



LCSG

LITCHFIELD CYBER SECURITY GROUP

— DISCOVER. EXPLOIT. DEMONSTRATE. —

VULNERABILITY RESEARCH

DISCOVER. EXPLOIT. DEMONSTRATE.

Deep technical research focused on discovering previously unknown vulnerabilities, unconventional attack paths and exploitable weaknesses in complex technologies.

RESEARCH BEYOND CONVENTIONAL PENETRATION TESTING.

LCSG combines decades of vulnerability discovery experience with modern tooling and AI-accelerated analysis to investigate difficult security problems where the weakness is not already known.

Finding the Weakness That Is Not on the Checklist

Vulnerability research differs from conventional assessment work because the starting point may be an unexplained behavior, a complex technology, a protocol, a product or a hypothesis rather than a known vulnerability class. The objective is to understand the system deeply enough to identify where its assumptions fail.

ROOT-CAUSE FOCUSED Research goes beyond observable symptoms to understand the implementation or design condition that makes exploitation possible.	HYPOTHESIS DRIVEN Unexpected behavior is investigated, challenged and refined until it can be explained, reproduced or ruled out.
ATTACK-PATH ORIENTED Individual behaviors are examined for combinations that can transform a limited weakness into meaningful compromise.	EVIDENCE LED Findings are reproduced and validated with sufficient technical evidence to distinguish genuine vulnerabilities from anomalies.

The goal is not to match a known signature. It is to understand why the system can be made to behave in a way its designers did not intend.

Complex Technology. Unconventional Failure Modes.

Research engagements are tailored to the target technology and objective. LCSG can investigate individual products, protocols and components or follow interactions across multiple layers where trust assumptions and implementation details intersect.

APPLICATION & API LOGIC Complex authorization, state transitions, parser behavior, trust boundaries and unexpected interactions across application and API workflows.	AUTHENTICATION & IDENTITY Tokens, federation, session behavior, privilege boundaries, identity transitions and implementation-specific authentication weaknesses.
PROTOCOLS & SERVICES Protocol state, parsing, message handling, service interactions and conditions that create unexpected or exploitable behavior.	CLOUD & DISTRIBUTED SYSTEMS Cross-service trust, permissions, exposed interfaces and behaviors that emerge from combinations of cloud components.
CLIENT & MOBILE TECHNOLOGY Client-side trust assumptions, local controls, application-to-backend relationships and security-sensitive implementation behavior.	EMERGING TECHNOLOGY New platforms, AI-enabled systems and other technologies where established test patterns may not yet adequately describe the attack surface.

From Observation to Demonstrated Impact

Vulnerability research is inherently adaptive, but disciplined investigation helps turn unusual behavior into reproducible security knowledge.

01 UNDERSTAND

Build a technical model of the target, its components, data flows, trust assumptions and security boundaries.

02 OBSERVE

Identify unusual responses, inconsistencies, edge conditions and behaviors that merit deeper investigation.

03 HYPOTHESIZE

Develop possible explanations and attack theories, then design focused experiments to test them.

04 VALIDATE

Reproduce promising conditions, isolate the root cause and determine whether the behavior creates a security boundary failure.

05 EXPLOIT

Where authorized and safe, construct controlled proof that demonstrates what the vulnerability enables.

06 DOCUMENT

Capture the affected conditions, reproduction evidence, impact, root cause and practical remediation considerations.

AI Expands the Search Space. Experience Recognizes the Signal.

Modern AI can materially accelerate vulnerability research by processing large bodies of technical information, correlating behavior and helping explore hypotheses. It is most effective when directed by an experienced researcher who understands what is unusual, what is plausible and what deserves deeper investigation.

AI CAN ACCELERATE

- Large-scale technical analysis
- Code and JavaScript comprehension
- Protocol and data-structure analysis
- Pattern and anomaly correlation
- Hypothesis and test-case generation

EXPERIENCE DIRECTS

- Recognizing subtle security boundaries
- Understanding implementation intent
- Separating noise from exploitable behavior
- Constructing meaningful exploit chains
- Determining real-world impact

25+ YEARS OF VULNERABILITY RESEARCH EXPERIENCE

AI can suggest possibilities at extraordinary speed. Experience is what turns the interesting possibility into a validated vulnerability.

Technical Depth With Controlled Disclosure

Research may uncover weaknesses with significant security consequences. Engagements therefore establish clear authorization, handling and disclosure expectations before work begins.

AUTHORIZATION Research is performed within explicitly agreed technical and legal boundaries.	SAFE VALIDATION Proof is designed to establish impact while avoiding unnecessary disruption or access beyond what is required.
CONFIDENTIAL HANDLING Research artifacts, exploit material and sensitive technical details are handled according to agreed controls.	REPRODUCIBILITY Findings are documented sufficiently to allow the affected party to understand and reproduce the condition.
DISCLOSURE SUPPORT Where appropriate, LCSG can support coordinated communication of validated vulnerabilities to affected technology owners.	REMEDIATION CONTEXT Research explains the underlying security failure so corrective action can address root cause rather than only the demonstrated payload.

From Discovery to Actionable Technical Knowledge

The output of vulnerability research is designed to preserve the technical depth of the discovery while making the security consequence clear to engineering and decision-making teams.

RESEARCH SUMMARY The problem investigated, the resulting discovery and why the behavior matters.	TECHNICAL ROOT CAUSE A detailed explanation of the implementation, design or trust failure responsible for the vulnerability.
PROOF OF CONCEPT Controlled evidence demonstrating exploitability where appropriate and authorized.	IMPACT ANALYSIS The privileges, data, systems or security boundaries affected and the conditions required for exploitation.
REMEDIATION CONSIDERATIONS Technical guidance focused on correcting the underlying failure and reducing opportunities for variant vulnerabilities.	RETEST & VARIANT REVIEW Optional validation of remediation and focused investigation for related weaknesses created by the same underlying pattern.

DISCOVERY IS ONLY THE START. THE VALUE COMES FROM UNDERSTANDING WHY IT WORKS.



DISCOVER. EXPLOIT. DEMONSTRATE.

Deep vulnerability research backed by more than 25 years of hands-on offensive security and vulnerability discovery experience.

**VULNERABILITY RESEARCH | PENETRATION TESTING | RED TEAM
OPERATIONS**

M&A; CYBER DUE DILIGENCE | GOVERNMENT CYBER CAPABILITIES

LCSG.US

LITCHFIELD CYBER SECURITY GROUP