

Is jswen.com a scam? TrustSniffer's high-risk assessment: 5/100

jswen.com

Verdict

5

OUT OF 100

CRITICAL RISK

jswen.com 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

Governance Risk

Assessed 2026-09-22 by automated analysis. Classification confidence 75%.

What this site appears to be

A basic Apache-style directory index listing exposing server folders. No forms, login, or monetization elements are present.

Compromised host notice

A threat-intelligence feed listed a file on jswen.com as distributing malware (last seen 2026-09-04). TrustSniffer's evidence indicates that the site itself was compromised: the listing concerns a file placed on it by someone else, and the site's owner is most likely a victim, not the actor.

Until the file is removed, downloading anything from this site is not safe. If you run this site, remove the listed file, update the site software and its plugins, change its passwords and review it for other unauthorized changes.

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	13 flagged it	RISK
	VirusTotal	
Google Safe Browsing	Not listed	CLEAR
	Google	
Abuse reports on the host	0 reports	NOTED
	AbuseIPDB; shared hosting inflates this count	

Domain age	5.7 years old Registered history	CLEAR
Web archive	Archived since 2004 363 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://jswen.com/

Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
cgi-bin/	2026-08-31 17:51	-	
payment/	2026-09-03 14:19	-	
weeklyreport/	2026-09-03 16:52	-	

What jswen.com served when TrustSniffer captured it on 2026-09-22. 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 2004.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

The website is a bare Apache-style directory index rather than a conventional business or service site. It presents visitors with server folders labelled “cgi-bin/,” “payment/,” and “weeklyreport/,” but provides no identifiable product, service, commercial proposition, or interactive account function.

Scam/Impersonation Risk

Contradictory risk signals are present. The domain is externally blacklisted, with multiple security detections identifying malicious or suspicious activity; this is the decisive risk indicator and warrants a security-forward posture even though the homepage itself contains no login form, payment workflow, or explicit brand-impersonation content. The historical record also creates a provenance inconsistency: archived activity predates the current registration record, so the available history does not establish continuity between the present site and the earlier domain presence. The sparse directory page therefore provides no reliable basis for attributing the site to a legitimate operator.

EVIDENCE

- The homepage is titled "Index of /" and exposes the directories "cgi-bin/," "payment/," and "weeklyreport/," with no stated business identity or service description.
- External reputation telemetry records 13 malicious and 2 suspicious detections from 20 evaluated results; blacklist status is confirmed by two external sources.
- The registration record shows creation on 2021-01-10 and an age of 5.7 years, while archive records show 363 snapshots from 2004-11-12 through 2012-06-28, covering 9 tracked years.

Regulatory Verification Notes

The site does not present a business identity, licensing claim, registration number, regulated-service description, or governing legal terms on the observed page. This is a material disclosure gap rather than independent proof of fraud, but it prevents meaningful regulatory or operator verification. The real-world operator remains unverified. The registration record identifies Gname.com Pte. Ltd. as registrar, while the transport certificate provides only domain-level validation; neither establishes the identity or regulatory standing of the operator.

EVIDENCE

- The homepage contains only a directory listing and no legal, licensing, corporate, or regulatory disclosure.
- The domain is registered through Gname.com Pte. Ltd.; registrant details are redacted for privacy.
- The site uses a DV TLS certificate issued by YR1, valid through 2026-11-29.

What to Verify Next

No sensitive interaction should proceed unless an independently obtained corporate identity and any claimed authorization can be matched to an official registry. Any support or contact channel should be confirmed through an independently sourced route rather than information supplied only by the site. Security teams should also preserve and investigate the observed directory paths before allowing the domain or its content into an operational environment.

EVIDENCE

- The homepage supplies no operator identity, legal entity, license number, or official business contact context to validate independently.
- The observed site structure exposes server directories rather than a controlled, purpose-built business interface.

Summary Verdict

The overall posture is **critical risk**, with legitimacy and operator identity unestablished and external threat intelligence providing a confirmed adverse signal. The site is unsuitable for login, credential submission, payment activity, or other sensitive interaction.

Infrastructure Integrity

The site resolves directly to hosting associated with Sollutium-NL - SOLLUTIUM EU Sp z.o.o., PL, without a detected CDN or WAF layer; two likely origin addresses were identified, including infrastructure geolocated in Ukraine. This direct hosting posture offers limited protective separation and cannot offset the adverse reputation findings.

EVIDENCE

- Hosted on AS43641, Sollutium-NL - SOLLUTIUM EU Sp z.o.o., PL, with infrastructure country recorded as UA.
- Two likely origin IP addresses were identified and zero edge IP addresses were detected; no CDN was present.

Closing Assessment

The appropriate action is to block or isolate the domain for sensitive use and require independent identity, authorization, and content-safety clearance before any future operational engagement.

Written analysis generated 2026-09-22 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, external reputation.

01 Governance Risk

- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.
External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNVERIFIED
--------	------------

Identity score	30/100
Identity verification confidence	25%

- 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 jswen.com.

- The request stayed on jswen.com. It was not redirected to another domain. CLEAR
- Registration is published under Gname.com Pte. Ltd.. CLEAR
- DNS for this domain is served by v-sys.org, across 2 name servers. NOTED
- The registration is paid up to 2027-01-10. NOTED
- The earliest public archive of this site is from 2004-11-12. CLEAR
- It is hosted on Sollutium-NL, from a server in UA. NOTED

Domain intelligence

Registrar	Gname.com Pte. Ltd.
Hosting	Sollutium-NL - SOLLUTIUM EU Sp z.o.o., PL
Country	UA
Server IP	195.66.212.20
Name servers	NS3-AMS.V-SYS.ORG, NS4-AMS.V-SYS.ORG
SSL issuer	YR1
SSL expiry	2026-11-29
Domain age	5.70 years (continuous registration)
Domain expiry	2027-01-10
Archive first seen	2004-11-12
Archive snapshots	363
Reputation	VirusTotal: 13 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about jswen.com 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/jswen.com> · assessed 2026-09-22