NetSPI™

SAST & SCR

Static Application Security Testing (SAST) and Secure Code Review (SCR)

Proactively detect Application Security vulnerabilities through Source Code Analysis Web Application Penetration Testing by NetSPI

The Evolution of AppSec Programs Makes Secure Code Review Even More Critical

Secure Code Review (SCR) and Static Application Security Testing (SAST) are essential security touch points in any Secure SDLC, as an effort to identify and remediate security vulnerabilities earlier in the software development life cycle. Secure code review is an essential complement to web application testing. It involves systematically examining an application's source code to identify and remediate security vulnerabilities that might not be evident through testing alone.

Our service offerings enable application security teams and software development teams to leverage the appropriate level of secure code review services to detect, validate, and resolve security issues based on the business criticality and risk profile of their applications.

The Need for Secure Code Review

As development sprints approach warp speed, with the popular adoption of the DevSecOps culture, and the integration of machine learning and large language models (LLMs) to accelerate coding processes the need for early detection and remediation of security vulnerabilities becomes even more critical.

If security vulnerabilities are not detected and addressed earlier through Secure Code Review or SAST techniques, the cost of remediating these vulnerabilities can increase exponentially. Security is a key component of software development and doing secure code review ensures that security is being built into the software before it is deployed to production.

SCR involves inspecting the source code (and compiled code) to identify security bugs with full visibility into how an application is stitched together. There are many vulnerabilities that are hard to detect during time-boxed penetration tests and Source Code Review can complement an organization's penetration testing efforts to more comprehensively detect vulnerabilities and, in many cases, identify vulnerabilities that are not possible to discover during dynamic testing and analysis.

Secure Code Review Assessment results transform vulnerabilities into learning opportunities. By documenting discovered security weaknesses, developers gain insights into recurring coding patterns, understand root causes of flaws, and internalize secure coding principles. This feedback mechanism guides developers to proactively prevent similar issues, build security expertise, and adopt best practices across different projects and technology stacks.

The Benefits of Secure Code Review

Proactively Prevent Vulnerabilities

Identify and remediate security weaknesses is code before they reach production

Achieve Compliance

Meet security standards and regulatory requirements through systematic code analysis

Improve Security

Application security by systematically addressing code-level risks

Develop Secure Coding Expertise

Provide targeted feedback to improve developer security awareness and skills

Leverage NetSPI's Secure Code Review Services Based on Your Business Objectives and Application Risk Profile

Secure Code Review (SCR)

- Source code analyzed with commercial and open source SAST tools and medium and higher severity vulnerabilities triaged (false positives removed)
- Manually review source code to identify issues such as Authorization, Business Logic and Data Flow vulnerabilities not easily discovered by SAST tools
- Deep dive approach to review underlying frameworks and libraries for known vulnerabilities
- Remediation discussion with development team and actionable remediation advice
- Static analysis performed with a combination of commercial and open-source tools where all medium and high severity vulnerabilities are manually reviewed to triage and remove false positives
- Besides automated analysis, NetSPI will review source code manually to identify vulnerabilities that automated scanners cannot detect. Examples include: complex injection attacks, insecure business logic, use of weak or improper encryption techniques, insecure error handling, authentication and authorization issues
- We review code at a feature-level instead of only focusing on bad secure code patterns
- Review application's configuration, underlying frameworks and libraries to determine any known vulnerabilities that can be exploited based on how the application has been stitched together

Supported Languages: Java, .Net (C#, ASP, VB), SQL, JavaScript Frameworks, C/C++, PHP, Python, Android (Java), iOS (Objective-C & Swift), and Go

SAST Triaging

- Augment AppSec team's efforts to triage results from existing SAST tools
- Closely integrate with your organization's existing static analysis review process
- Expedite remediation efforts by providing security expertise and guidance to development teams
- Many organizations leverage SAST tools in their internal environment that addresses their Application Security Program's secure code review needs
- NetSPI can provide support to augment your organization's Application Security Program and in triaging efforts to remove any false positive findings before the results are provided to development teams
- Focus the efforts of the development teams on issues that need attention and remediation instead of having them burn their cycles trying to validate the exploitability of vulnerabilities
- Provide development teams access to security consultants that can discuss remediation techniques and strategies with the appropriate stakeholders

Supported Tools: Checkmarx (CxSAST), Semgrep, Veracode Static Analysis, Fortify on Demand /Fortify Static Code Analyzer, HCL AppScan Source, Blackduck Coverity, SonarQube, Semgrep

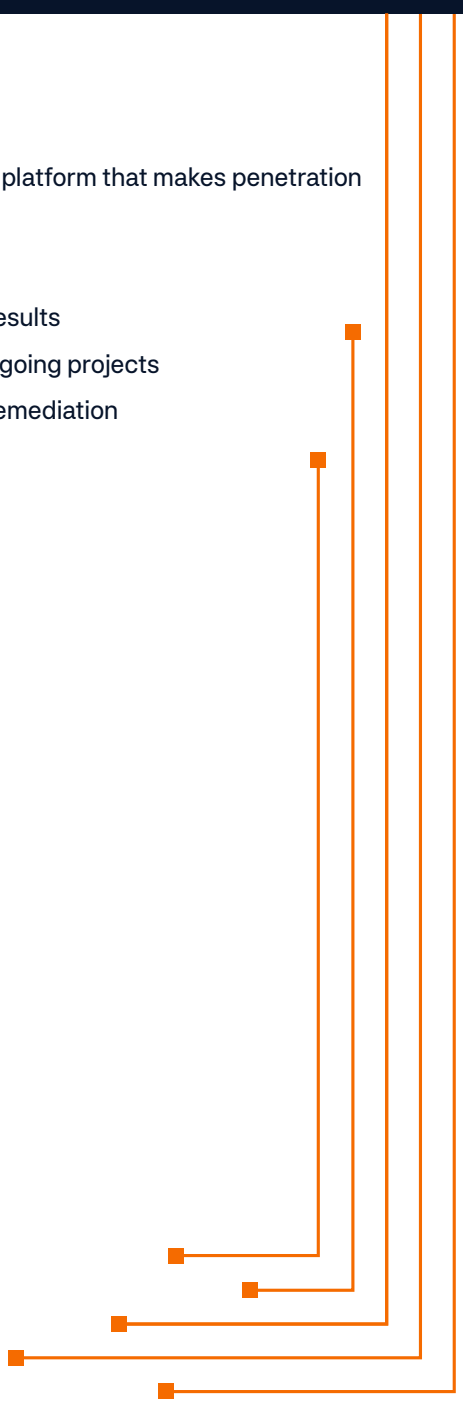
Tailored Software Security Offerings

- Comprehensive Dependency Risk Analysis
- SAST Rule Development
- Code Assisted Testing
- CI/CD Security Assessment

The NetSPI Difference

NetSPI delivers industry-leading penetration testing expertise and a vulnerability management platform that makes penetration test results actionable.

- A collaborative team with experience and expertise produces the highest quality of work
- Consistent processes with formalized quality assurance and oversight deliver consistent results
- Technology allows more focus on testing and scales to large engagements and multiple ongoing projects
- Actionable guidance by a trusted partner from the start of the engagement to the end of remediation



About NetSPI

NetSPI® pioneered Penetration Testing as a Service (PTaaS) and leads the industry in modern pentesting. Combining world-class security professionals with AI and automation, NetSPI delivers clarity, speed, and scale across 50+ pentest types, attack surface management, and vulnerability prioritization. The NetSPI platform streamlines workflows and accelerates remediation, enabling our experts to focus on deep dive testing that uncovers vulnerabilities others miss. Trusted by the top 10 U.S. banks and Fortune 500 companies worldwide, NetSPI has been driving security innovation since 2001. NetSPI is headquartered in Minneapolis, MN, and available on **AWS Marketplace**. Follow us on **LinkedIn** and **X**.