



PENETRATION TESTING

DISCOVER. EXPLOIT. DEMONSTRATE.

Hands-on penetration testing combining established security methodology, AI-accelerated analysis and more than 25 years of offensive security experience.

AI ACCELERATES THE WORK. EXPERIENCE DIRECTS IT.

LCSG uses modern AI capabilities to increase analytical speed and coverage, while testing strategy, exploitation, validation and impact assessment remain human-led.

Penetration Testing Without the Checklist Mentality

A penetration test should answer more than whether vulnerabilities exist. It should determine which weaknesses are genuinely exploitable, how they can be combined, what an attacker could reach, and what the resulting exposure means to the organization.

MANUAL FIRST

Experienced testers investigate application behavior, trust boundaries, authorization, identity and business logic rather than treating scanner output as the assessment.

EXPLOITATION FOCUSED

Where safe and authorized, weaknesses are validated through controlled exploitation to separate theoretical issues from practical attack paths.

BUSINESS CONTEXT

Technical findings are evaluated in the context of accessible data, privileges, systems and business processes.

DEPTH OVER VOLUME

The objective is not the longest vulnerability list. It is to identify the weaknesses and combinations that create meaningful exposure.

The result is an assessment built around what can actually be achieved - not simply what a tool can detect.

Coverage Built Around the Environment

Engagement scope is tailored to the technology, architecture and objectives of the client. Testing can be performed against individual systems or combined across multiple layers to expose attack paths that would otherwise remain hidden.

WEB APPLICATIONS Authentication, authorization, session handling, injection, business logic, file handling, client-side behavior and application-specific attack paths.	APIs & GRAPHQL Object- and function-level authorization, authentication, data exposure, business flows, server-side interactions, GraphQL controls and API-specific logic.
CLOUD Externally reachable services, cloud identities, permissions, storage, service configuration and exploitable relationships between cloud resources.	IDENTITY Authentication flows, privilege boundaries, role enforcement, federation, token handling and identity-driven attack paths.
NETWORK & INFRASTRUCTURE Exposed services, configuration weaknesses, trust relationships, segmentation and opportunities for controlled compromise.	MOBILE & CLIENT TECHNOLOGY Application-to-API trust, local security controls, authentication, data handling and attack paths spanning client and backend services.

Structured Methodology. Adaptive Testing.

LCSG uses recognized industry guidance as a foundation while allowing experienced testers to follow evidence, investigate unexpected behavior and pursue attack paths that rigid checklists can miss.

01 DEFINE

Confirm scope, objectives, test accounts, rules of engagement, communications and safety constraints.

02 DISCOVER

Map the attack surface, application behavior, technologies, roles, trust boundaries and exposed functionality.

03 TEST

Apply structured security testing across authentication, authorization, input handling, business logic, configuration and relevant technology-specific controls.

04 EXPLOIT

Validate vulnerabilities through controlled exploitation where authorized and safe, including attack chaining where it materially changes impact.

05 DEMONSTRATE

Establish what access, data, privileges or business functions become reachable and document evidence of impact.

06 REPORT & RETEST

Deliver prioritized findings, practical remediation guidance and optional verification of corrective actions.

Industry Guidance as a Baseline - Not a Ceiling

For web and API assessments, LCSG references the OWASP Web Security Testing Guide (WSTG) and OWASP API Security Top 10 as recognized sources of testing guidance and risk awareness. OWASP describes the WSTG as a comprehensive guide for testing web applications and web services, while its API Security project focuses specifically on risks unique to modern APIs.

OWASP WEB SECURITY TESTING GUIDE

Used as a structured reference for areas such as information gathering, identity and authentication, authorization, session management, input validation, error handling, cryptography, business logic, client-side behavior and API/web-service testing.

Reference: OWASP WSTG - <https://owasp.org/www-project-web-security-testing-guide/>

OWASP API SECURITY TOP 10

Used to ensure focused consideration of API-specific risks including broken object- and function-level authorization, authentication weaknesses, unrestricted business flows, SSRF, security misconfiguration, inventory issues and unsafe consumption of third-party APIs.

Reference: OWASP API Security - <https://owasp.org/API-Security/>

OWASP provides the framework. Experience determines where to look deeper.

Real applications contain implementation details, legacy behavior, custom workflows and unexpected interactions that cannot be reduced to a fixed list of tests. Our methodology uses standards to support consistency while preserving the freedom to investigate what the target actually reveals.

AI Is a Force Multiplier, Not the Tester

LCSG embraces AI as part of modern offensive security. It can accelerate analysis, correlate large volumes of technical information, identify patterns, assist with code and protocol understanding, and help testers explore a wider set of hypotheses.

WHERE AI HELPS

- Accelerating reconnaissance and technical analysis
- Correlating endpoints, parameters, identities and behaviors
- Supporting code, JavaScript, API and protocol analysis
- Generating and refining test hypotheses
- Reducing repetitive analytical work

WHERE EXPERIENCE LEADS

- Understanding context and business logic
- Recognizing abnormal or exploitable behavior
- Choosing meaningful attack paths
- Controlled exploitation and validation
- Determining technical and business impact

25+ YEARS OF OFFENSIVE SECURITY EXPERIENCE

AI changes how quickly information can be processed. It does not replace the judgement, intuition and technical experience required to recognize subtle weaknesses, combine vulnerabilities or understand what a successful attack actually means.

Clear Evidence. Practical Remediation.

The value of a penetration test depends on what the organization can do with the results. LCSG reporting is designed for both technical teams and decision-makers.

EXECUTIVE SUMMARY A concise explanation of the security posture, significant attack paths and the business implications of the assessment.	TECHNICAL FINDINGS Detailed evidence, affected components, exploitation conditions, severity rationale and reproduction information appropriate for remediation teams.
ATTACK PATHS Where individual weaknesses combine, the report explains the sequence and resulting impact rather than treating each issue in isolation.	REMEDIATION GUIDANCE Practical corrective actions focused on addressing root causes and reducing exploitable exposure.
EVIDENCE Screenshots, request/response evidence and other appropriate proof demonstrating what was validated during the engagement.	RETESTING Optional verification of remediation to confirm that identified weaknesses and attack paths have been effectively addressed.

FIND THE WEAKNESS. PROVE THE IMPACT. MAKE THE RESULT USEFUL.



DISCOVER. EXPLOIT. DEMONSTRATE.

Litchfield Cyber Security Group provides hands-on offensive security backed by decades of vulnerability research and real-world testing experience.

PENETRATION TESTING | RED TEAM OPERATIONS | VULNERABILITY RESEARCH

M&A; CYBER DUE DILIGENCE | GOVERNMENT CYBER CAPABILITIES

LCSG.US

LITCHFIELD CYBER SECURITY GROUP