WebAudit

Security Compliance Assessment

xyz.com

Scan Date: 2026-07-22

Frameworks assessed in this report:

- OWASP Top 10 2021
- PCI-DSS v4.0
- GDPR Article 32
- ISO 27001:2022 Annex A

Executive Summary

This report assesses the security posture of **xyz.com** against four major compliance frameworks. Each framework maps specific technical controls to the corresponding WebAudit scan findings. Requirements are marked **PASS** when all associated checks succeed, or **FAIL** when one or more checks are not met.

Framework	Requirements	Passed	Failed	Overall Status
OWASP Top 10 2021	7	4	3	■ PARTIAL
PCI-DSS v4.0	5	2	3	■ PARTIAL
GDPR Article 32	4	1	3	■ PARTIAL
ISO 27001:2022 Annex A	6	2	4	■ PARTIAL

OWASP Top 10 2021

Official documentation: https://owasp.org/Top10 | WebAudit guide: https://webaudit.in/compliance/owasp

The OWASP Top 10 is the most widely referenced standard for web application security risks, published by the Open Web Application Security Project. It identifies the ten most critical vulnerability categories affecting web applications globally. Compliance with the relevant OWASP Top 10 categories is a baseline expectation for any application handling user data or financial transactions.

Req ID	Requirement	WebAudit Check	Status	Finding
A01	Broken Access Control	X-Frame-Options Present; CORS No Wildcard Origin; Frame Embedding Restricted	✓ PASS	All checks passed.
A02	Cryptographic Failures	TLS Certificate Valid; HSTS Header Present; Cookies Have Secure Flag; No Mixed HTTP Content	✗ FAIL	Cookie(s) missing Secure flag: _ga.
A03	Injection (XSS)	Content Security Policy Present; CSP No unsafe-inline / unsafe-eval	✗ FAIL	Content-Security-Policy header is missing. Content-Security-Policy is not set.
A05	Security Misconfiguration	X-Content-Type-Options Present; Referrer-Policy Present; Permissions-Policy Present; Server Version Not Disclosed	✓ PASS	All checks passed.
A06	Vulnerable and Outdated Components	Subresource Integrity (SRI) Present	✓ PASS	All checks passed.
A07	Identification and Authentication Failures	Cookies Have HttpOnly Flag; Cookies Have SameSite Attribute	✓ PASS	All checks passed.
A08	Software and Data Integrity Failures	Subresource Integrity (SRI) Present; Content Security Policy Present	✗ FAIL	Content-Security-Policy header is missing.

PCI-DSS v4.0

Official documentation: https://www.pcisecuritystandards.org | WebAudit guide: https://webaudit.in/compliance/pci-dss

The Payment Card Industry Data Security Standard (PCI-DSS) is a mandatory security standard for organisations that handle credit card payments. Version 4.0, effective from March 2024, strengthens requirements around web application security. Any web application that processes,

stores, or transmits cardholder data must meet these technical controls at the application layer.

Req ID	Requirement	WebAudit Check	Status	Finding
4.2.1	Strong Cryptography in Transit	TLS Certificate Valid; HSTS Header Present; No Mixed HTTP Content	✓ PASS	All checks passed.
6.4.1	Public-Facing Web Application Protection	Content Security Policy Present; CSP No unsafe-inline / unsafe-eval; X-Frame-Options Present; X-Content-Type-Options Present	✗ FAIL	Content-Security-Policy header is missing. Content-Security-Policy is not set.
6.4.3	Payment Page Script Management	Subresource Integrity (SRI) Present; Content Security Policy Present	✗ FAIL	Content-Security-Policy header is missing.
8.3.6	Secure Transmission of Authentication Credentials	TLS Certificate Valid; Cookies Have Secure Flag; HSTS Header Present	✗ FAIL	Cookie(s) missing Secure flag: _ga.
12.3.3	Cryptographic Algorithm Review	TLS Certificate Valid	✓ PASS	All checks passed.

GDPR Article 32

Official documentation: https://gdpr-info.eu/art-32-gdpr | WebAudit guide: https://webaudit.in/compliance/gdpr

Article 32 of the General Data Protection Regulation (GDPR) requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including encryption of personal data and ongoing confidentiality, integrity, availability, and resilience of processing systems. These obligations apply to any organisation processing EU/EEA personal data.

Req ID	Requirement	WebAudit Check	Status	Finding
32(1)(a)	Encryption of Personal Data in Transit	TLS Certificate Valid; HSTS Header Present; Cookies Have Secure Flag	✗ FAIL	Cookie(s) missing Secure flag: _ga.
32(1)(b)	Ongoing Confidentiality and Integrity	Content Security Policy Present; X-Content-Type-Options Present; Server Version Not Disclosed; No Mixed HTTP Content	✗ FAIL	Content-Security-Policy header is missing.

Req ID	Requirement	WebAudit Check	Status	Finding
32(1)(c)	Resilience and Availability	CAA DNS Records Present; SPF DNS Record Present; DMARC DNS Record Present	✓ PASS	All checks passed.
32(1)(d)	Regular Testing and Assessment	DMARC Policy Enforced; Referrer-Policy Present; Permissions-Policy Present	✗ FAIL	DMARC policy is p=none — not enforced (needs quarantine or reject).

ISO 27001:2022 Annex A

Official documentation: https://www.iso.org/standard/27001 | WebAudit guide: https://webaudit.in/compliance/iso27001

ISO/IEC 27001:2022 is the international standard for information security management systems (ISMS). Annex A provides a reference set of controls that organisations must consider for their ISMS. The 2022 revision introduced four new technology-specific controls relevant to web application security. Certification requires documented implementation of applicable controls and ongoing monitoring.

Req ID	Requirement	WebAudit Check	Status	Finding
A.8.23	Web Filtering	Content Security Policy Present; CSP No unsafe-inline / unsafe-eval; CORS No Wildcard Origin	✗ FAIL	Content-Security-Policy header is missing. Content-Security-Policy is not set.
A.8.24	Use of Cryptography	TLS Certificate Valid; HSTS Header Present; Cookies Have Secure Flag	✗ FAIL	Cookie(s) missing Secure flag: _ga.
A.8.25	Secure Development Life Cycle	Subresource Integrity (SRI) Present; No Mixed HTTP Content	✓ PASS	All checks passed.
A.8.26	Application Security Requirements	Content Security Policy Present; X-Frame-Options Present; X-Content-Type-Options Present; Referrer-Policy Present; Permissions-Policy Present	✗ FAIL	Content-Security-Policy header is missing.
A.8.16	Monitoring Activities	DMARC DNS Record Present; DMARC Policy Enforced; SPF DNS Record Present	✗ FAIL	DMARC policy is p=none — not enforced (needs quarantine or reject).

Req ID	Requirement	WebAudit Check	Status	Finding
A.5.14	Information Transfer	HSTS Header Present; No Mixed HTTP Content; Cookies Have SameSite Attribute	✓ PASS	All checks passed.

Assessment Summary

Based on the scan of **xyz.com**, the overall risk level is **HIGH** — 13 of 22 requirements failed across all four frameworks. The framework with the weakest compliance posture is **ISO 27001:2022 Annex A** (4 failed requirements). The highest-priority finding is: *Cookie(s) missing Secure flag: _ga.* (requirement: Cryptographic Failures). WebAudit recommends addressing the items in the remediation plan below, starting with cryptographic and injection controls.

Finding	CWE Reference
CSP No unsafe-inline / unsafe-eval, Content Security Policy Present	CWE-79 — Improper Neutralisation of Input (XSS)
DMARC Policy Enforced	CWE-290 — Authentication Bypass by Spoofing

Remediation Plan

The following table lists all failed requirements, grouped by requirement ID. Address each item to improve your compliance posture.

Req ID	Requirement	Framework	Finding(s)	Recommended Fix
A02	Cryptographic Failures	OWASP Top 10 2021	Cookie(s) missing Secure flag: _ga.	Enforce HTTPS with Strict-Transport-Security (HSTS). Set the Secure flag on all cookies.
A03	Injection (XSS)	OWASP Top 10 2021	Content-Security-Policy header is missing. Content-Security-Policy is not set.	Deploy a Content Security Policy. Avoid 'unsafe-inline' and 'unsafe-eval' — use nonces or hashes for inline scripts instead.
A08	Software and Data Integrity Failures	OWASP Top 10 2021	Content-Security-Policy header is missing.	Deploy SRI for all externally loaded scripts and stylesheets. Use a strict CSP to prevent loading from untrusted origins.
6.4.1	Public-Facing Web Application Protection	PCI-DSS v4.0	Content-Security-Policy header is missing. Content-Security-Policy is not set.	Deploy a Content Security Policy. Set X-Frame-Options and X-Content-Type-Options headers.
6.4.3	Payment Page Script Management	PCI-DSS v4.0	Content-Security-Policy header is missing.	Add Subresource Integrity (integrity= attribute) to all external scripts. Use a strict CSP allowlist to restrict script sources.
8.3.6	Secure Transmission of Authentication Credentials	PCI-DSS v4.0	Cookie(s) missing Secure flag: _ga.	Ensure all authentication endpoints use HTTPS. Set Secure flag on all authentication cookies.
32(1)(a)	Encryption of Personal Data in Transit	GDPR Article 32	Cookie(s) missing Secure flag: _ga.	Enforce HTTPS on all endpoints. Deploy HSTS.
32(1)(b)	Ongoing Confidentiality and Integrity	GDPR Article 32	Content-Security-Policy header is missing.	Deploy CSP to prevent content injection. Set X-Content-Type-Options: nosniff.
32(1)(d)	Regular Testing and Assessment	GDPR Article 32	DMARC policy is p=none — not enforced (needs quarantine or reject).	Enforce DMARC policy (p=quarantine or p=reject). Set Referrer-Policy and Permissions-Policy to limit data leakage.
A.8.23	Web Filtering	ISO 27001:2022 Annex A	Content-Security-Policy header is missing. Content-Security-Policy is not set.	Implement a Content Security Policy with a strict allowlist for script, style, and resource sources. Remove CORS wildcards.
A.8.24	Use of Cryptography	ISO 27001:2022 Annex A	Cookie(s) missing Secure flag: _ga.	Use TLS 1.2+ with strong cipher suites. Enforce HSTS.

Req ID	Requirement	Framework	Finding(s)	Recommended Fix
A.8.26	Application Security Requirements	ISO 27001:2022 Annex A	Content-Security-Policy header is missing.	Deploy the full set of recommended security headers: CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy.
A.8.16	Monitoring Activities	ISO 27001:2022 Annex A	DMARC policy is p=none — not enforced (needs quarantine or reject).	Configure SPF and DMARC with p=quarantine or p=reject to receive delivery reports and detect email spoofing of your domain.

Disclaimer

This compliance report is generated automatically by WebAudit (webaudit.in) based on observable HTTP/TLS/DNS characteristics of the target domain. It assesses technical web-layer controls only and does not constitute a formal audit, legal advice, or certification under any of the frameworks referenced. Compliance with PCI-DSS, GDPR, ISO 27001, or OWASP requires additional organisational, procedural, and operational controls beyond those assessed here. Consult a qualified auditor or legal counsel for formal compliance determination.