

pub-e10d56052d2542d0b2f74abed3691951.r2.dev: TrustSniffer

assessment: 50/100

pub-e10d56052d2542d0b2f74abed3691951.r2.dev

Verdict

50

OUT OF 100

MODERATE TRUST

pub-e10d56052d2542d0b2f74abed3691951.r2.dev is moderately trusted.

Most signals looked ordinary, and some evidence was missing. Read the checks below before you pay or hand over personal details.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-10-01 by automated analysis. Classification confidence 55%.

What this site appears to be

A 404/Object not found page indicating the requested object is missing or not publicly accessible. No forms, links, or monetization present.

Evidence status and limitations

Evidence completeness: UNKNOWN

- The real-world operator identity was not independently verified.
- Module-level completeness metadata is unavailable for this legacy report.

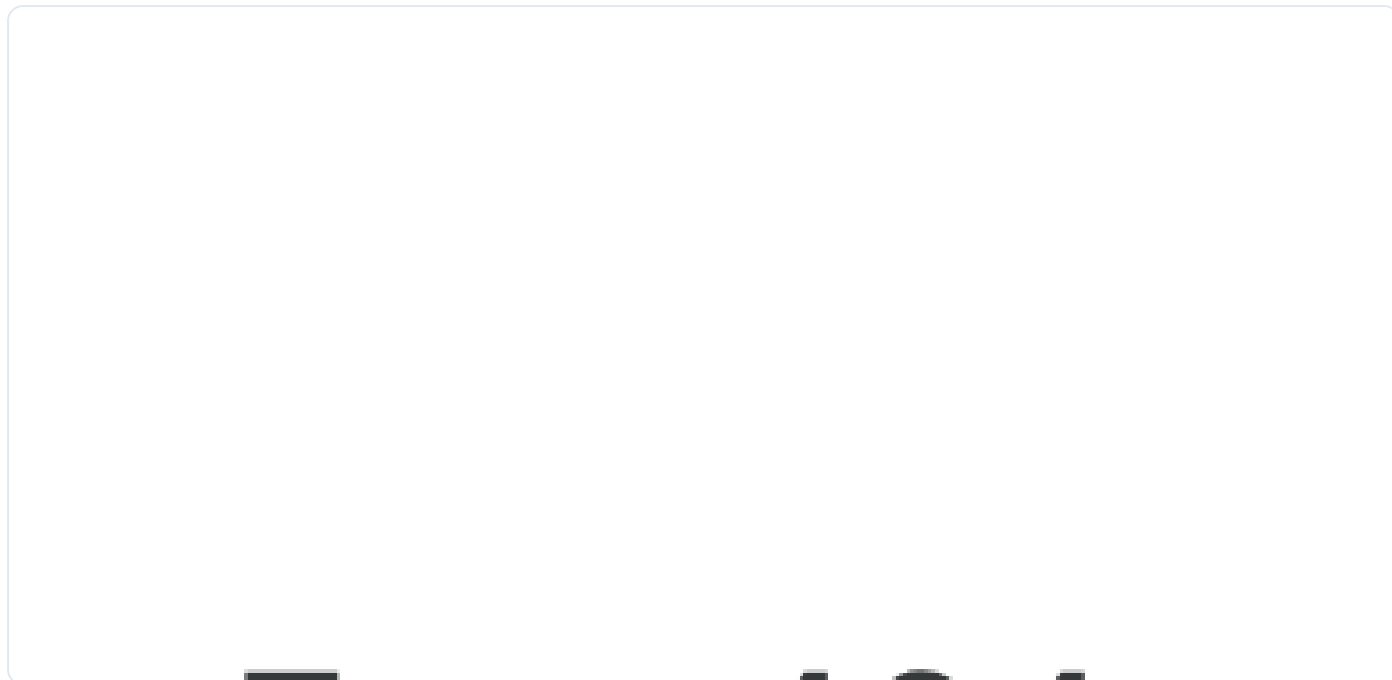
At a glance

The checks that decide most of this verdict.

Malware engines	6 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0% confidence AbuseIPDB, 2 reports; shared hosting inflates reports	CLEAR
Domain age	Not available No registration record was returned	NOTED
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by YE1	NOTED

The page as captured

<https://pub-e10d56052d2542d0b2f74abed3691951.r2.dev/>



What pub-e10d56052d2542d0b2f74abed3691951.r2.dev served when TrustSniffer captured it on 2026-10-01. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Security Alert

Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

This website is an object-storage or static-content endpoint presenting a “Not Found” and “Object not found” response rather than an identifiable business service. The accessible page contains no products, account functions, financial flows, forms, or clear operator information, so its apparent purpose cannot be established from the available content.

Scam/Impersonation Risk

A confirmed blacklist signal and multiple external malicious detections create a material risk for sensitive interaction, despite the accessible page itself being only a 404 response with no login form, payment mechanism, or explicit impersonation content. No distinct legal-entity identity contradiction or brand-impersonation indicator was observed. Two abuse reports were associated with a shared content-delivery address and were discounted because they applied to provider infrastructure rather than being reliably attributable to this site; that qualification does not offset the separate domain-level threat detections.

EVIDENCE

- The homepage returned “Not Found,” “Error 404,” and “Object not found,” with no forms, links, monetization, or authentication elements.
- External reputation analysis recorded 6 malicious detections among 11 effective detections, including a tier-one threat detection.
- The domain was recorded on an external blacklist; the broader safe-browsing check did not report a malicious result.
- Two abuse reports concerned a shared Cloudflare content-delivery IP and had zero confidence, with attribution explicitly discounted as shared infrastructure.

Regulatory Verification Notes

The accessible endpoint does not provide a usable legal, about, terms, licensing, or operator-identification page. Consequently, the real-world operator remains unverified and no licensing or registration disclosure can be assessed from the available site content. This is a regulatory-transparency gap distinct from the external threat signals; it does not independently establish fraud, but it prevents the site from supporting a regulated or accountable business identity.

EVIDENCE

- The captured homepage is an object-storage 404 page and exposes no legal entity, regulatory status, license number, or business description.
- TLS uses a domain-validated certificate issued by YE1, valid through 2026-12-06.
- The transport certificate establishes encrypted communication only; it does not independently verify the operator’s identity or regulatory standing.

What to Verify Next

Before any sensitive interaction, an organization should independently confirm the operator’s legal identity and any claimed authorization through the relevant official registry, using contact details obtained from an independently trusted source rather than from this endpoint. The external blacklist and malicious-detection findings should be resolved with the organization’s security team before the domain is permitted for login, credential submission, financial activity, or downloads. Any future page presenting a business service should also be checked for consistent legal, terms, privacy, refund, and contact disclosures.

EVIDENCE

- The accessible page contains no operator identity or licensing material to validate.
- The site is currently represented by an object-not-found response rather than a functioning service page.
- External threat detections remain unresolved in the supplied evidence.

Summary Verdict

The site has a moderate trust posture with elevated risk for sensitive interaction. Its accessible content is non-functional and its operator identity is unverified, while confirmed external threat signals materially reduce

confidence. No identity contradiction or direct impersonation finding was observed, but the available evidence is insufficient to support normal credential or financial use.

Infrastructure Integrity

The site is served through Cloudflare's CDN/WAF infrastructure, with all observed addresses identified as edge servers and no origin candidate observed. This provides a mitigating layer against direct origin exposure, but it is a protective hosting characteristic rather than evidence that the site or its operator is legitimate.

EVIDENCE

- Hosted on AS13335, CLOUDFLARENET—Cloudflare, Inc., US.
- Four observed addresses were Cloudflare edge addresses; zero likely origin addresses were identified.
- The site's transport encryption used a DV certificate issued by YE1, valid to 2026-12-06.

Closing Assessment

The proportionate course is to restrict the domain from sensitive use and require independent identity, authorization, and security clearance before any credentials, financial information, or downloads are permitted.

Written analysis generated 2026-10-01 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

4 findings contributed to this verdict, raised by governance, page content, external reputation, behaviour in a sandbox.

01 Governance

- What the site offers, as described on its own pages, limits how high the score can go until more of it can be verified.

Governance rule:gov_business_model_cap

02 Page content

- The page has very little readable content.

Page content rule:PAGE_CONTENT_THIN

- The page has no description for search engines, which established sites usually provide.

Page content rule:PAGE_SEO_MISSING_META

03 External reputation

- A widely visited domain carries an external threat flag, which calls for a closer look rather than a conclusion on its own.

External reputation rule:EXT_BLACKLIST_HIGH_RANK_REVIEW

04 Behaviour in a sandbox

- Most of what the page loaded came from other domains rather than from this one.

Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH

- The review of the page network activity found requests that look out of place.

Behaviour in a sandbox rule:BEHAV_GPT_SUSPICIOUS_NETWORK

Signals weighed against the site

- AbuseIPDB: 2 reports on hosting IP 2606:4700:311b::6812:362d (Cloudflare, Inc., Content Delivery Network), 0% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	50%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of pub-e10d56052d2542d0b2f74abed3691951.r2.dev.

- The request stayed on pub-e10d56052d2542d0b2f74abed3691951.r2.dev. It was not redirected to another domain. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Not available
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:311b::6812:362d
Name servers	Not available
CDN / edge network	Detected (cloudflare)
Resolved IP addresses	4
Edge IP addresses	4
Likely origin IP addresses	0
SSL issuer	YE1
SSL expiry	2026-12-06

Domain age	Not available (no registration date was returned)
Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 6 flagged AbuseIPDB: 0% confidence, 2 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about pub-e10d56052d2542d0b2f74abed3691951.r2.dev at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/pub-e10d56052d2542d0b2f74abed3691951.r2.dev> · assessed 2026-10-01