CERT-In Empanelled Since 2008

Web Application Penetration Testing

Platform-driven assessments. AI-validated coverage. Three layers of expert review. The consistency problem, solved.

6,700+	1,000+	150+	2006
ASSESSMENTS	CLIENTS	TEAM	FOUNDED

TRUSTED BY INDIA'S LEADING ENTERPRISES

STEP 01

Scope

We define the testing boundary, assemble your audit team, and set up the environment in Lemon.

STEP 02

Test

8–12 days of deep manual testing, AI-validated coverage, automated scanning, and three-layer QA review.

STEP 03

Deliver

Executive + technical reports with code-level fixes, retesting rounds, and security assessment certificate.

WHAT IS WEB APPLICATION PENETRATION TESTING?

Web application penetration testing (WAPT / VAPT) is a structured security assessment where certified experts simulate real-world cyberattacks against your application — including business logic analysis, authentication testing, and API security — to find exploitable vulnerabilities before attackers do. Required by RBI, SEBI, PCI DSS, ISO 27001, and SOC 2.

Beyond OWASP Top 10

Deep manual testing of business logic vulnerabilities that scanners miss — plus comprehensive automated coverage.

OWASP Top 10

Injection, broken access control, cryptographic failures, SSRF

Business Logic

Workflow manipulation, transaction abuse, multi-step exploits

Auth & SSO

OAuth, SAML, JWT, MFA bypass, session fixation

API Security

REST, GraphQL, WebSocket — OWASP API Top 10

Authorization & IDOR

Privilege escalation across all user roles

Data Protection

Encryption, PII exposure, storage security

File Upload & Input

Command injection, SSRF, unrestricted upload

Config & Infra

Server hardening, TLS, headers, error handling

Download: VAPT RFP Template → . Related: Secure Code Review →

OUR RESEARCH FEATURED IN

Economic Times CSO Online PCWorld Network World Hindustan Times CIO

6,700+ security assessments since 2006

METHODOLOGY

9 steps. Zero guesswork.

Every engagement follows this process through **Lemon**, our proprietary audit management platform.

DISCOVERY

01 Project Initiation & Kickoff
Scope validation, team assembly (L1/L2/L3), environment requirements — managed through Lemon.

02 Intelligent Fingerprinting
Lemon auto-detects tech stack and generates testing workflows from 6,700+ prior assessments.

03 Application Mapping
Deep enumeration of modules, APIs, parameters, and data flows with comprehensive mind maps.

04 AI Coverage Validation
AI cross-references all discovery artifacts to find missed attack surface before testing begins.

TESTING

05 Manual Testing & Business Logic
Thousands of test cases: auth bypass, IDOR, transaction abuse, privilege escalation.

06 Automated Scanning
Controlled scanners via Lemon — scheduled windows, client notifications, correlated results.

07 AI-Augmented Validation
AI recommends additional attacks, validates reproductions, reviews scan quality.

DELIVERY

08 Three-Layer QA Review
L1 Auditor → L2 Senior Consultant → L3 Security Architect. Every finding validated.

09 Reporting & Certification
Executive + technical reports with code-level fixes, retesting, and security certificate.

See a sample evidence pack →

> *"Security Brigade's structured approach through Lemon gave us complete visibility into the testing process. The three-layer review caught issues that our previous vendor missed entirely. Their reports were the first our developers could actually act on without a follow-up call."*

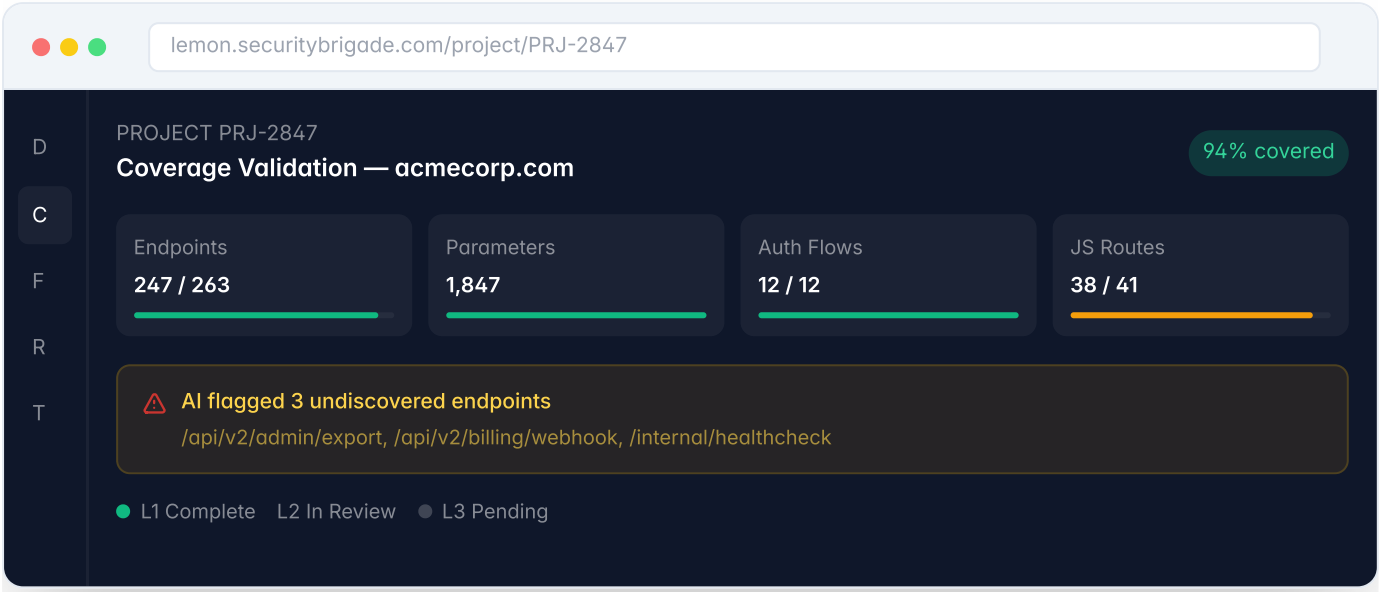
CISO, Leading Indian BFSI Enterprise
Indian Private Sector Bank

Read more client stories →

THE PLATFORM

Powered by Lemon

Most firms rely on individual tester skill. We built a platform that makes quality structural — informed by 6,700+ previous assessments.



Intelligent Orchestration

Auto-fingerprints your app, selects methodology, generates structured tasks from 6,700+ past engagements.

AI-Augmented Validation Engine

Cross-references auditor findings, spider results, JS analysis, route files, and server logs. Flags what was missed.

L1 → L2 → L3 Review

Three-layer expert review before any finding reaches your report. Every vulnerability validated, every gap caught.

COMPLIANCE-READY

Audit-ready reporting for every framework

As a CERT-In empanelled firm, our reports are accepted by all major Indian and global regulators.

- **CERT-In** — Empanelled since 2008
- **RBI** — Banks, NBFCs, payments
- **SEBI** — Exchanges, brokers, AMCs
- **IRDAI** — Insurance sector
- **PCI DSS v4.0** — Payment card data
- **ISO 27001** — Annex A 8.8
- **SOC 2** — Trust service criteria
- **DPDP Act** — Data protection

RBI Compliance Guide → SEBI Framework →

INDUSTRIES

1,000+ clients across verticals

Two decades of engagements across regulated and consumer-scale sectors.

BFSI
ICICI Bank, HDFC, Yes Bank, UTI MF, Edelweiss

Fintech & Payments
PhonePe, Amazon Pay, Groww, BillDesk

Manufacturing
Mahindra, Asian Paints, L&T, Hindalco

Retail & Consumer
Swiggy, Sephora, Pernod Ricard, Jubilant

Aviation & Logistics
Etihad Airways, DHL Express, Shadowfax

Healthcare
CloudNine, Pharmeasy, Wave Health

DELIVERABLES

What you get

Reports for two audiences — executives who need the risk picture, and developers who need to fix the issues. With code-level guidance, not vague advice.

Request sample report →

Read case studies →

Executive Report

Risk overview, critical findings, business impact, remediation priorities. Board-ready.

Technical Report

Step-by-step POCs, screenshots, request/response data, CVSS, and code-level fix examples.

Retesting & Support

Multiple retesting rounds. Remediation walkthroughs with your dev team or vendors.

Security Certificate

Formal certificate for compliance, customer assurance, and vendor due diligence.

FAQ

Common questions

Can't find what you're looking for? Talk to our team.

What is web application penetration testing?

Web application penetration testing (also called WAPT or web app VAPT in India) is a structured security assessment where certified experts simulate real-world attacks against your web application to identify vulnerabilities before malicious actors exploit them. It goes beyond automated scanning to include manual testing of business logic, authentication, authorization, and application-specific attack scenarios.

How long does a web application penetration test take?

A typical engagement follows an 8 to 12 business day cycle — from kickoff through application mapping, manual testing, automated scanning, multi-layer quality review, and final report delivery. Complex applications may require longer. Lemon enforces daily progress tracking.

How is manual testing different from automated scanning?

Automated scanners detect pattern-based vulnerabilities but miss business logic flaws — authorization bypass, transaction abuse, workflow manipulation. Our approach combines deep manual testing (thousands of test cases) with AI-validated coverage. The scanner is one data source; the real value is expert analysis.

Is penetration testing required for RBI compliance?

Yes, and the cadence is specific. The RBI (Commercial Banks — Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026 require vulnerability assessment at least once every six months and penetration testing at least once in 12 months for critical information systems and / or those in the DMZ with a customer interface (para 151), plus testing across the lifecycle — pre-implementation, post-implementation and after changes (para 150). Parallel Directions issued the same day cover small finance banks, payments banks, urban co-operative banks, NBFCs and credit information companies. Testing must be performed by trained and independent experts (para 155). Security Brigade has been CERT-In empanelled since 2008; under para 159, engaging an empanelled auditor brings CERT-In's Comprehensive Cyber Security Audit Policy Guidelines into the bank's supervisory relationship.

What is CERT-In empanelment?

CERT-In is India's national cybersecurity agency. Empanelment means Security Brigade has been vetted and approved to conduct security audits — mandatory for government and critical infrastructure assessments. We've held this since 2008.

How do you ensure coverage is complete?

AI-driven coverage validation cross-references auditor mind maps, spidering results, JS analysis, directory listings, route files, and server logs. No competitor offers equivalent coverage assurance.

What certifications does your team hold?

OSCP, OSCE, CRTP, CEH, ECPT, PEH, and CISEH — spanning offensive security, red teaming, and structured ethical hacking disciplines.

Do you provide remediation guidance?

Yes — reports include technology-specific code examples showing exactly how to fix each vulnerability. We also offer remediation walkthrough sessions with your dev team.

RELATED RESOURCES

Compliance Frameworks

RBI Cyber Security Compliance
India

SEBI Cyber Security Framework
India

PCI DSS v4.0 Penetration Testing
Global

SOC 2 Compliance Audit
Global

CERT-In Security Certification
India

IRDAI Cyber Security Compliance
India

Case Studies

BFSI
Critical Auth Bypass in Banking Portal
Discovered multi-step authorization flaw that scanners missed entirely.

Fintech
API Security Overhaul for Payment Platform
Full API security assessment leading to 40+ vulnerability remediation.

SaaS
Pre-Launch Security for Series B SaaS
Investor due diligence security assessment completed in 10 days.

Guides & Articles

OWASP Top 10 Explained for Business Leaders

VAPT vs Penetration Testing: The Difference

Manual vs Automated Penetration Testing

How to Choose a CERT-In Empanelled Auditor

VAPT RFP Template (free download)

How We Work — Engagement Models

RELATED SERVICES

Strengthen your security posture further

Mobile App Testing
iOS and Android security assessment with reverse engineering and API testing.

Secure Code Review
Manual + AI-powered source code analysis. Required for PCI DSS compliance.

Red Team Assessment
Realistic adversary simulation using ShadowMap attack surface intelligence.

Network Penetration Testing
Internal and external network VAPT with infrastructure hardening guidance.

Your application is being targeted.
Test it before attackers do.

Get a free scoping call with our security architects. We'll assess your risk profile and recommend the right approach.

Typically responds within 1 business day · No commitment required

Mumbai · London · New York · Singapore
in.sales@securitybrigade.com · +91 22 4164 2220