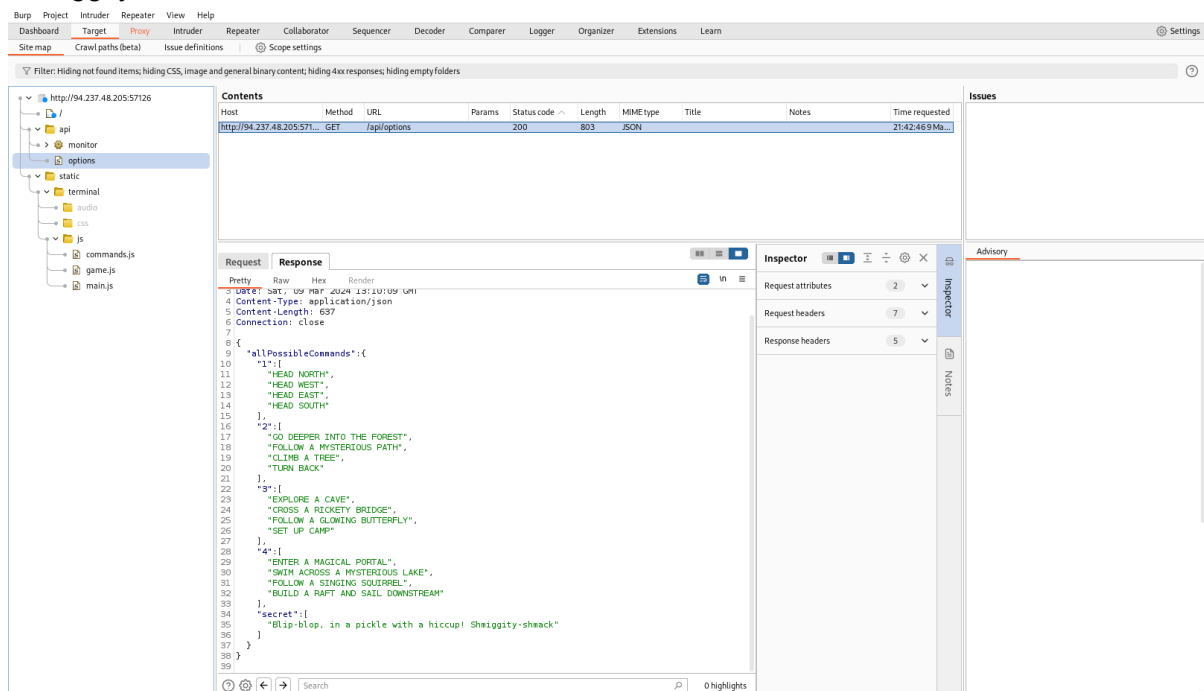


## Main Solution

Set Burp Suite to intercept all requests and responses under proxy settings:



Reload the page and start the game, you would notice that at some point during the loading phase the page makes a GET request to the /api/options, here you can see that there is a secret portion which you just need to set the command to “Blip-blop, in a pickle with a hiccup! Shmiggity-shmack”



Testing this theory, indeed the message returns the flag for this challenge

The screenshot shows the 'Edited request' and 'Response' tabs in a web browser's developer tools. The request is a POST to `/api/monitor` with a JSON body containing a command. The response is a 200 OK with a JSON body containing a message.

**Edited request**

```
1 POST /api/monitor HTTP/1.1
2 Host: 94.237.48.205:57126
3 Content-Length: 68
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/120.0.6099.71 Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://94.237.48.205:57126/
8 Referer: http://94.237.48.205:57126/
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Connection: close
12
13 {
  "command": "Blip-blop, in a pickle with a hiccup! Shwiggity-shmack"
}
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.1 Python/3.11.8
3 Date: Sat, 09 Mar 2024 19:43:21 GMT
4 Content-Type: application/json
5 Content-Length: 67
6 Connection: close
7
8 {
9   "message": "HTB{03v8l0p3r_t00l5_4r3_b3st_wh4t_y0u_Think??}"
10 }
11
```

**Inspector**

Request attributes: 2

Request headers: 10

Response headers: 5

# Rabbit Hole 1:

Under the main.js we can see that it does a check to see if message contains HTB{ or Game Over