GRYPHON
SECURITY

Web Application Penetration Testing

Real-World Application Abuse. Clear Business Impact.

A focused security assessment designed to simulate realistic attacks against web applications and application programming interfaces (APIs), where data integrity, availability, and trust in externally facing systems are critical.

Modern organizations rely heavily on web applications to deliver services, manage data, and support core operations. These applications are frequent targets for attackers seeking to exploit logic flaws, authentication weaknesses, insecure data handling, and misconfigurations. This service provides leadership with a clear, defensible understanding of how an attacker could realistically abuse a web application using controlled, authorized adversarial techniques.

Traditional reviews assess whether applications were designed securely. Web application penetration testing demonstrates how applications can be abused in practice.

What We Do

We conduct a controlled web application penetration test designed to simulate real-world attacks against web applications and APIs exposed to users or the internet.

The assessment identifies exploitable vulnerabilities, insecure design patterns, and business logic flaws that could allow unauthorized access, data manipulation, privilege escalation, or application compromise. Testing is performed safely, ethically, and within an approved scope to validate actual exploitability—not theoretical weakness.

The result is evidence-based insight into how an attacker could interact with, manipulate, or compromise the application.

Why This Matters

Web applications are often the most exposed and most targeted components of an environment. A single vulnerable application can provide attackers with access to sensitive data, user accounts, or backend systems.

Web application penetration testing demonstrates:

- How attackers can bypass authentication or authorization controls
- How application logic can be abused beyond intended use
- How input handling and data flows can be exploited

- Where application-level defenses and monitoring fail
- Which weaknesses pose real business and operational risk

This service equips leadership with defensible, real-world clarity before an application flaw is exploited externally.

Our Testing Approach

This service uses a structured, risk-focused web application penetration testing methodology aligned with **OWASP** guidance and industry-recognized attack techniques.

Testing begins with application mapping and attack surface analysis, followed by controlled exploitation to validate impact. Where in scope, authentication flows, authorization enforcement, session handling, and business logic are tested to demonstrate realistic abuse scenarios.

The engagement is not a certification, compliance audit, or automated scan. It is a deliberate simulation designed to answer one core question:

"If an attacker interacted with this application as a user, what could they realistically exploit, and what would the impact be?"

What's Tested

Testing scope is tailored to the application but commonly includes:

- **Authentication & Session Management**
  Login workflows, credential handling, session controls, and token security
- **Authorization & Access Control**
  Privilege boundaries, role enforcement, and direct object access
- **Input Handling & Injection**
  Validation, encoding, and protection against injection and manipulation attacks
- **Application Logic & Workflow Abuse**
  Misuse of intended functionality, state manipulation, and logic flaws
- **Date Protection**
  Exposure of sensitive data, insecure storage or transmission, and improper error handling
- **Detection & Visibility Gaps**
  Ability to detect and respond to malicious application-level activity

Testing aligns with common **OWASP Top 10** risk categories and real-world exploitation techniques.

What You Receive

You receive clear, actionable deliverables – not raw scan output:

- **Executive Summary**
  Plain-English overview of application risk and impact
- **Risk-Rated Findings**
  Critical → High → Medium → Low

- **Documented Exploitation Scenarios**
  How an attacker could abuse the application, with business impact explained
- **Evidence-Backed Remediation Roadmap**
  Prioritized 30 / 60 / 90-day recommendations mapped to application risk

Reports are suitable for executive leadership, development teams, and technical remediation.

Who This Service Is For

This service is designed for:

- Organizations operating customer-facing or internal web applications
- Teams deploying custom applications or APIs
- Environments concerned about data exposure, account compromise, or application abuse
- Organizations validating secure development and deployment practices

This Service Is *Not* Designed For

- Organizations seeking a checkbox compliance assessment
- Organizations looking for automated vulnerability scanning only
- Environments without commitment to remediation and secure development improvement

Gryphon Security focuses on clarity, independence, and defensible outcomes.

Why Gryphon Security

- Real-world offensive tradecraft
- OWASP-aligned testing grounded in actual exploitation
- Evidence-driven, non-alarmist reporting
- No product resale or vendor bias
- Built for executives, developers, and security teams

We focus on how applications are supposed to work and how they are actually attacked.

Next Steps

An initial conversation is structured, confidential, and obligation-free.

We will:

- Confirm application scope and architecture
- Discuss key risk concerns
- Explain exactly what testing will and will not include

We will not pressure you into tools, managed services, or long-term contracts.

Gryphon Security, LLC
Offensive Security & Risk-Based Testing
info@gryphonsec.com | www.gryphonsec.com