

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

FOFA

"https://www.muji.com/" && icon\_hash="1618606921"

统计聚合面板

网站指纹排名

Jj2vX...

2CH7...

/b+AF...

vKYe...

2lq0IE...

14

10

5

3

2

国家/地区排名

>> 日本

>> 美国

>> 中国香港...

>> 德国

28

7

2

1

端口排名

443

80

35

3

网站标题排名

MUJI Online -

Found MUJI | 無印良品

3

2

foundmuji.muji.com

cloud\_name: Cloudfront

Cloudfront

Header

Products

CName

Found MUJI | 無印良品

54.192.18.16

中国香港特别行政区 / 中国香港特别行...

ASN: 16509

组织: AMAZON-02

muji.com

2025-04-11

HTTP/1.1 200 OK

Connection: close

Transfer-Encoding: chunked

Cache-Control: max-age=60

Content-Type: text/html

Date: Fri, 11 Apr 2025 14:59:42 GMT

Set-Cookie: UqZBpD3n3PIDwJU=v1E9KDgwSDdDj; Expires=Mon, 09-Apr-2035 14:59:42 GMT; Path=

Via: 1.1 f641be1cd0aede19638606022b71f85e2.cloudfront.net (CloudFront)

X-Amz-CF-Id: 0HW5U6\_U-OspDVLhoeR-F9mRopDlu\_eniR\_zHl4qoVXw0YFOEJIR-Q==

https://foundmuji.muji.com

Cloudfront

Header

Products

CName

Found MUJI | 無印良品

54.192.18.73

中国香港特别行政区 / 中国香港特别行...

ASN: 16509

组织: AMAZON-02

muji.com

2025-04-11

HTTP/1.1 200 OK

Connection: close

Transfer-Encoding: chunked

Cache-Control: max-age=60

Content-Type: text/html

Date: Fri, 11 Apr 2025 14:29:45 GMT

Set-Cookie: UqZBpD3n3PIDwJU=v1E9KDgwSDdDj; Expires=Mon, 09-Apr-2035 14:29:45 GMT; Path=

Via: 1.1 ea3ab3ba863446bb1632fe25698154f4.cloudfront.net (CloudFront)

X-Amz-CF-Id: FHzkmvIGRIB-zqnuup0HzPpYsOUqMI-2MH2q3UR9V9CxHCq4zs8r5Q==



+ Certificate

TLS 1.3

29d29...

FOFA "https://muji.com/"

FOFA AI+ beta




相关icon(2):   全选

10 条匹配结果 ( 9 条独立IP ), 309 ms, 全文搜索。  
显示一年内数据, 点击 all 查看所有。

网站指纹排名

5kG+i...	3
63Rf/l...	2
MFsdo...	1
phEL...	1
Hp2hy...	1

国家/地区排名

>> 美国 	8
>> 加拿大 	1
>> 新加坡 	1

端口排名

301 Moved Permanently

104.26.5.47

美国 / California / San Francisco

ASN: 13335

组织: CLOUDFLARENET

muji.com.hk

2025-04-23

cloudflare

Header Products

HTTP/1.1 301 Moved Permanently  
Connection: close  
Transfer-Encoding: chunked  
Cache-Control: max-age=2592000  
Cf-Cache-Status: DYNAMIC  
Cf-Ray: 9349dce1ae70e2e2-HKG  
Content-Type: text/html; charset=iso-8859-1  
Date: Wed, 23 Apr 2025 02:17:08 GMT  
Expires: Fri, 23 May 2025 02:06:06 GMT  
Location: https://www.muji.com.hk/

+ Certificate

























































https://muji.com.vn

aws

Header Products

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
faq.muji.com    	[A] 104.16.207.191 [CNAME] ch-861d8ff8-200d-45b2-85f3-0aae981f1a56.customers.helpfeel.com	美国
stg-support-media-jp.muji.com    	--	--
stg-supply-media-jp.muji.com    	--	--
muji.com    	[A] 3.5.156.228	日本东京都东京
localnippon.muji.com    	[A] 18.239.199.128	美国加利福尼亚州旧金山
hotel.muji.com    	[A] 13.33.183.83	印度泰米尔纳德邦金奈
www.muji.com <span>CDN</span>    	[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    	[A] 13.32.208.6	美国哥伦比亚特区华盛顿
cafemeal.muji.com    	[A] 3.163.125.96 [CNAME] d39oblz17boex.cloudfront.net	美国乔治亚州亚特兰大
housevision.muji.com    	--	--
house.muji.com    	[A] 13.33.21.104	美国加利福尼亚州洛杉矶
careers.muji.com    	[A] 13.32.121.8 [CNAME] d2paf9xnb6qih2.cloudfront.net	德国巴伐利亚邦纽伦堡
atelier.muji.com    	[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
baconstructorasac.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	<div><div> 水滴信用</div><div> 官网认证</div><div> 未启用</div></div>

5. nmap端口扫描

ScanToolsProfileHelp

Target: muji.com

Command: nmap -T4 -A -v muji.com

HostsServices

OS	Host
	muji.com (3.5.156.74)
	house.muji.com

Nmap OutputPorts / HostsTopologyHost DetailsScans

nmap -T4 -A -v muji.com

Discovered open port 80/tcp on 3.5.156.74  
Discovered open port 444/tcp on 3.5.156.74  
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)

Target: house.muji.com

Command: nmap -T4 -A -v house.muji.com

Hosts Services

OS Host

house.muji.com

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v house.muji.com

rDNS record for 13.33.21.104: server-13-33-21-104.lax53.r.cloudfront.net

**Not shown:** 998 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Amazon CloudFront httpd

|\_ http-title: Page Not Found | MUJI \xE7\x84\xA1\xE5\x8D\xB0\xE8\x89\xAF\xE5\x93\x8

|\_ http-server-header:

|\_ Apache/2.4.52 () OpenSSL/1.0.2k-fips

|\_ CloudFront

|\_ http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

|\_ http-favicon: Unknown favicon MD5: 2734BD392FB6D2803CFF20879DBAD129

443/tcp	open	ssl/http	Amazon CloudFront httpd
---------	------	----------	-------------------------

|\_ http-title: Page Not Found | MUJI \xE7\x84\xA1\xE5\x8D\xB0\xE8\x89\xAF\xE5\x93\x8

|\_ http-favicon: Unknown favicon MD5: 2734BD392FB6D2803CFF20879DBAD129

|\_ ssl-cert: Subject: commonName=\*.muji.com/organizationName=Ryohin Keikaku Co., LTD

|\_ Subject Alternative Name: DNS:\*.muji.com, DNS:muji.com

|\_ Issuer: commonName=DigiCert Global G2 TLS RSA SHA256 2020 CA1/organizationName=Di

|\_ Public Key type: rsa

|\_ Public Key bits: 2048

|\_ Signature Algorithm: sha256WithRSAEncryption

|\_ Not valid before: 2024-09-25T00:00:00

|\_ Not valid after: 2025-10-26T23:59:59

|\_ MD5: 04c9 fa28 e923 1b40 0713 d613 13fb 5f53

|\_ SHA-1: 3974 586d 50e8 8101 8b59 c9a0 ff62 698b 63bc c4a1

|\_ SHA-256: 85f0 0620 c389 a287 8ac4 1e42 8cfb 24a9 6028 fdd7 8683 7c4d e2b0 8efb 99

|\_ http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

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

muji.com/jp/a/shop

DOCKER Hub Conta... ddd\flag - 博客园 ChatGPT Gemini claude123 (接通... DeepSeek - 探索未... 哔哩哔哩 (゜-゜)つ... GitHub

MUJI 無印良品 婦人服 紳士服 こども服 生活雑貨 家具・収納・家電 食品

店舗を探す

キーワードで探す

店名、住所

検索

近隣店舗を探す

都道府県から探す

サービスから探す

取り扱い商品から探す

千鳥ヶ淵公園 皇居 大手町 日本橋三越本店 日本橋 茅場町

Google Analytics GA4

Facebook Pixel 2.9.201

安全

Akamai Bot Manager

HSTS

JavaScript 庫

JsObservable

JsViews

字体脚本

Google Font API

lit-html 3.2.1

lit-element 4.1.1

杂项

Open Graph

ServiceNow

Web 服务器

Nginx

Adobe DTM

Adobe Experience Platform Launch

Google Tag Manager

JsRender 1.0.6

core-js 3.32.2

Modernizr 2.7.1

jQuery 1.11.0

foundmuji.muji.com

EventProductColumnOnline Store

FoundMUJI

Wappalyzer

TECHNOLOGIESMORE INFOExport

分析

Adobe Analytics

Google AnalyticsGA4

Facebook Pixel2.9.201

Google Ads Conversion Tracking

JavaScript 框架

Emotion

Astro

安全

Akamai Bot Manager

标签管理器

Adobe Experience Platform Launch

Google Tag Manager

开发

Emotion

静态站点生成器

Astro

JavaScript 库

Swiper

core-js2.6.11