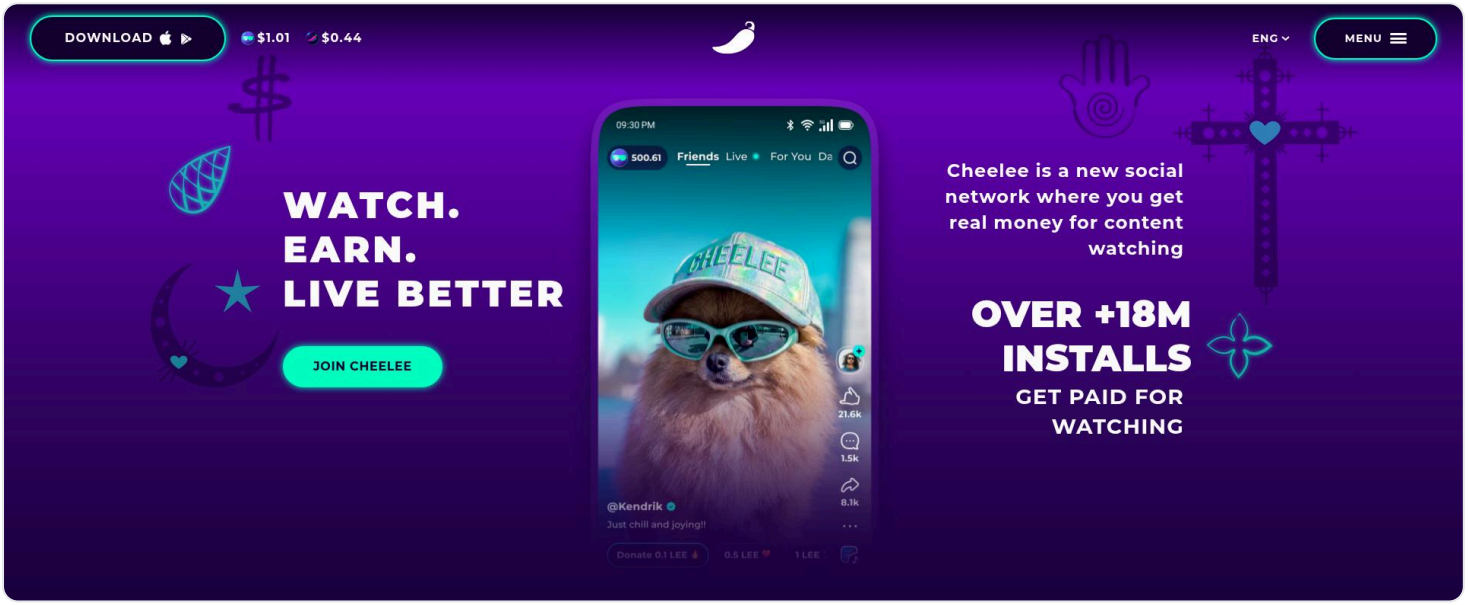
59
/100

## https://cheelee.io/

SUSPICIOUS | AI: 25/100 · MEDIUM RISK

Resolved IP: 104.18.20.229 · Server: cloudflare

| MALWARE | SAFE BROWSING | SSL | DOMAIN AGE |
|---|---|---|---|
| Clean | Clean | Valid | 1316d |




Desktop view — cheelee.io

### THREAT DETECTION

| | |
|---|---|
| URLhaus | CLEAN |
| Google Safe Browsing | CLEAN |
| Spamhaus | NOT LISTED |
| SURBL | NOT LISTED |
| Checked IP | 104.18.20.229 |

## SSL CERTIFICATE

| | |
|---|---|
| Status | VALID |
| Protocol | TLSv1.3 |
| Cipher Suite | TLS_AES_256_GCM_SHA384 |
| Subject | cheelee.io |
| Issuer | WE1 (Google Trust Services) |
| Valid From | Mar 11 18:27:35 2026 GMT |
| Expires | Jun 9 19:27:34 2026 GMT (83 days remaining) |
| HSTS | Not set |
| OCSP | unknown |
| Key | ECDSA prime256v1 256 bits |
| Serial Number | 02AF21F7EE8AC1861158C090CB275888 |
| SANs | cheelee.io |

## HTTP SECURITY HEADERS

Status: **200 OK** · Final URL: https://cheelee.us/

| HEADER | STATUS | VALUE |
|---|---|---|
| HSTS | missing | – |
| X-Content-Type-Options | present | nosniff |
| X-Frame-Options | missing | – |
| CSP | missing | – |
| Referrer-Policy | present | strict-origin-when-cross-origin |
| Permissions-Policy | missing | – |
| COOP | missing | – |
| COEP | missing | – |
| CORP | missing | – |
| X-XSS-Protection | missing | – |

## DNS RECORDS

18 records

| Type | Name | Value | TTL |
|---|---|---|---|
| A | cheelee.io | 104.18.20.229 | 299 |
| A | cheelee.io | 104.18.21.229 | 299 |
| AAAA | cheelee.io | 2606:4700::6812:14e5 | 299 |
| AAAA | cheelee.io | 2606:4700::6812:15e5 | 299 |
| MX | cheelee.io | alt4.aspmx.l.google.com | 0 |
| MX | cheelee.io | alt1.aspmx.l.google.com | 0 |
| MX | cheelee.io | alt2.aspmx.l.google.com | 0 |
| MX | cheelee.io | aspmx.l.google.com | 0 |
| MX | cheelee.io | alt3.aspmx.l.google.com | 0 |
| NS | cheelee.io | kayleigh.ns.cloudflare.com | 0 |
| NS | cheelee.io | henrik.ns.cloudflare.com | 0 |
| TXT | cheelee.io | yandex-verification: 67fd3383d0acb997 | 0 |
| TXT | cheelee.io | google-site-verification=7nUbTP-EZje4vT4KuJKdGzEiHuH5eO1dws1ck1c0avY | 0 |
| TXT | cheelee.io | google-site-verification=jKWecaFBHZWhJKWqI_fCFT5xSD6swvHr6mQg5OSAXog | 0 |
| TXT | cheelee.io | google-site-verification=o3OMHbDQZUXzjWVIuWuBnpJbJzp-XED4POKu-iX-kNY | 0 |
| TXT | cheelee.io | v=spf1 include:mxsspf.sendpulse.com include:_spf.google.com ip4:63.179.28.166 ~all | 0 |
| TXT | cheelee.io | yandex-verification: 006f091371a860d6 | 0 |
| SOA | cheelee.io | henrik.ns.cloudflare.com dns.cloudflare.com 2398494296 | 1800 |

## WHOIS REGISTRATION

| | |
|---|---|
| Registrar | GoDaddy.com, LLC |
| Registrant Org | Domains By Proxy, LLC |
| Registrant Country | US |
| Domain Age | 1316 days |
| Created | 2022-08-10T08:24:05Z |
| Updated | 2025-08-11T16:31:04Z |
| Expires | 2026-08-10T08:24:05Z |
| Nameservers | henrik.ns.cloudflare.com<br>kayleigh.ns.cloudflare.com |

## TECHNOLOGY STACK

| TECHNOLOGY | CATEGORY | CONFIDENCE | EVIDENCE |
|---|---|---|---|
| **Cloudflare** | CDN | high | Header: server: cloudflare |
| **Google Analytics** | Analytics | medium | HTML pattern: googletagmanager\.com |
| **Google Tag Manager** | Tag Manager | medium | HTML pattern: googletagmanager\.com\/gtm\.js |

## AI SECURITY ANALYSIS

gpt-4.1-nano · two-pass analysis

### INTELLIGENCE KNOWLEDGE CHECK

UNKNOWN | Unknown — suspicious pattern | Unknown domain

The domain cheelee.io does not correspond to any major brand, public service, or well-known infrastructure. Its registration via GoDaddy and relatively recent age (around 4 years) do not inherently indicate maliciousness, but the domain name itself does not suggest a trusted or established entity. Without additional context, it appears obscure and potentially suspicious.

⚠ No known association with reputable brands or infrastructure

⚠ Domain name does not match common trusted patterns

⚠ Potential for being used as a dropper or phishing domain due to lack of reputation

### SCAN EVIDENCE VERDICT

**25** /100 MEDIUM RISK

The domain cheelee.io is unfamiliar and lacks a reputable reputation, aligning with prior suspicion. The real-time evidence shows a young domain with a valid SSL certificate but missing critical security headers, and it redirects to cheelee.us, which could be a red flag. The absence of known brand association and the redirect chain increase concern, though no active threats are detected in blocklists. Overall, the evidence confirms moderate suspicion consistent with an obscure, potentially suspicious domain.

1. Monitor traffic to cheelee.io and its redirect cheelee.us for unusual activity or payload delivery.
2. Consider blocking or further analyzing the redirect destination cheelee.us for malicious content.
3. Implement additional security controls such as HSTS and Content Security Policy headers if hosting or interacting with this domain.
4. Conduct a deeper investigation into the redirect chain and associated infrastructure for potential malicious intent.