STROZ FRIEDBERG
A LevelBlue Company

SERVICE BRIEF

Application Security Testing

Stroz Friedberg's Application Penetration Testing Services

Stroz Friedberg's Application Penetration Testing provides organisations with a comprehensive assessment of their websites, APIs, thick clients, and other custom applications to help identify potential weaknesses. This testing is specifically designed to assess the resilience of these digital assets against application-specific attacks and vulnerabilities that could be exploited by malicious actors. The assessment can help ensure that organisations can identify and mitigate risks before they are exploited, thus improving the overall security posture of their applications.

Determine Application Attack and Vulnerability Resilience

Our proprietary testing approach combines industry-standard security frameworks and guidelines to ensure thorough assessment coverage. These include the OWASP Top Ten, which identifies the most critical web application security risks, and the OWASP Code Review Guide, which provides best practices for secure coding. Additionally, the testing references the CWE/SANS Top 25 Most Dangerous Software Errors, a list of the most serious vulnerabilities that could pose significant risks to software systems. This comprehensive method helps organisations identify vulnerabilities specific to their applications and take proactive steps to improve security.

DYNAMIC TESTING

The Stroz Friedberg team tests running applications for vulnerabilities such as injections, data exposure, access control, authentication failures, security misconfigurations, outdated components and business logic flaws. This testing is performed as both authenticated and unauthenticated users.

CODE REVIEW

The Stroz Friedberg team reviews code and configurations for web applications, mobile apps, APIs and more using industry standards. When vulnerabilities are found, the codebase is checked for similar issues. Secure code reviews help identify security flaws early in development, preventing future exploitation.

HYBRID TESTING

Hybrid testing combines dynamic application penetration testing with secure code review techniques. Clients gain the advantage of testing a live, running application to develop proof-of-concept exploits, along with source code analysis to identify root causes. These assessments enable more comprehensive and in-depth evaluation coverage.

Full-Spectrum Application Penetration Testing

Our penetration testing services include thorough assessments of APIs, web applications, and thick clients. We combine manual testing methods with various tools and approaches – proprietary, open-source, and commercial – to find vulnerabilities in applications. Testing is done from the perspectives of both unauthenticated and authenticated users in different roles.

APIS

API security is essential for modern applications. We ensure that endpoints are thoroughly tested for issues like improper data handling, authorisation problems, broken authentication, and access control flaws. We use both automated and manual methods to identify security weaknesses that might be missed in standard API testing.

WEB APPLICATIONS

Our team evaluates the entire stack – including front-end and back-end components – to identify potential vulnerabilities such as cross-site scripting (XSS), injection attacks (SQLi), and misconfigurations that could result in unauthorised access or data leaks.

Focusing on both unauthenticated and authenticated scenarios, we simulate real-world attacks from multiple user perspectives to provide a comprehensive view of potential security threats across application layers.

THICKCLIENTS

Our penetration testing of thick client applications covers areas such as local storage, memory exploitation, authentication, access control and communication protocols. This ensures that client-server interactions are secure, and that the application's internal logic is not readily vulnerable to manipulation or exploitation.

SF STROZ FRIEDBERG
A LevelBlue Company

About Stroz Friedberg

Stroz Friedberg, a LevelBlue company, delivers intelligence-driven digital risk management with expert-led services designed for adaptive resilience.

With over 25 years of leading the resolution of the most complex, high-stakes digital risk issues, we manage the entire digital risk lifecycle – from cyber threats and insider risks to IP theft and regulatory compliance. Our approach combines managed security services with expert analysis and strategy, supported by threat intelligence gathered from thousands of engagements across various industries.

We translate complex technical and legal risks into actionable strategies, helping CISOs and legal teams turn digital risks into board-ready insights. Our comprehensive services include managed cyber defense, digital forensics and incident response, trade secret protection, expert witness support, threat intelligence, security strategy and governance, attack path mapping and testing, and resilience engineering.

Operating as one trusted partner, we align technical precision with business priorities to protect critical assets, adapt to evolving threats, and maximize ROI through proven outcomes. Through LevelBlue's portfolio, these specialized services integrate seamlessly with 24/7 managed security operations and AI-driven threat detection for comprehensive digital risk protection.

Cybersecurity. Simplified.

levelblue.com/strozfriedberg

| 633SVB 09-2025