



CODE REVIEW

305-828-1003

info@infosightinc.com

Overview

The primary goal of a code review is to identify and address issues, bugs, security vulnerabilities, and maintainability concerns in the codebase before it is deployed into the production environment. A secondary goal is to ensure the security of the code over its life and changes are made. Code reviews can take place at various stages of the development process, so understanding how security can be considered during all phases is crucial.

The Challenge

There are several challenges that developers face when attempting to write secure code. The sheer complexity of security and keeping up with the ever-evolving security landscape can be daunting. This is exacerbated by the pressure to deliver applications quickly. Additionally, trying to balance Security and Usability can add to the effort because having a positive end-user experience is key to achieving business goals. There are also other challenges such as Legacy Code and Dependencies, a Lack of Resources, Human Error and Compliance and Regulatory Requirements.





How We Solve It



To address these challenges, we first familiarize ourselves with the Application in scope. We approach the code review with the goal of helping the developer. We ensure that the code follows the established coding security guidelines. We assess the code against OWASP Top 10, CWE Top 25, and other relevant security standards. We scrutinize the code for potential security vulnerabilities, and common issues like input validation issues, SQL injection, cross-site scripting (XSS), and sensitive data exposure. In the final stages of the review, we provide actionable recommendations for each identified vulnerability, including code fixes, configuration changes, and security improvements.

Our Objectives are to identify and document security vulnerabilities, including but not limited to:

- Authentication and Authorization flaws;
- Input validation and data sanitization issues;
- Insecure coding practices;
- Security misconfigurations;
- Vulnerable third-party libraries or dependencies;
- Cryptographic weaknesses.

Other Assessments:



Vulnerability & Penetration Testing

Consists of a multi-disciplinary, multi-faceted review of the organization's systems which identifies vulnerabilities outside and inside the network and attempts to exploit any vulnerabilities in the same way a malicious actor would.



Red Team / Blue Team Testing

Designed to test an organization's readiness to detect, withstand and respond to a targeted attack. The red team's goal is to find and exploit any identifiable weaknesses in the organization's security as the blue team works to defend the organization by finding and patching vulnerabilities and responding to successful breaches.



Web & Mobile Security & API

Involves the security testing of web, mobile and software application interfaces to identify privilege escalation, authorization creep, and security controls bypass. It includes a detailed report outlining discovered vulnerabilities and remediation steps.

After testing is complete, Digital reports are delivered via our proprietary **Mitigator Vulnerability and Threat Management Platform**. Reports can be exported in multiple formats and printed.



The Outcome



Our reporting is actionable! It allows developers to secure code but to make it more cyber resilient. Our goal of the code review is to assist developers in delivering high-quality software that meets security and maintainability requirements. We help organizations prioritize security as an integral part of the development process and foster a security-conscious culture within their development teams. By implementing the security strategies, you'll be well on your way to elevating your code quality!

