

Is 101.99.90.156 a scam? TrustSniffer's high-risk assessment: 0/100

101.99.90.156

Verdict

0

OUT OF 100

CRITICAL RISK

101.99.90.156 shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Assessed 2026-08-18 by automated analysis. Classification confidence 70%.

WHAT THIS SITE APPEARS TO BE

A mid-maturity ad-supported adult video site focused on 'Desi/Indian' porn. The site aggregates explicit video listings, categories, and uses third-party analytics. Operator identity and contact details are minimal; monetization appears to rely on ads and external partner links.

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.

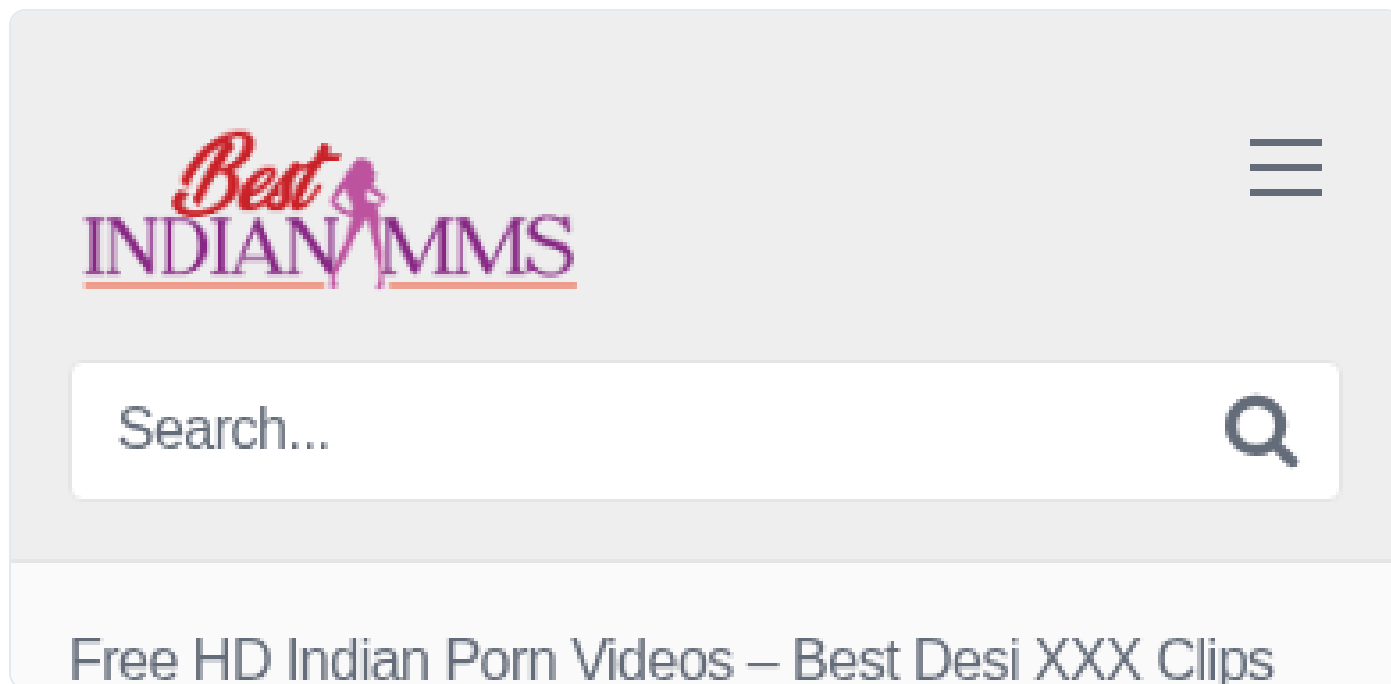
At a glance

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 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	4.9 years old Registered history	CLEAR
Web archive	Archived since 2021 71 snapshots	CLEAR

The page as captured

https://101.99.90.156/



What 101.99.90.156 served when TrustSniffer captured it on 2026-08-18. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2021.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

The website is an ad-supported adult-content platform presenting free Indian/Desi explicit video listings, category navigation, newsletter registration, advertising, analytics, and links to external partner services; its apparent business model is audience aggregation rather than direct on-site sales.

Scam/Impersonation Risk

The site presents a **high-risk sensitive-interaction posture** because external reputation checks recorded multiple malicious detections and a corroborated blacklist status. This is a confirmed reputational contradiction, although the available page evidence does not establish brand impersonation, phishing forms, or an identity contradiction between legal entities. The site's notice that it may disappear if authorities or internet providers block it, combined with requests to subscribe for future address changes, adds operational uncertainty. Browser observation also identified substantial external network activity, requests to disable ad-blocking, and material page changes after interaction; these conditions increase exposure to advertising, tracking, and third-party content risk. The site does not display a direct payment flow, but this does not make credential, download, or external-link interactions appropriate. Evidence:

- The homepage presents explicit video aggregation, regional categories, newsletter subscription, and external partner content.
- External reputation checks recorded 6 malicious detections and 1 suspicious detection, with the domain marked blacklisted by multiple sources.
- Browser testing recorded 55 external XHR requests, 24 non-whitelisted external XHR requests, 11 external POST requests, and 1 non-whitelisted external POST request.
- The homepage requests that visitors disable ad-blocking and states that the site may change its web address if access is restricted.

Regulatory Verification Notes

The about and contact pathways provide limited operator information, and the available site content does not clearly identify a responsible legal entity, physical address, or applicable licensing position. These are disclosure and accountability gaps rather than independent proof of fraud, but they materially limit the ability to attribute the service to a verified real-world operator. The business model is also not presented as a clearly defined product or regulated service, with monetization apparently dependent on advertising, analytics, and external partner links. No broker match was identified in the available third-party contextual check. Evidence:

- The site's about and contact pages provide minimal operator and contact detail.
- The homepage and associated site pages do not present a clear legal entity or licensing disclosure.
- The site's business description identifies advertising, tracking/analytics, newsletter subscription, and external partner links as the apparent monetization mechanisms.

What to Verify Next

Before any sensitive interaction, an enterprise or prospective user should independently establish the responsible operator and confirm applicable content, privacy, and communications requirements through authoritative registries or offline channels. Any external partner destination should be assessed separately rather than trusted through the site's referral path, and browser isolation, current endpoint protection, and download controls should be applied when accessing the pages. Official support and contact channels should be confirmed independently before responding to subscription or address-change requests. Evidence:

- The contact and about pathways do not provide sufficient information for independent operator attribution.
- The site links to external services and uses third-party analytics, creating separate trust boundaries outside the site's own pages.
- Interaction testing identified 4,804 maximum DOM differences after interaction and 2,402 DOM changes per density measurement.

Summary Verdict

The available evidence supports a **critical trust posture** with elevated risk for sensitive interactions. The site may provide informational or entertainment content, but its external reputation contradictions, limited accountability, and observed browser and network behavior prevent it from being treated as a trusted service environment.

Infrastructure Integrity

The site resolves directly to two likely origin addresses and does not use a detected CDN or WAF layer. Hosting is provided by Shinjiru Technology Sdn Bhd in Malaysia; this identifiable infrastructure is a limited technical positive, but it supplies little protective separation or reputational mitigation against the external threat findings.

EVIDENCE

- Hosted on AS45839 (SHINJIRU-MY-AS-AP - Shinjiru Technology Sdn Bhd, MY).
- Infrastructure resolution identified 2 unique IP addresses, both classified as likely origin addresses, with 0 edge IP addresses.
- No CDN was detected.

Closing Assessment

The proportionate course is to restrict the site to tightly controlled, read-only review and prevent credential submission, downloads, payments, or onward interaction with linked services until independent attribution and security validation are complete.

Written analysis generated 2026-08-18 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by analysis engine, behaviour in a sandbox.

01 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- The page rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.
Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- The page exchanged network traffic with destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
- The page replaced a large part of its own content after loading.
Behaviour in a sandbox rule:BEHAV_DOM_CHANGE_HIGH
- The page made background requests to destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR
- A large share of what the page loaded came from other domains.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE

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 101.99.90.156.

- The request stayed on 101.99.90.156. It was not redirected to another domain. CLEAR
- The earliest public archive of this site is from 2021-09-18. CLEAR

Domain intelligence

Registrar	Not available
Hosting	Not available
Country	Not available
Server IP	101.99.90.156
Name servers	Not available
SSL issuer	Not available
SSL expiry	Not available
Domain age	4.91 years (continuous registration)
Domain expiry	Not available
Archive first seen	2021-09-18
Archive snapshots	71
Reputation	VirusTotal: 6 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 101.99.90.156 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/101.99.90.156> · assessed 2026-08-18