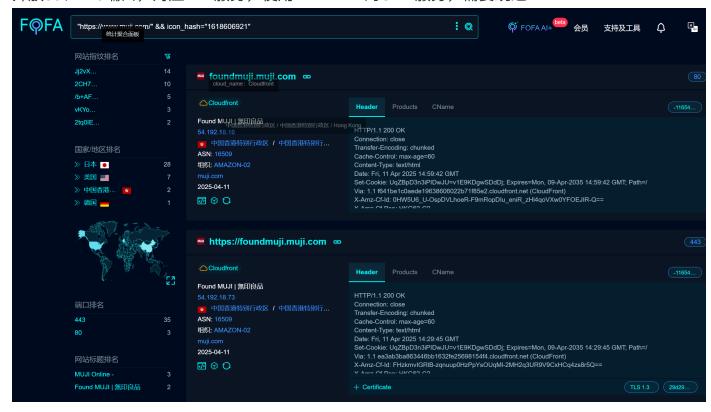
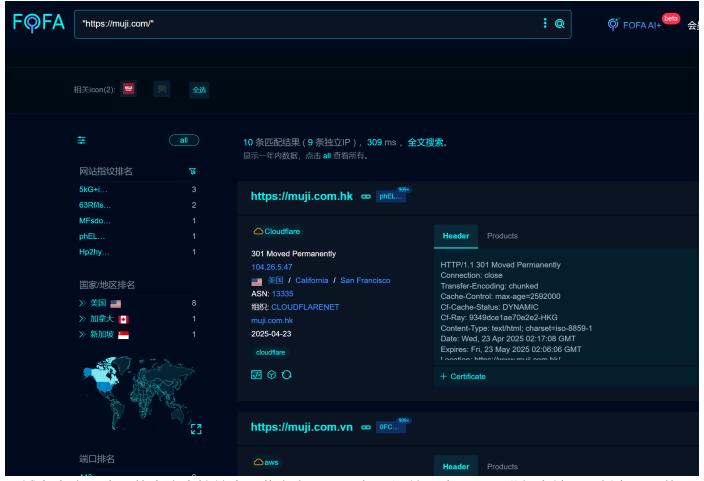
目标网站: https://www.muji.com/hk/

1. FOFA查询

开放80、443端口,对应web服务,使用cloudfront的CDN服务,需要绕过





2. 子域名查询,这里的查询直接给出哪些存在CDN,如果没给,也可以再进行多地ping判定是否使用 CDN

muji.com的子域名列表(14)		
子域名	解析值	归属地 ②
faq.muji.com ⊕ ② ⊖ ⋜	[A] 104.16.207.191 [CNAME] ch-861d8ff8-200d-45b2-85f3-0aae981f1a56.customers.helpfeel.com	美国
stg-support-media-jp.muji.coi ⊕ ೧ ⊖ =		
stg-supply-media-jp.muji.com ⊕ ೧ ⊖ =		
muji.com ⊕ ② ⊖ ⋜	[A] 3.5.156.228	日本东京都东京
localnippon.muji.com ⊕ ② ⊖ =	[A] 18.239.199.128	美国加利福尼亚州旧金山
hotel.muji.com ⊕ ② ⊖ ≥	[A] 13.33.183.83	印度泰米尔纳德邦金奈
www.muji.com CDN ⊕ ① ⊕ 忌	[A] 23.212.62.217 [CNAME] www.muji.com.edgekey.net	美国加利福尼亚州旧金山
tokyo.muji.com ⊕ ② ⊖ ⋜	[A] 13.32.208.6	美国哥伦比亚特区华盛顿
cafemeal.muji.com ⊕ ② ⊖ =	[A] 3.163.125.96 [CNAME] d39oblnz17boex.cloudfront.net	美国乔治亚州亚特兰大
housevision.muji.com ⊕ ② ⊖ 忌		
house.muji.com ⊕ ① ⊕ 忌	[A] 13.33.21.104	美国加利福尼亚州洛杉矶
careers.muji.com ⊕ ② ⊖ 忌	[A] 13.32.121.8 [CNAME] d2paf9xnb6qih2.cloudfront.net	德国巴伐利亚邦纽伦堡
atelier.muji.com ⊕ ② ⊖ ⊰	[A] 13.35.210.13	印度特伦甘纳邦海得拉巴
shop.muji.com	[A] 3.167.212.68	美国华盛顿州西雅图

3. ip反查域名

13.33.183.83解析过的域名 (767)

域名	域名年龄
cloud.nikke-kr.com	4年
www.afrojamznetworks.com	1年
www.socanberra.com.au	
garageportarnykoping.se	1年
www.seattleconcerts2025.com	1年
www.onthetreeplus.co.kr	5年
603.nz	8年
cdn.faleno.net	5年
khanumoory.com	1年
spatialized.link	5年
afoxdesign.co.kr	7年
www.ecogreencamping.com	5年
khanacademy.org	20年
www.slide-stream.com	1年
slide-stream.com	1年
westernchairs.com.au	
www.ck-devops.com	1年
www.simplymayeddy.com	1年

naconstructorasacicom

www.haconstructorasac.com

1年

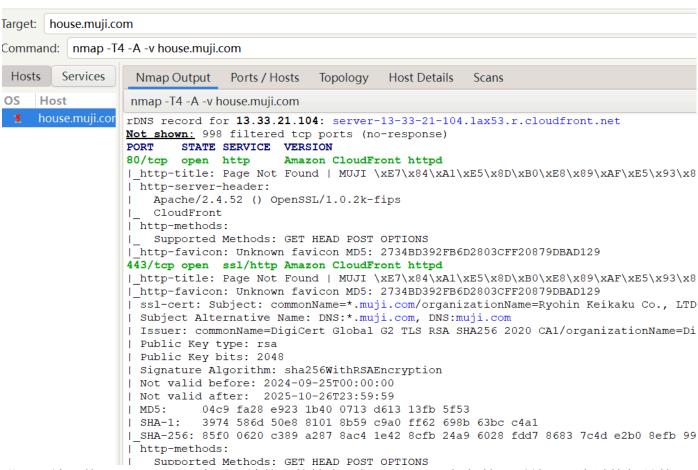
4. whois

muji.com域名信息 2025-03-09 06:48:44

域名	muji.com 2
注册商	1API GmbH 德国
注册商服务器	whois.1api.net
注册商电话	4968949396850
注册商邮箱	abuse@1api.net
更新时间	2024年09月20日
注册时间	1997年06月13日
过期时间	2025年06月12日(29天后到期)
域名年龄	28年
DNS	ns-1405.awsdns-47.org
	ns-1591.awsdns-06.co.uk
	ns-395.awsdns-49.com
	ns-709.awsdns-24.net
状态	注册商设置禁止转移(clientTransferProhibited)
安全认证	水滴信用 官网认证 章 未启用

5. nmap端口扫描

```
Scan Iools Profile Help
Target: muji.com
Command: nmap -T4 -A -v muji.com
 Hosts
        Services
                   Nmap Output
                                 Ports / Hosts
                                             Topology Host Details
                                                                     Scans
OS
                  nmap -T4 -A -v muji.com
    Host
 muji.com (3.5.)
                  Discovered open port 80/tcp on 3.5.156.74
                  Discovered open port 444/tcp on 3.5.156.74
     house.muji.cor
                  Completed SYN Stealth Scan at 11:56, 7.84s elapsed (1000 total ports)
                  Initiating Service scan at 11:56
                  Scanning 4 services on muji.com (3.5.156.74)
                  Service scan Timing: About 50.00% done; ETC: 12:02 (0:02:44 remaining)
                  Completed Service scan at 11:59, 169.03s elapsed (4 services on 1 host)
                  Initiating OS detection (try #1) against muji.com (3.5.156.74)
                  Retrying OS detection (try #2) against muji.com (3.5.156.74)
                  Initiating Traceroute at 11:59
                  Completed Traceroute at 11:59, 9.09s elapsed
                  Initiating Parallel DNS resolution of 2 hosts. at 11:59
                  Completed Parallel DNS resolution of 2 hosts. at 11:59, 0.51s elapsed
                  NSE: Script scanning 3.5.156.74.
                  Initiating NSE at 11:59
                  Completed NSE at 12:01, 82.52s elapsed
                  Initiating NSE at 12:01
                  Completed NSE at 12:01, 40.98s elapsed
                  Initiating NSE at 12:01
                  Completed NSE at 12:01, 0.00s elapsed
                  Nmap scan report for muji.com (3.5.156.74)
                  Host is up (0.092s latency).
                  Other addresses for muji.com (not scanned): 3.5.158.111 52.219.136.128 3
                  rDNS record for 3.5.156.74: s3-website.ap-northeast-1.amazonaws.com
                  Not shown: 996 filtered tcp ports (no-response)
                  PORT STATE SERVICE
                                             VERSION
                  80/tcp
                          open http
                                             Amazon S3 httpd
                  | http-methods:
                  | Supported Methods: GET HEAD
                  | http-server-header: AmazonS3
                  | http-title: Did not follow redirect to http://www.muji.com/
                  443/tcp open https?
                  444/tcp open snpp?
                  8080/tcp open http-proxy?
                  Warning: OSScan results may be unreliable because we could not find at 1
                  OS fingerprint not ideal because: Missing a closed TCP port so results i
                  No OS matches for host
                  Network Distance: 25 hops
                  TCP Sequence Prediction: Difficulty=241 (Good luck!)
                  IP ID Sequence Generation: All zeros
                 TRACEROUTE (using port 443/tcp)
```



6. 进入网站,使用Wappalyzer查看网站使用的技术,如Nginx、JS框架等,后续可以尝试找相关的已 披露漏洞进行利用

