

TARGET

xyz.com

19

19 / 22 requirements

19 of 22 requirements across four frameworks show a web-layer gap.

OWASP

1/7

PCI-DSS

2/5

GDPR

0/4

ISO 27001

0/6

PREPARED FOR
XYZ Ltd.

PREPARED BY
A. Mehta · Independent
security consultant

ASSESSED
30 Sep 2026

METHOD
Passive · one live
request

xyz.com shows 19 requirement gaps. *They trace back to seven fixes.*

Most frameworks test the same handful of web-layer controls, so one missing control fails several requirements at once. The table below ranks those controls by severity, then by how many requirements each one clears.

FRAMEWORKS • 22 REQUIREMENTS ASSESSED

	FRAMEWORK	ASSESSED	MET	GAPS	STATUS
01	OWASP Top 10 2021	7	1	6	PARTIAL
02	PCI-DSS v4.0	5	2	3	PARTIAL
03	GDPR Article 32	4	0	4	GAPS FOUND
04	ISO 27001:2022 Annex A	6	0	6	GAPS FOUND

FIX THESE FIRST

CLEARs

01	Content-Security-Policy missing Critical · Content-Security-Policy header is missing.	7
02	X-Content-Type-Options missing Important · X-Content-Type-Options header is missing.	4
03	DMARC not enforced (p=none) Important · DMARC policy is p=none — not enforced (needs quarantine or reject).	2
04	Cookies missing security attributes Minor · Cookie(s) missing Secure flag: last_visit. Cookie(s) missing HttpOnly flag: last_visit. Cookie(s) without SameSite attribute: last_visit.	6
05	External scripts without Subresource Integrity Minor · External script/stylesheets(s) loaded without Subresource Integrity (SRI).	4

OWASP Top 10 2021

The risk categories web applications most often get wrong.

1 OF 7 REQUIREMENTS MET • PARTIAL

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.

Standard: <https://owasp.org/Top10> • Guide: <https://secrescanr.com/compliance/owasp>

A02 • Cryptographic Failures

MINOR

Gap

1 OF 4 CHECKS

REQUIREMENT	Failures related to cryptography which expose sensitive data in transit. Includes missing HTTPS enforcement, weak TLS, and insecure cookies.
WHAT FAILED	Cookies without Secure — Cookie(s) missing Secure flag: last_visit.
ALSO CHECKED	TLS Certificate Valid, HSTS Header Present, No Mixed HTTP Content — passed
FIX	Enforce HTTPS with Strict-Transport-Security (HSTS). Set the Secure flag on all cookies. Eliminate mixed HTTP/HTTPS content.

A03 • Injection (XSS)

CRITICAL

Gap

2 OF 2 CHECKS

REQUIREMENT	Cross-site scripting (XSS) allows attackers to inject client-side scripts into web pages viewed by other users. A strong Content Security Policy is the primary browser-side defence.
WHAT FAILED	Content-Security-Policy missing — Content-Security-Policy header is missing.
FIX	Deploy a Content Security Policy. Avoid 'unsafe-inline' and 'unsafe-eval' — use nonces or hashes for inline scripts instead.

A05 • Security Misconfiguration IMPORTANT

Gap

2 OF 4 CHECKS

REQUIREMENT	Insecure default configurations, incomplete configurations, or misconfigured HTTP headers that expose unnecessary attack surface.
WHAT FAILED	X-Content-Type-Options missing — X-Content-Type-Options header is missing. Referrer-Policy missing — Referrer-Policy header is missing.
ALSO CHECKED	Permissions-Policy Present, Server Version Not Disclosed — passed
FIX	Set X-Content-Type-Options: nosniff, Referrer-Policy, and Permissions-Policy. Remove server version headers (Server, X-Powered-By).

A06 • Vulnerable and Outdated Components MINOR

Gap

1 OF 1 CHECKS

REQUIREMENT	Components (libraries, frameworks) running with known vulnerabilities. Subresource Integrity (SRI) ensures external scripts have not been tampered with.
WHAT FAILED	External scripts without Subresource Integrity — External script/stylesheets(s) loaded without Subresource Integrity (SRI).
FIX	Add integrity= and crossorigin= attributes to all external <script> and <link> tags. Use npm audit / pip audit to find vulnerable packages.

A07 • Identification and Authentication Failures MINOR

Gap

2 OF 2 CHECKS

REQUIREMENT	Authentication weaknesses including session cookie misconfigurations that allow session hijacking.
WHAT FAILED	Cookies without HttpOnly — Cookie(s) missing HttpOnly flag: last_visit. Cookies without SameSite — Cookie(s) without SameSite attribute: last_visit.
FIX	Set HttpOnly and SameSite=Lax (or Strict) on all session cookies to prevent JavaScript access and CSRF-based session theft.

A08 • Software and Data Integrity Failures

CRITICAL

Gap

2 OF 2 CHECKS

REQUIREMENT	Code and infrastructure that does not protect against integrity violations. Includes CI/CD pipeline integrity and client-side supply chain attacks via unverified scripts.
WHAT FAILED	External scripts without Subresource Integrity — External script/stylesheet(s) loaded without Subresource Integrity (SRI). Content-Security-Policy missing — Content-Security-Policy header is missing.
FIX	Deploy SRI for all externally loaded scripts and stylesheets. Use a strict CSP to prevent loading from untrusted origins.

MET (1)

✓ A01 • Broken Access Control

3 checks passed

02 / PCI-DSS V4.0

PCI-DSS v4.0

What a site that touches card data must enforce at the web layer.

2 OF 5 REQUIREMENTS MET • PARTIAL

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.

Standard: <https://www.pcisecuritystandards.org> • Guide: <https://secrescanr.com/compliance/pci-dss>

6.4.1 • Public-Facing Web Application Protection

CRITICAL

Gap

3 OF 4 CHECKS

REQUIREMENT	Public-facing web applications must be protected against known attacks via security controls — including injection attacks, broken access control, and cross-site scripting.
WHAT FAILED	Content-Security-Policy missing — Content-Security-Policy header is missing. X-Content-Type-Options missing — X-Content-Type-Options header is missing.
ALSO CHECKED	X-Frame-Options Present — passed
FIX	Deploy a Content Security Policy. Set X-Frame-Options and X-Content-Type-Options headers. Conduct regular vulnerability assessments.

6.4.3 • Payment Page Script Management

CRITICAL

Gap

2 OF 2 CHECKS

REQUIREMENT	All scripts loaded on payment pages must be authorised, have their integrity verified, and be inventoried to prevent supply-chain skimming attacks.
WHAT FAILED	External scripts without Subresource Integrity — External script/stylesheet(s) loaded without Subresource Integrity (SRI). Content-Security-Policy missing — Content-Security-Policy header is missing.
FIX	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

MINOR

Gap

1 OF 3 CHECKS

REQUIREMENT	Authentication credentials must not be transmitted in cleartext or in a way that can be intercepted by attackers on the network.
WHAT FAILED	Cookies without Secure — Cookie(s) missing Secure flag: last_visit.
ALSO CHECKED	TLS Certificate Valid, HSTS Header Present — passed
FIX	Ensure all authentication endpoints use HTTPS. Set Secure flag on all authentication cookies. Enable HSTS to prevent downgrade.

MET (2)

✓ 4.2.1 • Strong Cryptography in Transit	3 checks passed
✓ 12.3.3 • Cryptographic Algorithm Review	1 check passed

GDPR Article 32

Technical measures that protect personal data in transit.

0 OF 4 REQUIREMENTS MET • GAPS FOUND

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.

Standard: <https://gdpr-info.eu/art-32-gdpr> • Guide: <https://secrescanr.com/compliance/gdpr>

32(1)(a) • Encryption of Personal Data in Transit

MINOR

Gap

1 OF 3 CHECKS

REQUIREMENT	Pseudonymisation and encryption of personal data. Web applications must encrypt all data in transit between the browser and server.
WHAT FAILED	Cookies without Secure — Cookie(s) missing Secure flag: last_visit.
ALSO CHECKED	TLS Certificate Valid, HSTS Header Present — passed
FIX	Enforce HTTPS on all endpoints. Deploy HSTS. Set the Secure flag on all cookies containing session identifiers or personal data.

32(1)(b) • Ongoing Confidentiality and Integrity

CRITICAL

Gap

2 OF 4 CHECKS

REQUIREMENT	The ongoing confidentiality, integrity, availability, and resilience of processing systems and services must be ensured.
WHAT FAILED	Content-Security-Policy missing — Content-Security-Policy header is missing. X-Content-Type-Options missing — X-Content-Type-Options header is missing.
ALSO CHECKED	Server Version Not Disclosed, No Mixed HTTP Content — passed
FIX	Deploy CSP to prevent content injection. Set X-Content-Type-Options: nosniff. Remove server version disclosure headers.

32(1)(c) • Resilience and Availability

MINOR

Gap

1 OF 3 CHECKS

REQUIREMENT	Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
WHAT FAILED	No CAA record — CAA (Certification Authority Authorization) DNS records are not published.
ALSO CHECKED	SPF DNS Record Present, DMARC DNS Record Present — passed
FIX	Publish CAA records to restrict certificate authorities. Configure SPF and DMARC to prevent email spoofing that could enable phishing attacks targeting your users.

32(1)(d) • Regular Testing and Assessment

IMPORTANT

Gap

2 OF 3 CHECKS

REQUIREMENT	A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring security of processing.
WHAT FAILED	DMARC not enforced (p=none) — DMARC policy is p=none — not enforced (needs quarantine or reject). Referrer-Policy missing — Referrer-Policy header is missing.
ALSO CHECKED	Permissions-Policy Present — passed
FIX	Enforce DMARC policy (p=quarantine or p=reject). Set Referrer-Policy and Permissions-Policy to limit data leakage. Conduct periodic security assessments.

ISO 27001:2022 Annex A

The Annex A controls a public web layer can evidence.

0 OF 6 REQUIREMENTS MET • GAPS FOUND

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.

Standard: <https://www.iso.org/standard/27001> • Guide: <https://secrescanr.com/compliance/iso27001>

A.8.23 • Web Filtering CRITICAL

Gap

2 OF 3 CHECKS

REQUIREMENT	Access to external websites must be managed to reduce exposure to malicious content. On the server side, CSP restricts what external resources your web application loads.
WHAT FAILED	Content-Security-Policy missing — Content-Security-Policy header is missing.
ALSO CHECKED	CORS No Wildcard Origin — passed
FIX	Implement a Content Security Policy with a strict allowlist for script, style, and resource sources. Remove CORS wildcards.

A.8.24 • Use of Cryptography MINOR

Gap

1 OF 3 CHECKS

REQUIREMENT	Rules for the effective use of cryptography, including cryptographic key management, must be defined and implemented.
WHAT FAILED	Cookies without Secure — Cookie(s) missing Secure flag: last_visit.
ALSO CHECKED	TLS Certificate Valid, HSTS Header Present — passed
FIX	Use TLS 1.2+ with strong cipher suites. Enforce HSTS. Protect session cookies with the Secure flag.

A.8.25 • Secure Development Life Cycle

MINOR

Gap

1 OF 2 CHECKS

REQUIREMENT	Rules for the secure development of software and systems must be established and applied. Includes supply-chain integrity controls.
WHAT FAILED	External scripts without Subresource Integrity — External script/style sheet(s) loaded without Subresource Integrity (SRI).
ALSO CHECKED	No Mixed HTTP Content — passed
FIX	Add Subresource Integrity to all external scripts and stylesheets. Eliminate HTTP resources loaded on HTTPS pages.

A.8.26 • Application Security Requirements

CRITICAL

Gap

3 OF 5 CHECKS

REQUIREMENT	Information security requirements must be identified, specified, and approved when developing or acquiring applications.
WHAT FAILED	Content-Security-Policy missing — Content-Security-Policy header is missing. X-Content-Type-Options missing — X-Content-Type-Options header is missing. Referrer-Policy missing — Referrer-Policy header is missing.
ALSO CHECKED	X-Frame-Options Present, Permissions-Policy Present — passed
FIX	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

IMPORTANT

Gap

1 OF 3 CHECKS

REQUIREMENT	Networks, systems, and applications must be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
WHAT FAILED	DMARC not enforced (p=none) — DMARC policy is p=none — not enforced (needs quarantine or reject).
ALSO CHECKED	DMARC DNS Record Present, SPF DNS Record Present — passed
FIX	Configure SPF and DMARC with p=quarantine or p=reject to receive delivery reports and detect email spoofing of your domain.

A.5.14 • Information Transfer

MINOR

Gap

1 OF 3 CHECKS

REQUIREMENT	Information transfer rules, procedures, and controls must be in place for all types of transfer facilities within the organisation and with external parties.
WHAT FAILED	Cookies without SameSite — Cookie(s) without SameSite attribute: last_visit.
ALSO CHECKED	HSTS Header Present, No Mixed HTTP Content — passed
FIX	Enforce HSTS. Eliminate mixed content. Set SameSite=Lax or Strict on cookies to prevent cross-site data transfer.

05 / WEAKNESS REFERENCES

CWE references

The weakness classes behind the gaps, for tickets and audit trails.

CWE	WEAKNESS • WHAT WAS OBSERVED
CWE-79	Improper Neutralization of Input During Web Page Generation (XSS) Content-Security-Policy header is missing.
CWE-290	Authentication Bypass by Spoofing DMARC policy is p=none — not enforced (needs quarantine or reject).
CWE-295	Improper Certificate Validation CAA (Certification Authority Authorization) DNS records are not published.
CWE-353	Missing Support for Integrity Check External script/stylesheets loaded without Subresource Integrity (SRI).
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute Cookie(s) missing Secure flag: last_visit. Cookie(s) missing HttpOnly flag: last_visit. Cookie(s) without SameSite attribute: last_visit.
CWE-1004	Sensitive Cookie Without 'HttpOnly' Flag Cookie(s) missing Secure flag: last_visit. Cookie(s) missing HttpOnly flag: last_visit. Cookie(s) without SameSite attribute: last_visit.

The plan

One row per control. The Met column is the requirements met once that row and every row above it are done.

CONTROL · FIX	MET	OWNER	DONE ON
☐ Content-Security-Policy missing CRITICAL · CLEARS 7: OWASP A03, OWASP A08, PCI-DSS 6.4.1, PCI-DSS 6.4.3, GDPR 32(1)(B), ISO 27001 A.8.23, ISO 27001 A.8.26 <pre>Content-Security-Policy: default-src 'self'; script-src 'self'; object-src 'none'; base-uri 'self'; frame-ancestors 'self'; form-action 'self'</pre>	5/22		
☐ X-Content-Type-Options missing IMPORTANT · CLEARS 4: OWASP A05, PCI-DSS 6.4.1, GDPR 32(1)(B), ISO 27001 A.8.26 <pre>X-Content-Type-Options: nosniff</pre>	7/22		
☐ DMARC not enforced (p=none) IMPORTANT · CLEARS 2: GDPR 32(1)(D), ISO 27001 A.8.16 <pre>_dmarc.xyz.com. TXT "v=DMARC1; p=quarantine; rua=mailto:dmarc@xyz.com"</pre>	8/22		
☐ Cookies missing security attributes MINOR · CLEARS 6: OWASP A02, OWASP A07, PCI-DSS 8.3.6, GDPR 32(1)(A), ISO 27001 A.8.24, ISO 27001 A.5.14 <pre>Set-Cookie: <name>=<value>; Path=/; Secure; HttpOnly; SameSite=Lax</pre>	14/22		
☐ External scripts without Subresource Integrity MINOR · CLEARS 4: OWASP A06, OWASP A08, PCI-DSS 6.4.3, ISO 27001 A.8.25 <pre><script src="https://cdn.example.com/lib.js" integrity="sha384-..." crossorigin="anonymous"></script></pre>	18/22		

CONTROL • FIX		MET	OWNER	DONE ON
☐	Referrer-Policy missing MINOR • CLEARS 3: OWASP A05, GDPR 32(1)(D), ISO 27001 A.8.26 Referrer-Policy: strict-origin-when-cross-origin	21/22		
☐	No CAA record MINOR • CLEARS 1: GDPR 32(1)(C) xyz.com. CAA 0 issue "letsencrypt.org"	22/22		

A / SCOPE

What this report is — and is not

Evidence about controls you can see from outside; not a certification.

SecureScanr made one live, non-intrusive request to xyz.com and read its response headers, TLS certificate, DNS records, cookies and page markup. Each framework requirement listed here maps to one or more of those technical checks; a requirement is **met** when every mapped check passed, and shows a **gap** when at least one did not.

That makes this a web-layer gap assessment. Compliance with PCI-DSS, GDPR, ISO 27001 or the OWASP Top 10 also depends on organisational, procedural and application-level controls that no external scan can observe — access management, logging, data handling, secure development. "No gaps found" means no web-layer gaps were found, not that the organisation is compliant; "Gaps found" is not a finding of non-compliance. Consult a qualified assessor for a formal determination.

Results reflect the moment of the scan; configuration can change after it.