Web Application & API Security

Methodology and Testing Checklist

Document Version	1.0
Prepared By	Lorikeet Security
Contact	lorikeetsecurity.com

1. Executive Overview

> *A comprehensive assessment framework covering OWASP Top 10, API Security Top 10, business logic, and infrastructure for modern web applications and APIs.*

Lorikeet Security's web application and API penetration testing practice follows a structured, risk-driven methodology aligned to OWASP WSTG v4.2, OWASP API Security Top 10, and applicable compliance frameworks including PCI DSS v4.0, SOC 2, and HIPAA. Assessments cover the full application attack surface from authentication and authorization through injection, business logic, and underlying infrastructure.

All engagements begin with a scoping call to define the application inventory, user roles in scope, and any sensitive areas requiring restricted testing windows. Active testing is conducted in a staging or production environment as agreed, with destructive test cases (e.g., account takeover chains, race conditions) performed during low-traffic windows when production scope is required.

2. Assessment Methodology

> *Three-phase engagement model: Reconnaissance, Active Assessment, and Reporting.*

Phase 1: Scoping and Reconnaissance

Passive and active reconnaissance to establish the complete attack surface prior to any active exploitation attempts. This phase includes technology fingerprinting, endpoint enumeration, authentication flow mapping, and threat modeling against the specific application architecture.

Phase 2: Active Assessment

Testing is organized across eight domains covering authentication, authorization, injection, XSS, business logic, API-specific vectors, and infrastructure. Both manual testing and automated scanning are used; automated results are always manually triaged and verified before inclusion in the report.

Black-box: Black-box testing: no prior access to source code or internal architecture

- Simulates an external attacker with no privileged knowledge

Gray-box: Gray-box testing: authenticated accounts and API documentation provided

- Simulates an authenticated user, insider threat, or compromised account

White-box: White-box testing: full source code, architecture diagrams, and environment access

- Maximum coverage; used for code-assisted testing and compliance reviews

Phase 3: Reporting and Debrief

Formal findings report with CVSS scoring, reproduction steps, and remediation guidance. A debrief session is conducted with the development and security teams to walk through findings and answer questions.

3. Scope of Assessments

> *Standard scope covers the full web application, all API surfaces, authentication infrastructure, and underlying cloud/hosting configuration.*

Component	Scope Details
Web Application	All pages, forms, user flows, file uploads, and client-side logic within the defined application boundary
REST / GraphQL APIs	All API endpoints including versioned, deprecated, and internally consumed endpoints; mobile backend APIs
Authentication System	Login, registration, password reset, MFA, SSO/SAML/OIDC flows, and session management
Authorization Controls	Role-based access control, object-level permissions, and resource ownership enforcement
Third-Party Integrations	OAuth providers, payment gateways, webhooks, and externally called APIs
Infrastructure Surface	TLS/SSL configuration, HTTP headers, DNS, CDN, cloud storage, and subdomains
Business Logic	Transaction workflows, pricing logic, rate limiting, and multi-step process integrity
Mobile APIs	Backend APIs consumed by iOS/Android clients, including certificate pinning bypass where applicable

4. Tools and Techniques

> *A combination of manual testing, commercial tooling, and custom scripts is used across all assessment domains.*

Domain	Tools	Techniques
Reconnaissance	Amass, Subfinder, httpx, Shodan, GAU, waybackurls	Subdomain enumeration, endpoint discovery, JS analysis
Web Proxy / Interception	Burp Suite Pro, ZAP, mitmproxy	Request/response manipulation, active scanning, workflow analysis
Authentication Testing	Custom scripts, jwt_tool, oauth-tester	Token analysis, algorithm confusion, OAuth flow abuse

Domain	Tools	Techniques
Injection Testing	SQLMap, custom payloads, Dalfox (XSS)	SQLi, NoSQLi, SSTI, XXE, SSRF, command injection
API Testing	Postman, Bruno, custom fuzzing scripts, Arjun	Endpoint fuzzing, parameter discovery, verb tampering
Infrastructure	Nmap, testssl.sh, nuclei, trufflehog	TLS audit, header review, CVE scanning, secrets detection
Business Logic	Manual testing with Burp Suite, race condition tooling (Turbo Intruder)	Workflow bypass, race conditions, price manipulation

5. Testing Checklist by Domain

> *Comprehensive test cases across all eight assessment domains. Each mapped to OWASP or applicable compliance standard with risk classification.*

Risk Level Key: Critical = Immediate remediation required | High = Remediate within 30 days | Medium = Remediate within 90 days | Low = Informational

ID	Test Case	Standard	Risk Level
1. Reconnaissance and Enumeration			
REC-01	Enumerate all application endpoints, subdomains, and externally exposed services via passive and active reconnaissance	OWASP WSTG-INFO	**High**
REC-02	Identify technology stack, frameworks, CDN, WAF, and third-party services via fingerprinting and header analysis	OWASP WSTG-INFO-02	**Medium**
REC-03	Enumerate all API endpoints from documentation (Swagger/OpenAPI), JS bundles, and traffic analysis	OWASP API Top 10	**High**
REC-04	Identify all authentication mechanisms, session token patterns, and OAuth/OIDC flows	OWASP WSTG-ATHN	**High**
REC-05	Map content discovery: hidden directories, backup files, admin panels, staging environments, and unlinked endpoints	OWASP WSTG-INFO-04	**High**
REC-06	Review JavaScript source files for hardcoded credentials, API keys, internal endpoints, and sensitive business logic	OWASP WSTG-INFO-05	**Critical**
2. Authentication and Session Management			
AUTH-01	Test for username enumeration via differential responses on login, password reset, and registration flows	OWASP WSTG-ATHN-04	**Medium**
AUTH-02	Assess password policy enforcement: minimum complexity, breach password checks, lockout thresholds	NIST SP 800-63B	**High**
AUTH-03	Test for authentication bypass via parameter manipulation, HTTP method switching, and forced browsing to authenticated pages	OWASP WSTG-ATHN-02	**Critical**
AUTH-04	Evaluate MFA implementation: test for bypass via code reuse, brute force, SIM swap vectors, and fallback mechanism weaknesses	NIST SP 800-63B	**High**

ID	Test Case	Standard	Risk Level
AUTH-05	Inspect session token entropy, predictability, and transmission security; test for session fixation and token leakage in referrer/logs	OWASP WSTG-SESS-01	Critical
AUTH-06	Test session timeout, logout invalidation server-side, and concurrent session handling	OWASP WSTG-SESS-06	High
AUTH-07	Evaluate OAuth 2.0/OIDC implementation: test for open redirect abuse, PKCE enforcement, state parameter CSRF, and token leakage	RFC 6749 / OWASP	Critical
AUTH-08	Assess JWT implementation: test for algorithm confusion (RS256 to HS256), none algorithm acceptance, weak secrets, and claim manipulation	OWASP WSTG-SESS	Critical
3. Authorization and Access Control			
AUTHZ-01	Test for Insecure Direct Object Reference (IDOR): manipulate IDs, GUIDs, and filenames to access other users' resources	OWASP API2 / WSTG-ATHZ	Critical
AUTHZ-02	Test horizontal and vertical privilege escalation across all user roles and permission levels	OWASP WSTG-ATHZ-01	Critical
AUTHZ-03	Assess API endpoint authorization: verify every endpoint enforces object-level and function-level access control independently	OWASP API1 / API5	Critical
AUTHZ-04	Test for mass assignment vulnerabilities: submit undocumented fields in API requests targeting role, admin flags, or pricing	OWASP API6	High
AUTHZ-05	Evaluate path traversal and directory traversal on file access, download, and upload endpoints	OWASP WSTG-ATHZ-01	High
AUTHZ-06	Test CORS configuration: identify overly permissive Access-Control-Allow-Origin policies and credential exposure	OWASP WSTG-SESS-07	High
4. Injection and Input Validation			
INJ-01	Test all input fields and parameters for SQL injection: error-based, blind boolean, time-based, and out-of-band vectors	OWASP A03:2021	Critical
INJ-02	Assess NoSQL injection vectors in MongoDB, Cassandra, and Redis query parameters	OWASP WSTG-INPV-05	Critical
INJ-03	Test for OS command injection in all parameters that interact with system calls, file operations, or shell execution	OWASP WSTG-INPV-12	Critical
INJ-04	Evaluate Server-Side Request Forgery (SSRF) vectors: URL parameters, webhook endpoints, PDF generators, and image fetchers; test for cloud metadata access	OWASP A10:2021	Critical
INJ-05	Test for XML External Entity (XXE) injection in XML parsers, SOAP endpoints, and file upload processors	OWASP A05:2017	High
INJ-06	Assess LDAP, XPath, and SSTI (Server-Side Template Injection) in relevant input contexts	OWASP WSTG-INPV	High
INJ-07	Test for HTTP request smuggling via CL.TE and TE.CL desync in reverse proxy and load balancer configurations	OWASP WSTG-INPV-15	High
INJ-08	Evaluate GraphQL endpoints for introspection exposure, batching abuse, field suggestion leakage, and injection vectors	OWASP API9 / GraphQL Top 10	High

ID	Test Case	Standard	Risk Level
5. Cross-Site Scripting (XSS) and Client-Side Security			
XSS-01	Test all reflection points for reflected, stored, and DOM-based XSS including HTML, attribute, JavaScript, and URL contexts	OWASP A03:2021	High
XSS-02	Assess Content Security Policy (CSP) for bypass opportunities: unsafe-inline, unsafe-eval, wildcard domains, and JSONP endpoints	OWASP WSTG-CLNT-12	High
XSS-03	Test for Cross-Site Request Forgery (CSRF) on all state-changing operations; verify token implementation and SameSite cookie enforcement	OWASP WSTG-SESS-05	High
XSS-04	Evaluate clickjacking exposure via X-Frame-Options and frame-ancestors CSP directives	OWASP WSTG-CLNT-09	Medium
XSS-05	Assess postMessage handlers for origin validation weaknesses and data injection vulnerabilities	OWASP WSTG-CLNT-10	High
XSS-06	Review SubResource Integrity (SRI) enforcement on third-party scripts and CDN resources	OWASP WSTG-CLNT-13	Medium
6. Business Logic and Workflow Testing			
BL-01	Test for price manipulation in e-commerce flows: negative quantities, currency parameter tampering, discount stacking	OWASP WSTG-BUSL	Critical
BL-02	Assess race condition vulnerabilities in financial transactions, coupon redemption, referral systems, and inventory operations	OWASP WSTG-BUSL-09	Critical
BL-03	Test for workflow bypass: skipping multi-step processes, replaying requests, and accessing later stages without completing prerequisites	OWASP WSTG-BUSL-04	High
BL-04	Evaluate rate limiting on all sensitive operations: login, registration, password reset, OTP, and API calls	OWASP API4	High
BL-05	Test file upload functionality for MIME type bypass, malicious file execution, path traversal, and storage location exposure	OWASP WSTG-BUSL-08	High
BL-06	Assess account takeover chains: password reset poisoning, response manipulation, and insecure token handling	OWASP WSTG-ATHN	Critical
7. API-Specific Security Testing			
API-01	Verify API versioning security: test deprecated/legacy API versions for missing security controls present in current versions	OWASP API9	High
API-02	Test for Broken Object Property Level Authorization: selectively expose or modify object properties beyond permitted scope	OWASP API3	Critical
API-03	Assess API key management: test for key exposure in URLs, logs, responses, and lack of key rotation or scoping	OWASP API8	High
API-04	Evaluate REST API for HTTP verb tampering, HTTP method override headers, and unsafe method exposure	OWASP WSTG-INPV-06	Medium
API-05	Test WebSocket endpoints for authentication enforcement, message injection, and cross-site WebSocket hijacking	OWASP WSTG-CLNT-10	High
API-06	Assess gRPC or GraphQL subscription endpoints for authentication, authorization, and resource exhaustion vulnerabilities	OWASP API4	High

ID	Test Case	Standard	Risk Level
API-07	Review API response verbosity: test for excessive data exposure in responses including PII, internal fields, and debug information	OWASP API3	High
8. Infrastructure and Configuration			
INFRA-01	Verify TLS configuration: cipher suite strength, protocol version enforcement (TLS 1.2+ minimum), certificate validity, and HSTS enforcement	PCI DSS 4.2 / NIST	High
INFRA-02	Audit HTTP security headers: HSTS, X-Content-Type-Options, X-Frame-Options, Referrer-Policy, Permissions-Policy	OWASP WSTG-CONF	Medium
INFRA-03	Test for sensitive information disclosure: stack traces, debug endpoints, server version banners, and internal IP addresses	OWASP WSTG-INFO-02	Medium
INFRA-04	Assess cloud storage misconfiguration: publicly accessible S3 buckets, Azure blobs, and GCS buckets containing application data	CIS Benchmarks	Critical
INFRA-05	Evaluate dependency and supply chain risk: test for known CVEs in third-party libraries using SCA tooling	OWASP A06:2021	High
INFRA-06	Test for subdomain takeover on dangling DNS records pointing to deprovisioned cloud resources	OWASP WSTG-CONF	High

6. Compliance Standards Reference

> *Lorikeet Security aligns web and API assessments to the following primary standards and frameworks.*

Standard	Relevance
OWASP Top 10 (2021)	Primary reference for web application vulnerability categories; all findings are mapped to applicable OWASP categories.
OWASP API Security Top 10	Governs API-specific testing coverage including broken object-level authorization, mass assignment, and security misconfiguration.
OWASP WSTG v4.2	Detailed testing methodology and test cases used as the basis for all web application assessment procedures.
NIST SP 800-63B	Authentication and session management standards; applied during MFA, credential, and session token evaluation.
PCI DSS v4.0	Applied for engagements involving cardholder data environments; drives TLS, encryption, logging, and access control requirements.
SOC 2 (CC6-CC9)	Applied for SaaS engagements; maps to logical access, change management, and availability controls.
HIPAA Security Rule	Applied for healthcare applications; drives PHI access control, audit logging, and transmission security requirements.
CIS Benchmarks	Cloud and infrastructure hardening guidance applied during configuration review components of web assessments.

7. Deliverables and Engagement Model

> *Standard deliverables for every web application and API security assessment.*

- **Final Report:** Final penetration test report with executive summary, technical findings (CVSS v3.1), reproduction steps, and remediation roadmap
- **Evidence Package:** Raw evidence package: request/response logs, screenshots, and tool output organized by finding
- **Attestation Letter:** Signed attestation letter confirming scope and testing completion, suitable for auditors and compliance reviewers
- **Debrief Session:** Live debrief session with development and security teams; optional developer-focused walkthrough available
- **Retest:** Optional retest engagement to verify remediation of critical and high findings at no additional cost within 30 days

Typical engagement timelines: 3-5 business days for single web application; 5-10 days for complex multi-service environments with extensive API surfaces. Source-assisted (white-box) reviews typically add 2-3 additional days.