# API SECURITY AUDIT CHECKLIST

SECURE APIS. PROTECT DATA. BUILD TRUST.



By: Dr. Nath Alagbe

# API Security Audit Checklist

## Introduction to API Security Audit

In today's interconnected digital landscape, Application Programming Interfaces (APIs) serve as the backbone of modern software architecture, enabling seamless communication between disparate systems. However, this connectivity also introduces significant security risks. An API Security Audit is a systematic evaluation of an organization's API ecosystem to identify vulnerabilities, ensure compliance with industry standards, and verify the effectiveness of security controls.

### What API Security Audit Entails

A professional API security audit goes beyond simple vulnerability scanning. It involves a deep dive into the design, implementation, and operational aspects of APIs. Key areas of focus include:

- ✓ Authentication and Authorization mechanisms
- ✓ Data protection and privacy controls
- ✓ Infrastructure security and configuration
- ✓ Inventory management and governance
- ✓ Business logic and abuse protection

**Author: Dr. Nath Alagbe**; CISA, CISM, CISSP, CRISC, CCAK, AAIA, AAISM, CCEP, CFE, FCA, FCTI, FFAR, MBA, PhD

— Dr. Nath Alagbe —

## Domain 1: API Governance and Inventory

| Control Areas | Risk Addressed | Control Objective | Test Steps | Evidence Required | Framework |
|---|---|---|---|---|---|
| **API Inventory Management** | Shadow/Zombie APIs | Maintain a complete list of all APIs | Review API registry vs traffic logs | API Inventory list, Traffic logs | NIST SP 800-228 |
| **API Documentation** | Misuse due to lack of clarity | Ensure all APIs have up-to-date documentation | Inspect documentation for completeness | OpenAPI specs | OWASP API10:2023 |
| **API Lifecycle Management** | Insecure deprecated versions | Formal process for design, deploy, and retire | Review lifecycle policy and retirement logs | Lifecycle policy, Change logs | ISO 27001 |
| **Third-Party API Risk Management** | Supply chain attacks | Assess the security of external APIs | Review vendor assessment reports | Vendor risk assessments | NIST CSF |
| **API Security Policy** | Inconsistent security controls | Establish formal API security standards | Verify the existence and communication of policy | API Security Policy document | CIS Controls |

| | | | | | |
|---|---|---|---|---|---|
| **Data Classification for APIs** | Sensitive data exposure | Classify data handled by each API | Review data classification tags in the API registry | Data classification matrix | GDPR/CCPA |
| **API Ownership and Accountability** | Unmanaged endpoints | Assign owners to every API | Check the owner field in the API inventory | Ownership records | COBIT |
| **Compliance Alignment** | Regulatory fines | Map APIs to regulatory requirements | Review the compliance mapping document | Compliance report | PCI DSS |
| **API Security Training** | Developer errors | Train developers on API security best practices | Review training attendance logs | Training certificates/logs | OWASP |
| **Incident Response for APIs** | Delayed breach detection | Specific IR plan for API incidents | Review IR plan for API-specific scenarios | IR Plan, Tabletop exercise results | NIST SP 800-61 |

## Domain 2: Authentication and Authorization

| Control Areas | Risk Addressed | Control Objective | Test Steps | Evidence Required | Framework |
|---|---|---|---|---|---|
| **Broken Object Level Authorization (BOLA)** | Unauthorized data access | Ensure users only access their own objects | Attempt to access the object ID of another user | Test scripts, Burp Suite logs | OWASP API1:2023 |
| **Broken Authentication** | Account takeover | Secure authentication mechanisms | Check for weak passwords, lack of MFA | Auth config files | OWASP API2:2023 |
| **Broken Object Property Level Authorization** | Sensitive property exposure | Restrict access to sensitive object properties | Check if unauthorized users can read/write sensitive fields | API response logs | OWASP API3:2023 |
| **Unrestricted Resource Consumption** | DoS | Implement rate limiting and quotas | Perform load testing/stress testing | Rate limit config, Load test report | OWASP API4:2023 |
| **Broken Function Level Authorization** | Privilege escalation | Restrict administrative functions | Attempt to call admin endpoints with user token | Access logs, Test results | OWASP API5:2023 |
| **Unrestricted Access to Sensitive Business Flows** | Business logic abuse | Protect sensitive flows | Analyze flow for automation/abuse potential | Business logic review notes | OWASP API6:2023 |
| **Server Side Request Forgery (SSRF)** | Internal network scanning | Prevent APIs from making arbitrary requests | Inject internal URLs into API parameters | Test logs | OWASP API7:2023 |
| **Security Misconfiguration** | Exposing internal details | Secure API infrastructure and | Scan for missing security headers | Scan reports | OWASP API8:2023 |

| | | | | | |
|---|---|---|---|---|---|
| | | headers | | | |
| **Improper Inventory Management** | Exposing old versions | Secure all versions and environments | Check for exposed staging/dev environments | Environment list, DNS records | OWASP API9:2023 |
| **Unsafe Consumption of APIs** | Trusting third-party data | Sanitize data from external APIs | Review code for third-party data handling | Code review reports | OWASP API10:2023 |

## Domain 3: Data Protection and Privacy

| Control Areas | Risk Addressed | Control Objective | Test Steps | Evidence Required | Framework |
|---|---|---|---|---|---|
| **Encryption in Transit** | MitM attacks | Enforce TLS 1.2+ | Check SSL/TLS configuration | SSL Labs report | NIST SP 800-52 |
| **Encryption at Rest** | Data breach from storage | Encrypt sensitive API data in DBs | Verify DB encryption settings | DB config screenshots | ISO 27001 |
| **Sensitive Data Masking** | PII exposure in logs | Mask PII in API responses and logs | Inspect logs for cleartext PII | Log samples | GDPR |
| **Token Security (JWT)** | Token theft/forgery | Secure JWT implementation | Decode JWT and check claims/alg | JWT samples | RFC 7519 |
| **API Key Management** | Hardcoded keys | Secure storage and rotation of keys | Scan code for hardcoded keys | Secret scanner results | NIST SP 800-57 |
| **Data Minimization** | Excessive data exposure | Return only necessary fields | Compare API response vs UI requirements | API response samples | Privacy by Design |
| **Error Message Sanitization** | Information leakage | Prevent stack traces in errors | Trigger errors and check responses | Error response samples | OWASP |
| **CORS Configuration** | Cross-origin attacks | Restrict CORS to trusted domains | Check Access-Control-Allow-Origin header | Header logs | W3C CORS |
| **Secure Headers** | Clickjacking/XSS | Implement security headers | Scan API endpoints for headers | Security header check results | OWASP |
| **Data Residency Compliance** | Legal non-compliance | Ensure data stays in required regions | Review data flow diagrams and server locations | Data flow diagrams | GDPR |

## Domain 4: Infrastructure and Operations

| Control Areas | Risk Addressed | Control Objective | Test Steps | Evidence Required | Framework |
|---|---|---|---|---|---|
| **API Gateway Security** | Bypassed controls | Centralize security at the gateway | Verify all traffic goes through gateway | Network diagrams, Gateway config | NIST SP 800-204 |
| **Logging and Monitoring** | Undetected attacks | Log all security-relevant events | Check SIEM for API logs | SIEM dashboard screenshots | NIST SP 800-92 |
| **Rate Limiting and Throttling** | DoS/Brute force | Prevent abuse via request limits | Send high volume of requests | 429 Too Many Requests responses | OWASP |
| **Input Validation** | Injection (SQLi, NoSQLi) | Sanitize all input data | Inject malicious payloads into parameters | Test reports | OWASP ASVS |
| **WAF for APIs** | Web-based attacks | Deploy WAF with API-specific rules | Check WAF logs for blocked API attacks | WAF config/logs | PCI DSS |
| **Patch Management** | Exploited vulnerabilities | Keep API servers and libraries updated | Review patch logs for API infrastructure | Patching reports | NIST SP 800-40 |
| **Secure CI/CD Pipeline** | Insecure code deployment | Integrate security scans in CI/CD | Verify SAST/DAST in pipeline | Pipeline config, Scan results | DevSecOps |
| **DDoS Protection** | Service unavailability | Protect APIs from large-scale DDoS | Review DDoS protection service config | DDoS service contract/config | NIST CSF |
| **Backup and Recovery** | Data loss | Regular backups of API configurations and data | Review backup logs and restore tests | Backup logs, Restore test report | ISO 27001 |
| **Audit Trail Integrity** | Tampered logs | Protect logs from unauthorized modification | Check log file permissions and integrity checks | Log server config | PCI DSS |

***Follow me on:***

📌 Click 👉 ***here*** for my LinkedIn Profile.
📌 Click 👉 ***here*** for CyberVerge's LinkedIn Page
📌 Click 👉 ***here*** & 👉 ***here*** for X Accounts