Security Testing Statement

Infrastructure Security & Application Security Practices

Version: 1.0 **Date:** April 2026 **Classification:** Public

Executive Summary

ScamZero operates on a **serverless architecture** built entirely on Cloudflare's enterprise platform. This fundamentally changes how security testing applies to our infrastructure.

- No servers, network perimeter, or physical infrastructure to pen test
- Cloudflare conducts regular penetration testing (covered under SOC 2 Type II)
- ScamZero focuses on application-layer security practices
- All infrastructure services (Workers, D1, R2) are SOC 2 certified

Serverless Architecture Overview

What "Serverless" Means for Security Testing

Traditional penetration testing is designed for environments with servers, networks, and physical infrastructure. ScamZero's architecture has none of these:

Traditional Infrastructure	ScamZero (Serverless)
Physical/virtual servers to scan	No servers - code runs on Cloudflare's edge
Network perimeter to test	No network - requests route through Cloudflare's anycast
Database servers to secure	D1 is managed SQLite - no direct access
File servers and storage	R2 object storage - access-controlled by Cloudflare
OS-level vulnerabilities	No OS - Workers run in V8 isolates

> **Key Insight**
>
> There is nothing to "penetrate" in the traditional sense. Security responsibility is shared between Cloudflare (infrastructure) and ScamZero (application code).

Infrastructure Security (Cloudflare's Responsibility)

Cloudflare's Security Testing

Cloudflare maintains rigorous security testing for all services ScamZero uses:

Service	ScamZero Usage	Cloudflare Certifications
Workers	Application logic, API endpoints	SOC 2 Type II, ISO 27001
D1 Database	Data storage	SOC 2 Type II, ISO 27001
R2 Storage	File and image storage	SOC 2 Type II, ISO 27001
Pages	Static website hosting	SOC 2 Type II, ISO 27001
DNS	Domain routing	SOC 2 Type II, ISO 27001

What Cloudflare's SOC 2 Covers

- ✓ Regular penetration testing by independent third parties
- ✓ Continuous vulnerability scanning
- ✓ Bug bounty program
- ✓ Security incident response procedures
- ✓ Physical security of data centers
- ✓ Employee background checks and security training

Cloudflare's SOC 2 Type II report is available upon request under NDA.

Application Security (ScamZero's Responsibility)

ScamZero's Application-Layer Security Practices

While Cloudflare secures the infrastructure, ScamZero is responsible for application code security:

Secure Development Practices

- ✓ **Input Validation:** All user inputs are validated and sanitized
- ✓ **Parameterized Queries:** D1 database queries use parameterized statements to prevent SQL injection
- ✓ **Output Encoding:** All outputs are properly encoded to prevent XSS
- ✓ **Authentication:** Session management follows OWASP best practices
- ✓ **Authorization:** Role-based access control for admin functions

OWASP Top 10 Coverage

OWASP Category	Mitigation
A01: Broken Access Control	Role-based permissions, session validation
A02: Cryptographic Failures	TLS 1.3 enforced, no sensitive data stored
A03: Injection	Parameterized queries, input sanitization
A04: Insecure Design	Minimal data collection, ephemeral processing
A05: Security Misconfiguration	Infrastructure-as-code, no exposed admin interfaces
A06: Vulnerable Components	Minimal dependencies, regular updates
A07: Auth Failures	Secure session handling, no credential storage
A08: Data Integrity Failures	Version-controlled deployments, signed releases
A09: Logging Failures	Cloudflare logging, audit trails for admin actions
A10: SSRF	No server-side URL fetching of user input

Code Review Process

- All code changes reviewed before deployment
- Security-focused review for authentication and data handling code
- Version control with full audit trail (Git)

Future Security Assessment Plans

As ScamZero scales, we plan to engage third-party security firms for:

- **Application Security Assessment:** OWASP-focused testing against our API endpoints
- **Code Review:** Third-party review of authentication and data handling logic
- **Bug Bounty Program:** Consideration for responsible disclosure program

These assessments will focus on application-layer security, as infrastructure security is already covered by Cloudflare's certifications.

Summary

Q: Does ScamZero conduct penetration testing?

Our infrastructure runs on Cloudflare's serverless platform, which Cloudflare penetration tests as part of their SOC 2 Type II compliance. For our application layer, we follow secure development practices and OWASP guidelines. Traditional network penetration testing is not applicable to our serverless architecture.

Cloudflare's SOC 2 report (available under NDA) documents their security testing program covering all infrastructure services ScamZero uses.

Questions?

For security inquiries, contact security@scamzero.com