69

/100

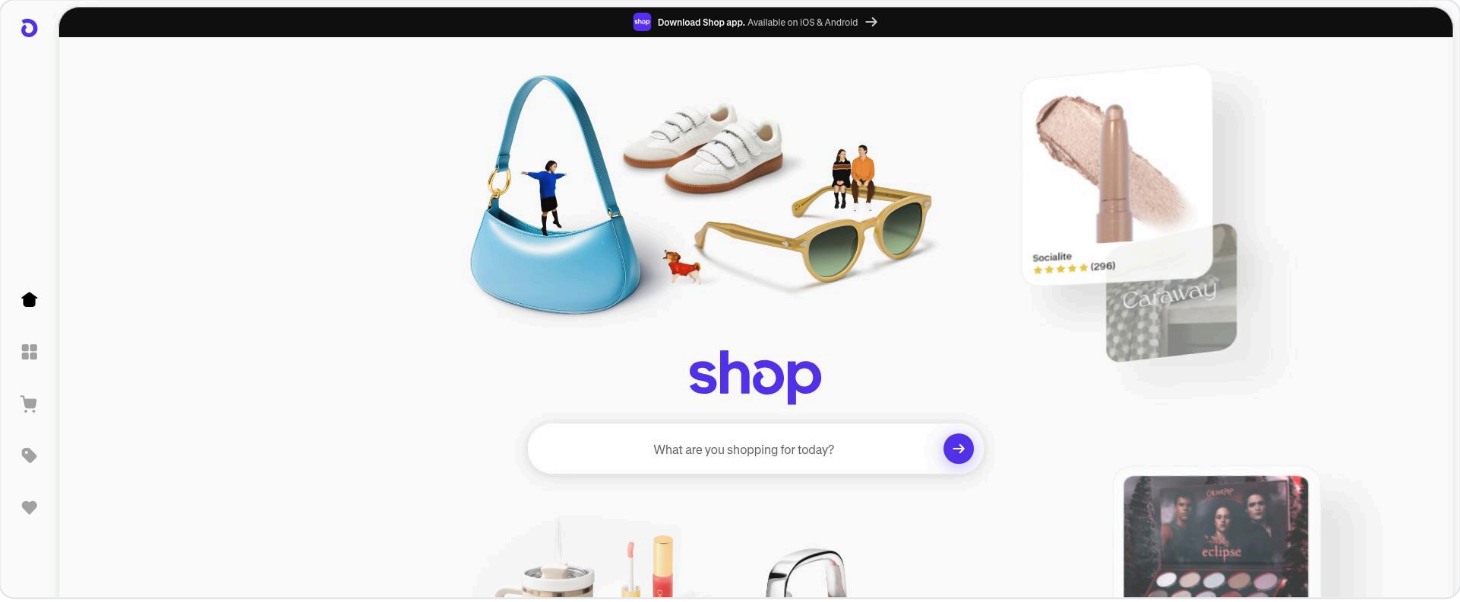
https://shop.app/

SUSPICIOUS

AI: 25/100 · MEDIUM RISK

Resolved IP: 185.146.173.20 · Server: cloudflare

MALWARE	SAFE BROWSING	SSL	DOMAIN AGE
Clean	Clean	Valid	Unknown


Download Shop app. Available on iOS & Android
shop
What are you shopping for today?
Socialite
(296)
Caraway
eclipse

Desktop view — shop.app

THREAT DETECTION

URLhaus	CLEAN
Google Safe Browsing	CLEAN
Spamhaus	NOT LISTED
SURBL	NOT LISTED
Checked IP	185.146.173.20

SSL CERTIFICATE

Status	VALID
Protocol	TLSv1.3
Cipher Suite	TLS_AES_256_GCM_SHA384
Subject	shop.app
Issuer	WE1 (Google Trust Services)
Valid From	Mar 8 13:22:11 2026 GMT
Expires	Jun 6 14:22:04 2026 GMT (79 days remaining)
HSTS	Enabled max-age=15552000; includeSubDomains; preload
OCSP	unknown
Key	ECDSA prime256v1 256 bits
Serial Number	36EEC416EC0C23CD0D7DD8C9B59C1D01
SANs	shop.app

HTTP SECURITY HEADERS

Status: **200 OK** · Final URL: `https://shop.app/`

HEADER	STATUS	VALUE
HSTS	present	`max-age=15552000; includeSubDomains; preload`
X-Content-Type-Options	present	`nosniff`
X-Frame-Options	missing	—
CSP	present	`default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval' blob: cdnjs.cloudflare.com https://*.googleapis.com https://www.gstatic.com https://unpkg.com https://cdn.shopifycloud.com https://cdn.shopify.com https://shopify-assets.shopifycdn.com https://sessions.bugsnag.com https://notify.bugsnag.com https://monorail-edge.shopifysvc.com https://www.google-analytics.com https://stats.g.doubleclick.net https://atlas.shopifysvc.com https://hcaptcha.com https://*.hcaptcha.com https://connect.facebook.net https://www.googletagmanager.com https://googleads.g.doubleclick.net https://checkout.pci.shopifyinc.com https://www.googleadservices.com https://www.google.com/recaptcha/ https://recaptcha.google.com/recaptcha/ https://www.youtube.com ; style-src 'self' 'unsafe-inline' blob: cdn.shopify.com shopify-assets.shopifycdn.com sdks.shopifycdn.com https://cdn.shopify.com https://shopify-assets.shopifycdn.com https://cdn.shopifycloud.com https://hcaptcha.com https://*.hcaptcha.com https://*.googleapis.com; media-src 'self' blob: data: cdn.shopify.com shopify-assets.shopifycdn.com proxy.shopifycdn.com; img-src 'self' data: blob: https: cdn.shopify.com shopify-assets.shopifycdn.com proxy.shopifycdn.com sdks.shopifycdn.com shopify-arrive.s3.amazonaws.com storage.googleapis.com v.shopify.com; child-src blob: merchant-feedback.shopify.com; worker-src 'self' blob:; font-src 'self' https: data: https://cdn.shopify.com https://shopify-assets.shopifycdn.com https://cdn.shopifycloud.com; connect-src 'self' wss: wss://web-shop-client.shop.dev https: https://cdn.shopify.com https://shopify-assets.shopifycdn.com data:; object-src 'none'; upgrade-insecure-requests; frame-ancestors 'none'; frame-src 'self' https://www.google.com/recaptcha https://recaptcha.google.com/recaptcha https://www.googletagmanager.com https://td.doubleclick.net https://shop.app https://www.youtube.com https://app.datadoghq.com https://lookerstudio.google.com/ https://js.stripe.com https://hooks.stripe.com https://www.sandbox.paypal.com https://www.paypal.com https://t.paypal.com https://www.paypalobjects.com https://c.paypal.com https://uri.paypal.com https://centinelapi.cardinalcommerce.com https://*.shopifycs.com https://*.shopifyinc.com https://*.pci.shopifyinc.com https://pay.shopify.com https://checkout.pci.shopifyinc.com/ https://www.affirm.com https://api.global.sandbox.affirm.com https://uk.affirm.com https://sandbox.uk.affirm.com https://cdn1-sandbox.affirm.com https://www.google.com https://recaptcha.google.com https://hcaptcha.com https://*.hcaptcha.com https://*.myshopify.com https://checkout.shopify.com ; report-uri /csp-report?source%5Bapp%5D=shop_client_web; report-to shopify-csp`
Referrer-Policy	missing	—

HEADER	STATUS	VALUE
Permissions-Policy	missing	–
COOP	missing	–
COEP	missing	–
CORP	missing	–
X-XSS-Protection	missing	–

DNS RECORDS

22 records

Type	Name	Value	TTL
A	shop.app	185.146.173.20	20
AAAA	shop.app	2620:127:f00f:ff00::	38
MX	shop.app	aspmx.l.google.com	0
MX	shop.app	alt3.aspmx.l.google.com	0
MX	shop.app	alt4.aspmx.l.google.com	0
MX	shop.app	alt1.aspmx.l.google.com	0
MX	shop.app	alt2.aspmx.l.google.com	0
NS	shop.app	blue.foundationdns.com	0
NS	shop.app	blue.foundationdns.net	0
NS	shop.app	blue.foundationdns.org	0
TXT	shop.app	google-site-verification=LRLUGRDXKD09LLfSBqOn_4rynB1eV21cVUpEPv6h-MA	0
TXT	shop.app	google-site-verification=aGEGmddfRqtcab3XHZhCiFS1IyIO3o_kA_T0RdJ1aDY	0
TXT	shop.app	have-i-been-pwned-verification=89fa3bbb54579507c8eba5137da8108e	0
TXT	shop.app	MS=ms16944936	0
TXT	shop.app	google-site-verification=TAA04FEZVfcZMw4EzB5obR2c9gjXESaMiHF2MdGi5WM	0
TXT	shop.app	pinterest-site-verification=ca3929090beef9bac92b4d3cd51f17db	0
TXT	shop.app	mailru-verification: 3d23e6e7961b42c0	0
TXT	shop.app	v=spf1 include:mail.zendesk.com ~all	0
TXT	shop.app	google-site-verification=XK6a65ejYM4x4_qShAHs3_AP1rQL6zLvdEW7VrijgUA	0
TXT	shop.app	google-site-verification=Vc7VeMMI1glUzyT5QQagcxJc9KtkcMDf6NUFqjEE4qA	0
TXT	shop.app	yahoo-verification-key=it0A6wDiskchiCoBuBG5aU7TQzmpKcLAMGkfxFzNGf4=	0
SOA	shop.app	blue.foundationdns.com dns.cloudflare.com 2399331507	1800

WHOIS REGISTRATION

Error: getaddrinfo ENOTFOUND whois.nic.google

TECHNOLOGY STACK

TECHNOLOGY	CATEGORY	CONFIDENCE	EVIDENCE
Cloudflare	CDN	high	Header: server: cloudflare

AI SECURITY ANALYSIS

gpt-4.1-nano · two-pass analysis

INTELLIGENCE KNOWLEDGE CHECK

UNKNOWN E-commerce platform Unknown domain

The domain 'shop.app' appears to be a legitimate domain likely associated with an e-commerce or shopping-related service, possibly a branded app storefront. There are no known associations with malicious activity or threat infrastructure based on training data. Its structure and naming pattern are consistent with standard commercial domains.

SCAN EVIDENCE VERDICT

25 /100 MEDIUM RISK

The domain 'shop.app' appears to be an unfamiliar, newly registered domain with no prior reputation or known malicious associations. Real-time scan evidence shows a valid SSL certificate from a reputable issuer, standard security headers, and no redirects, which suggests legitimate intent. However, the lack of comprehensive security headers (e.g., missing X-Frame-Options, Referrer-Policy) and the domain's unknown status introduce some caution, especially given its unfamiliarity and absence from threat blocklists. Overall, the evidence neither confirms malicious activity nor guarantees trustworthiness, warranting a cautious stance.

1. Monitor the domain for any suspicious activity or user reports before fully trusting it.
2. Implement additional security controls if integrating with sensitive systems or handling user data.
3. Perform further reconnaissance, such as checking domain age and registration details when available, to assess legitimacy.
4. Consider blocking or sandboxing access if the domain is encountered in critical environments until more information is obtained.