Penetration Test Scope - XDC Gateway

Penetration Test Scope & Summary

Organization: XDC Gateway (xdcrpc.com)
Test Period: February 2026
Testing Firm: Independent Third-Party Security Consultants
Report Version: 1.0
Classification: Restricted — Summary Only

Executive Summary

XDC Gateway commissioned a full-scope penetration test in February 2026. The assessment identified 3 medium and 5 low severity findings. Zero critical or high severity vulnerabilities were found. All identified issues have been remediated.

Overall Risk Rating: LOW

Severity	Count	Status
Critical	0	N/A
High	0	N/A
Medium	3	Remediated
Low	5	Remediated
Informational	4	Acknowledged

Test Scope

In-Scope Assets

Web Applications

- `platform.xdcrpc.com` — Main customer dashboard (Next.js)
- `api.xdcrpc.com` — REST API (Node.js/Fastify)
- `trust.xdcrpc.com` — Trust Center (Next.js)
- `docs.xdcrpc.com` — Documentation portal
- `/api/*` routes including authentication, billing, RPC proxy

Network

- Production server external attack surface
- Nginx reverse proxy configuration
- TLS/SSL configuration across all domains
- Firewall rule review (external perspective)
- DNS configuration and zone transfer attempts

APIs

- All public REST API endpoints
- WebSocket endpoints (`wss://rpc.xdcrpc.com`)
- Rate limiting bypass attempts
- Authentication and authorization flows
- API key security and entropy validation

Mobile/SDK (Limited)

- Public SDK package review (npm package analysis)
- SDK authentication implementation review

Out-of-Scope

- Physical infrastructure (co-location facilities)
- Denial of Service (DoS) testing
- Social engineering
- Customer data or accounts (synthetic test accounts used)
- Third-party services (Cloudflare, Hetzner internal networks)
- Blockchain node consensus manipulation

Methodology

Testing was conducted using a combination of:

- **OWASP Testing Guide v4.2** methodology for web application assessment
- **PTES (Penetration Testing Execution Standard)** for network testing
- **OWASP API Security Top 10** for API assessment
- Manual testing combined with automated scanning

Phases

1. **Reconnaissance** — Passive and active information gathering
2. **Scanning** — Service enumeration, vulnerability scanning
3. **Exploitation** — Controlled exploitation of identified weaknesses
4. **Post-Exploitation** — Lateral movement assessment (limited)
5. **Reporting** — Findings documentation and remediation guidance

---

Key Findings Summary

Medium Severity (All Remediated)

M1 — Missing HSTS Preload on Subdomains
Some secondary subdomains were missing HTTP Strict Transport Security preload headers. Resolved by adding `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload` to Nginx configuration.

M2 — API Rate Limiting Bypass via Header Manipulation
Using certain IP-spoofing headers (X-Forwarded-For), automated rate limit detection could be partially bypassed on API endpoints. Resolved by stripping spoofable headers at the Cloudflare edge and trusting only known proxy IPs.

M3 — Session Token Entropy Below Recommendation
API session tokens used 128-bit entropy which, while secure, was below the recommended 256-bit for enterprise-grade services. Token generation updated to use 256-bit cryptographically random values.

Low Severity (All Remediated)

L1 — Verbose Error Messages on API Endpoints
Some API error responses included stack traces in non-production configurations that were inadvertently reachable. Resolved with environment-aware error filtering.

L2 — DNS Zone Transfer Not Disabled
AXFR zone transfer was responding to external queries. Configured to deny external zone transfer requests.

L3 — Outdated npm Dependencies (Non-Critical)
14 npm packages were more than 2 major versions behind. Updated and locked dependency ranges.

L4 — Missing CSP on Trust Center Subdomain
Content-Security-Policy header was absent from the initial trust center deployment. Added comprehensive CSP headers.

L5 — WebSocket Origin Validation
WebSocket connections did not validate Origin header. Added origin allowlist validation to WebSocket upgrade handler.

Informational

- Server software version exposed in `Server` response header (Nginx) — accepted risk
- Default Nginx page accessible on non-vhosted IP — accepted risk
- SSL certificate transparency logs disclosed internal subdomain names — accepted risk
- `robots.txt` disallowed paths disclosed admin route names — low risk, accepted

---

Remediation Status

All medium and low severity findings have been fully remediated as of March 2026. Informational findings have been reviewed and accepted with documented rationale.

Remediation verification testing was conducted by the same firm on March 8, 2026. All fixes confirmed.

Re-Test Schedule

- **Next Annual Pentest:** February 2027
- **Targeted re-tests:** Following major architectural changes

- **Continuous scanning:** Automated DAST scanning via CI/CD pipeline

---

Contact

For questions about this assessment or to request the full report under NDA:

security@xdcrpc.com

This is a summary document. The full penetration test report is available to enterprise customers under NDA. Contact enterprise@xdcrpc.com for access.