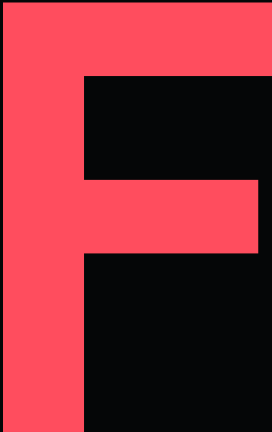


TARGET

www.xyz.com



37 / 100

Twelve findings across five of six groups. One is critical.

HTTP SECURITY HEADERS	TLS / CERTIFICATE	EMAIL & DNS	COOKIES	CROSS-ORIGIN ISOLATION	PAGE INTEGRITY
-35	0	-8	-10	-6	-4

PREPARED FOR	PREPARED BY	ASSESSED	METHOD
XYZ Ltd.	A. Mehta · Independent security consultant	30 Sep 2026	Passive · one live request

www.xyz.com scores 37 — an F. *The one fix marked today would lift it to 57.*

That is a projection, not a promise: the score is additive, so removing these deductions returns exactly their points. 12 findings in all; 6 of the 14 checks passed outright.

WHERE THE POINTS WENT

Starting score	100
01 HTTP security headers	-35
02 TLS / certificate	0
03 Email & DNS	-8
04 Cookies	-10
05 Cross-origin isolation	-6
06 Page integrity	-4
Final score • F	37

FINDINGS BY SEVERITY

1	CRITICAL FINDING Fix today
2	IMPORTANT FINDINGS Fix this week
9	MINOR FINDINGS Fix this month

CONTROL MATRIX • 14 CHECKS

CONTROL	RESULT	PTS	CONTROL	RESULT	PTS
01 CSP	FAIL	-20	08 Fingerprint	PASS	—
02 HSTS	PASS	—	09 TLS	PASS	—
03 X-Frame	PASS	—	10 Email auth	FAIL	-3
04 X-Content-Type	FAIL	-10	11 CAA / DNSSEC	FAIL	-5
05 Referrer	FAIL	-5	12 Cookies	FAIL	-10
06 Permissions	PASS	—	13 Isolation	FAIL	-6
07 CORS	PASS	—	14 Page integrity	FAIL	-4

FIX TODAY

37 → 57

01	Content-Security-Policy	+20
	HTTP SECURITY HEADERS	

HTTP security headers

What the browser is told to enforce.

3 FINDINGS • -35 OF THE 63 POINTS LOST

Content-Security-Policy

CRITICAL**-20**

POINTS

OBSERVED

Not sent

WHY IT MATTERS

Content Security Policy (CSP) tells the browser which sources of content (scripts, images, styles) are allowed to load on your page. Without it, attackers can inject malicious scripts via XSS attacks.

IF EXPLOITED

A successful XSS attack lets attackers steal session tokens, log keystrokes, redirect users, and exfiltrate data — all invisibly in the background.

FIXMEDIUM EFFORT
HIGH IMPACT

```
Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self'; img-src 'self' data:; font-src 'self'; object-src 'none'; base-uri 'self'; form-action 'self';
```

X-Content-Type-Options

IMPORTANT**-10**

POINTS

OBSERVED

Not sent

WHY IT MATTERS

X-Content-Type-Options with the value 'nosniff' stops browsers from guessing (sniffing) the content type of a response, which can allow attackers to trick browsers into executing files as a different type.

IF EXPLOITED

Browsers may execute uploaded images or text files as scripts, turning a file-upload feature into a remote code execution vector.

FIXLOW EFFORT
MEDIUM IMPACT

```
X-Content-Type-Options: nosniff
```

Referrer-Policy

MINOR

-5

POINTS

OBSERVED

Not sent

WHY IT MATTERS

Referrer-Policy controls how much referrer information is included with requests. Without it, the full URL of your page (including sensitive query parameters) may leak to third-party sites.

IF EXPLOITED

Full page URLs — including session tokens or internal paths in query strings — leak to every analytics or ad service your site loads.

FIX

LOW EFFORT
LOW IMPACT

Referrer-Policy: strict-origin-when-cross-origin

PASSED (6)

✓ Strict-Transport-Security	max-age=15768000
✓ X-Frame-Options	SAMEORIGIN
✓ Permissions-Policy	interest-cohort=()
✓ Access-Control-Allow-Origin	Not sent (normal for most sites)
✓ Server (version disclosure)	BunnyCDN-MU1-1528
✓ X-Powered-By (version disclosure)	Not sent

02 / TLS / CERTIFICATE

TLS / certificate

Whether the connection can be trusted.

0 FINDINGS • NO POINTS LOST

Every check in this group passed.

PASSED (1)

✓ Certificate & protocol	TLSv1.3 • valid 77 more days
--------------------------	------------------------------

Email & DNS

Who can send as you, and who can issue for you.

3 FINDINGS • -8 OF THE 63 POINTS LOST

DMARC

IMPORTANT**-3**

POINTS

OBSERVED

v=DMARC1; p=none; rua=mailto:dmARC@xyz.com;

WHY IT MATTERS

DMARC tells receiving mail servers what to do with emails that fail SPF/DKIM checks.

IF EXPLOITED

p=none only monitors — spoofed emails reach inboxes unchecked while you receive reports that rarely lead to action.

FIX

LOW EFFORT
MEDIUM IMPACT

Update to p=reject or p=quarantine: v=DMARC1; p=reject;
rua=mailto:dmARC@xyz.com; pct=100

DNSSEC

MINOR**-3**

POINTS

OBSERVED

Not enabled

WHY IT MATTERS

DNSSEC is not enabled. DNSSEC adds cryptographic signatures to DNS records, protecting against cache poisoning attacks where attackers redirect your domain to malicious servers.

IF EXPLOITED

DNS cache poisoning can silently redirect your domain to attacker-controlled servers, intercepting all user traffic without their knowledge.

FIX

LOW EFFORT
MEDIUM IMPACT

Enable DNSSEC at your domain registrar or DNS provider for xyz.com.

CAA MINOR

-2
POINTS

OBSERVED	No record published
WHY IT MATTERS	No CAA records found. CAA (Certification Authority Authorization) DNS records restrict which CAs can issue TLS certificates for your domain, preventing unauthorised certificate issuance.
IF EXPLOITED	Without CAA records, any trusted Certificate Authority can issue a certificate for your domain — enabling MITM attacks if a CA's infrastructure is compromised.
FIX LOW EFFORT MEDIUM IMPACT	0 issue "letsencrypt.org" (add as CAA record on xyz.com)

PASSED (2)

✓ SPF	v=spf1 ip4:192.0.2.14 ip4:198.51.100.5 ip4:198.51.100.76 ip6:2001:db8:400::1001 ip6:2001:d
✓ DKIM	v=DKIM1; h=sha256; k=rsa; s=email; p=i9DYdWQZ6iKXpndux/xaPsQFQi6wJbp+G0g2ckzI/kIa6j5TY6HWY

04 / COOKIES

Cookies

What the site stores in every visitor's browser.

1 FINDING · -10 OF THE 63 POINTS LOST

Cookie: last_visit MINOR

-10
POINTS

OBSERVED	Secure: no · HttpOnly: no · SameSite: not set
WHY IT MATTERS	Missing Secure flag — cookie transmitted over HTTP (interception risk); Missing HttpOnly flag — readable by JavaScript (XSS escalation risk); SameSite=None or Missing — cookie sent with cross-site requests (CSRF risk; informational, no score impact)
IF EXPLOITED	Cookie can be stolen over plain HTTP and read by injected JavaScript — both network and XSS attackers can hijack this session.
FIX LOW EFFORT MEDIUM IMPACT	Set-Cookie: last_visit=<value>; Path=/; Secure; HttpOnly; SameSite=Lax

Cross-origin isolation

How much other sites can reach into this one.

3 FINDINGS • -6 OF THE 63 POINTS LOST

Cross-Origin-Opener-Policy

MINOR**-2**

POINTS

OBSERVED

Not sent

WHY IT MATTERS

COOP prevents other sites from getting a window reference to this page, blocking cross-origin attacks like Spectre and clickjacking via window handles.

IF EXPLOITED

Pages opened as pop-ups retain a window reference to your page, enabling cross-origin DOM probing and Spectre-class timing attacks.

FIX

LOW EFFORT
MEDIUM IMPACT

Cross-Origin-Opener-Policy: same-origin

Cross-Origin-Embedder-Policy

MINOR**-2**

POINTS

OBSERVED

Not sent

WHY IT MATTERS

COEP prevents the page from loading cross-origin resources that don't grant explicit permission, required to enable SharedArrayBuffer and high-resolution timers.

IF EXPLOITED

Cross-origin isolation is disabled — your page cannot use SharedArrayBuffer and remains exposed to Spectre hardware timing side-channels.

FIX

LOW EFFORT
MEDIUM IMPACT

Cross-Origin-Embedder-Policy: require-corp

Cross-Origin-Resource-Policy

MINOR

-2

POINTS

OBSERVED	Not sent
WHY IT MATTERS	CORP tells browsers to block no-cors cross-origin requests to this resource, preventing cross-origin data leaks via or <script> tags.
IF EXPLOITED	Other sites can embed your resources and infer their content through timing side-channel measurements, leaking sensitive data.
FIX LOW EFFORT MEDIUM IMPACT	Cross-Origin-Resource-Policy: same-origin

06 / PAGE INTEGRITY

Page integrity

Whether the page loads only what it means to.

2 FINDINGS · -4 OF THE 63 POINTS LOST

Subresource Integrity

MINOR

-2

POINTS

OBSERVED	<code>https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js</code>
WHY IT MATTERS	1 external script/stylesheet is loaded without Subresource Integrity (SRI) checks. An attacker who compromises the CDN could inject malicious code.
FIX LOW EFFORT MEDIUM IMPACT	Pin each external script and stylesheet to a hash: <pre><script src="https://cdn.example.com/lib.js" integrity="sha384-..." crossorigin="anonymous"></script></pre>

Base tag

MINOR

-2

POINTS

OBSERVED	<code><base href="https://www.xyz.com/index.html"></code>
WHY IT MATTERS	A <base> tag is present. If an attacker can inject arbitrary HTML, they can override the base URL and redirect all relative links to a malicious domain (base tag hijacking).
FIX LOW EFFORT LOW IMPACT	Remove the <base> tag and use root-relative URLs (/path), so injected HTML cannot repoint every relative link on the page.

PASSED (1)

✓ Mixed content

None found

07 / REMEDIATION PLAN

The plan

Work down the list; each tier's projected score assumes the tiers above it are done.

Fix today

SCORE AFTER THIS TIER 57 • D

FINDING	PTS	OWNER	DONE ON
☐ Content-Security-Policy HTTP SECURITY HEADERS • MEDIUM EFFORT	+20		

Fix this week

SCORE AFTER THIS TIER 70 • B

FINDING	PTS	OWNER	DONE ON
☐ X-Content-Type-Options HTTP SECURITY HEADERS • LOW EFFORT	+10		
☐ DMARC EMAIL & DNS • LOW EFFORT	+3		

Fix this month

SCORE AFTER THIS TIER 100 • A+

FINDING	PTS	OWNER	DONE ON
☐ Cookie: last_visit COOKIES • LOW EFFORT	+10		
☐ Referrer-Policy HTTP SECURITY HEADERS • LOW EFFORT	+5		
☐ DNSSEC EMAIL & DNS • LOW EFFORT	+3		
☐ CAA EMAIL & DNS • LOW EFFORT	+2		
☐ Cross-Origin-Opener-Policy CROSS-ORIGIN ISOLATION • LOW EFFORT	+2		
☐ Cross-Origin-Embedder-Policy CROSS-ORIGIN ISOLATION • LOW EFFORT	+2		

FINDING	PTS	OWNER	DONE ON
☐ Cross-Origin-Resource-Policy CROSS-ORIGIN ISOLATION • LOW EFFORT	+2		
☐ Subresource Integrity PAGE INTEGRITY • LOW EFFORT	+2		
☐ Base tag PAGE INTEGRITY • LOW EFFORT	+2		

A / APPENDIX

Technical record

The raw values behind the findings, as observed at the time of the scan.

CERTIFICATE & CONNECTION

SUBJECT	www.xyz.com
ISSUER	YE1
VALID	2026-09-17 → 2026-12-16 (77 days left)
NAMES (SAN)	www.xyz.com
PROTOCOL / CIPHER	TLSv1.3 • TLS_AES_256_GCM_SHA384 • 256-bit

DNS RECORDS

SPF	v=spf1 ip4:192.0.2.14 ip4:198.51.100.5 ip4:198.51.100.76 ip6:2001:db8:400::1001 ip6:2001:db8::1102 ip4:192.0.2.87 ip6:2001:db8:416d::1 ~all
DMARC	v=DMARC1; p=none; rua=mailto:dmarc@xyz.com;
DKIM	selector mail: v=DKIM1; h=sha256; k=rsa; s=email; p=i9DYdWQZ6iKXpndux/xaPsQFQi6wJbp+G0g2ckzI/kIaGj5TY6HWY81H5BV6s8+V...
CAA	None published
DNSSEC	Not enabled

COOKIES SET ON THE RESPONSE

LAST_VISIT	domain .xyz.com • Secure no • HttpOnly no • SameSite not set • expires Thu, 30 Sep 2027 11:00:31 GMT
------------	--

STACK & DELIVERY

SERVER HEADER	BunnyCDN-MU1-1528
CDN / PROXY	Not detected
IP ADDRESS	203.0.113.15
REDIRECT CHAIN	https://www.xyz.com/
EXTERNAL DOMAINS	cdn.jsdelivr.net

METHODOLOGY & SCOPE

SecureScanr made one live, non-intrusive request to the target — the same response a visitor receives — and read its headers, certificate, DNS records, cookies and page markup. Nothing was attacked, fuzzed or brute-forced. Every site starts at 100; each failed check deducts the points shown, and the total is floored at 0. The full rubric is published at [securescanr.com/methodology](https://www.securescanr.com/methodology).

A+ 90-100 A 80-89 B 70-79 C 60-69 D 50-59 F <50

This is an automated external assessment of configuration. It does not test application logic, authentication, or server-side code, and it does not replace a manual penetration test. Results reflect the moment of the scan; configuration can change after it.