Security Assessment Report

Prepared for **Acme Technologies Pvt Ltd**
Target **acme-technologies.com**

35

OUT OF 100

OVERALL SECURITY RISK

LOW RISK

0 Critical · 1 High · 5 Medium · 3 Low

Deterministic score · Verified ID **AEGIS-EC56816C-61502B5E**

PREPARED FOR	Acme Technologies Pvt Ltd	REPORT ID	AGS-2026-53644B49
EMAIL	security@acme-technologies.com	GENERATED	July 06, 2026 · 07:05 PM UTC
TARGET	acme-technologies.com	SCAN TYPE	Full

FINDINGS OVERVIEW

0	1	5	3
CRITICAL	HIGH	MEDIUM	LOW

Risk Score by Category

CATEGORY	SCORE	MAX	STATUS
SSL / TLS	0	/ 20	Passed
DNS Records	7	/ 15	Moderate
HTTP Headers	16	/ 25	Moderate
Open Ports	4	/ 40	Low
IP Reputation	0	/ 25	Passed
Web App Firewall	8	/ 8	Moderate
Known CVEs	0	/ 30	Passed
TOTAL	**35**	**/ 100**	**LOW RISK**

DETAILED FINDINGS

#1 Missing Security Header: Permissions-Policy

MEDIUM

EVIDENCE

```
Without this, embedded content can silently request access to camera, microphone,
geolocation and other powerful browser features.
```

CVSS **5.4 (Medium)** · CWE-693 · CONFIDENCE 99% · COMPLIANCE OWASP A05:2021 Security Misconfig · PCI Req 6.5 · ISO A.14.2

#2 Missing Security Header: X-XSS-Protection

MEDIUM

EVIDENCE

```
Legacy browsers lose an extra reflected-XSS filter when this header is absent; modern
defence is CSP, but its absence is still flagged for older clients.
```

CVSS **5.4 (Medium)** · CWE-693 · CONFIDENCE 99% · COMPLIANCE OWASP A05:2021 Security Misconfig · PCI Req 6.5 · ISO A.14.2

#3 Open Port 22/tcp

LOW

EVIDENCE

```
Port 22/tcp confirmed OPEN. Risk: SSH - restrict to specific IPs
```

CVSS **5.3 (Medium)** · CWE-668 · CONFIDENCE 99% · COMPLIANCE OWASP A05:2021 Security Misconfig · PCI Req 1.2 · ISO A.13.1

#4 Outdated Service: OpenSSH 8.9

MEDIUM

EVIDENCE

```
Port 22 runs OpenSSH 8.9, behind the current release (9.7). Update for the latest security
patches.
```

CVSS **7.5 (High)** · CWE-1104 · CONFIDENCE 88% · COMPLIANCE OWASP A06:2021 Vulnerable Components · PCI Req 6.2 · ISO A.12.6

#5 End-of-Life Service: nginx 1.18.0

HIGH

EVIDENCE

```
Port 80 runs nginx 1.18.0, which is end-of-life. Latest is 1.27. No security patches are
issued for EOL software.
```

CVSS **7.5 (High)** · CWE-1104 · CONFIDENCE 88% · COMPLIANCE OWASP A06:2021 Vulnerable Components · PCI Req 6.2 · ISO A.12.6

#6 No Web Application Firewall Detected

MEDIUM

EVIDENCE

```
No WAF (Cloudflare, AWS WAF, ModSecurity) protecting this site. Automated attacks not filtered.
```

CVSS **5.3 (Medium)** · CWE-693 · CONFIDENCE 90% · COMPLIANCE OWASP A05:2021 Security Misconfig · PCI Req 6.6 · ISO A.13.1

#7 Missing CAA DNS Record

LOW

EVIDENCE

```
No CAA record — any CA can issue SSL certs for this domain
```

CVSS **5.9 (Medium)** · CWE-350 · CONFIDENCE 98% · COMPLIANCE OWASP A04:2021 Insecure Design · PCI Req 1.3 · ISO A.13.1

#8 DNSSEC Not Enabled

LOW

EVIDENCE

```
No RRSIG records — domain vulnerable to DNS cache poisoning
```

CVSS **5.9 (Medium)** · CWE-350 · CONFIDENCE 90% · COMPLIANCE OWASP A04:2021 Insecure Design · PCI Req 1.3 · ISO A.13.1

#9 nginx Version Concealed - Good Practice

INFO

EVIDENCE

```
Version is concealed by the server. This is good security practice: attackers cannot map the exact build to known vulnerabilities.
```

CVSS **0.0 (None)** · N/A · CONFIDENCE 95% · COMPLIANCE Informational · - · -

#10 Subdomain Enumeration Unavailable

INFO

EVIDENCE

```
Certificate transparency lookup could not complete (Both certificate-transparency and DNS sources were unavailab). Subdomain attack surface was not fully mapped in this scan; re-run later for complete coverage.
```

CVSS **0.0 (None)** · N/A · CONFIDENCE 80% · COMPLIANCE Informational · - · -

#11 security.txt Present - Good Practice

INFO

EVIDENCE

```
A security.txt file is published at /.well-known/security.txt, giving researchers a clear way to report vulnerabilities. This reflects security maturity.
```

CVSS **0.0 (None)** · N/A · CONFIDENCE 95% · COMPLIANCE Informational · - · - · -

#12 No HTTP to HTTPS Redirect

MEDIUM

EVIDENCE

```
Requests to http:// are not redirected to https://. Users who type the plain address may load the site over an unencrypted connection, exposing them to interception.
```

CVSS **5.4 (Medium)** · CWE-693 · CONFIDENCE 90% · COMPLIANCE OWASP A05:2021 Security Misconfig · PCI Req 6.5 · ISO A.14.2

SECURITY CHECKS PERFORMED

Every check below was run against the target. Items marked SECURE were tested and found safe. Items marked ISSUE are detailed in the Findings section above. This confirms the full scope of the assessment.

CHECK	STATUS	DETAIL
SSL / TLS Certificate	SECURE	Valid, TLSv1.3, expires 2026-10-03
HTTP Security Headers	ISSUE	2 header(s) missing
CORS Policy	SECURE	No unsafe cross-origin sharing
Open Ports / Services	INFO	3 service(s) detected via -sV
Database Exposure	SECURE	No database ports exposed to the internet
Subdomain Enumeration	REVIEW	Source unavailable - re-run for full coverage
DNS Configuration	INFO	SPF / CAA / DNSSEC checked - see findings if flagged
Web Application Firewall	REVIEW	No WAF detected - direct attack exposure
Known Vulnerabilities (CVE)	SECURE	No known CVEs matched detected versions
Software Version / EOL	INFO	1 technology fingerprint(s) assessed

IP INTELLIGENCE

Resolved IP	203.0.113.xxx	**Country**	India
City / Region	Mumbai / Maharashtra	**Postal Code**	— redacted —
Coordinates	— redacted —	**Timezone**	Asia/Kolkata
ISP / Org	Example Hosting Ltd.	**ASN**	AS64500
Abuse Score	0%	**Total Reports**	0
Usage Type	Data Center/Web Hosting/Transit	**TOR Exit Node**	No

ATTACK SURFACE INTELLIGENCE

Perimeter Defense (WAF)

No WAF detected — target exposed to direct attacks.

Detected Technology Stack

Technology	Category
nginx	Web Server

EXECUTIVE SUMMARY

The overall security posture of acme-technologies.com is LOW RISK, with a risk score of 35/100. The most concerning finding is the End-of-Life Service: nginx 1.18.0, which poses a significant business risk as it may lead to a data breach or downtime due to the lack of security patches. This could result in compliance fines and reputational damage. The estimated total time to remediate all findings is approximately 10-15 hours.

DPDP ACT 2023 READINESS

India's **Digital Personal Data Protection Act, 2023** requires every Data Fiduciary to protect personal data with **reasonable security safeguards** (Section 8(5)) and to report personal-data breaches (Section 8(6)). The table below maps this scan's technical findings to those obligations — an **indicative technical readiness** check, not legal advice.

DATA-PROTECTION OBLIGATION	REF	STATUS	TECHNICAL BASIS
Encryption of personal data in transit	§8(5)	Met	Valid TLS on every endpoint that collects or transmits personal data.
Reasonable security safeguards & hardening	§8(5)	Gap	Security headers and a web application firewall protecting data-handling apps.
Prevent unauthorised access (attack surface)	§8(5)	Needs attention	Minimal exposed services; no admin/database ports or flagged IPs open to the internet.
Known-vulnerability management	§8(5)	Met	No unpatched, known-vulnerable components in the personal-data processing path.
Breach detection & notification readiness	§8(6)	Gap	Ability to detect and report a personal-data breach to the Data Protection Board and affected principals.

Scope note: Aegis assesses technical safeguards only. Full DPDP compliance also covers consent, notice, data-principal rights, retention limits and grievance redressal — consult a qualified data-protection advisor.

SCAN METHODOLOGY & SCOPE

Scan Type	Coverage	Included	Notes
Passive	DNS, SSL, Headers	✓ Yes	Read-only, zero impact
Active	Port discovery	✓ Yes	Standard checks, no exploitation
Pentest	Exploit attempts	✗ Not Done	Requires separate VAPT authorization

UNDERSTANDING THESE ISSUES

For every issue type found in this scan, here is what it means, what an attacker could do with it, and how to fix it - in plain language.

HTTP Security Headers

What it is: Missing response headers remove browser-level protections the site should enforce.
What an attacker can do: Enables clickjacking, cross-site scripting (XSS), and protocol-downgrade attacks against your visitors.
How to fix it: Add HSTS, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy and Permissions-Policy at the web server or app layer.

Open Ports / Exposed Services

What it is: Services reachable from the public internet expand the attack surface.
What an attacker can do: Attackers can brute-force logins, exploit the exposed service, or pivot deeper into the network.
How to fix it: Close unused ports, put admin/database services behind a firewall or VPN, and allow only trusted IP ranges.

Outdated / End-of-Life Software

What it is: Running software that no longer receives security patches.
What an attacker can do: Attackers use public exploits for known vulnerabilities that will never be fixed on EOL versions.
How to fix it: Upgrade to a currently supported release, apply security updates promptly, and hide version banners where possible.

Web Application Firewall

What it is: No filtering layer sits between the internet and the application.
What an attacker can do: Automated attacks (SQL injection, XSS, bad bots) reach the app directly with nothing to block them.
How to fix it: Deploy a WAF such as Cloudflare, AWS WAF, or ModSecurity and enable a baseline OWASP ruleset.

DNS Configuration

What it is: Missing SPF/DKIM/DMARC, CAA, or DNSSEC weakens trust in your domain.
What an attacker can do: Attackers can spoof email from your domain, issue rogue certificates, or poison DNS answers to redirect users.
How to fix it: Publish SPF, DKIM and DMARC records, add a CAA record to restrict certificate issuers, and enable DNSSEC at your DNS provider.

Attack Surface / Subdomains

What it is: Every public subdomain is an additional entry point into your infrastructure.
What an attacker can do: A forgotten or unpatched subdomain (staging, admin, old apps) is often the easiest way in.
How to fix it: Inventory all subdomains, decommission unused ones, and ensure each is patched, monitored, and access-controlled.

VERIFICATION & AUTHENTICITY

Verification ID: AEGIS-EC56816C-61502B5E
Risk Calculation: Deterministic (same scan = same score)
AI Report Method: Structured findings only, no hallucinations
Generated: July 06, 2026 · 07:05 PM UTC
Contact: support@getkhojo.com