COGNISYS

PENETRATION TESTING

Code review

Our source code review enhances your development process with proven security solutions.

Source code review is integral to identifying vulnerabilities within the application's codebase

This methodology provides a structured approach for conducting a thorough code review, ensuring that known and potential vulnerabilities are discovered and mitigated. This guide is valuable for organisations seeking to secure their applications by integrating security into the development lifecycle.

Scoping and planning

Define objectives

Clearly outline the goals of the source code review. This includes identifying the specific security requirements, compliance standards (e.g., OWASP, PCI DSS), and the critical areas of the application that need to be reviewed.

Identify the codebase

Determine which parts of the codebase will be reviewed. Depending on the project's scope, this might include the entire codebase or specific modules. It is essential to understand that the code related to the application's core functionality should receive the primary focus during the review process.

Access requirements

Ensure that all necessary access permissions are granted to the source code repository. Define the tools and environments required for the review process, including IDEs, static analysis tools, and documentation resources.

Review preparation

Gather documentations

Collect all relevant documentation, including architecture diagrams, design documents, API specifications, and any prior security assessments. This provides context and understanding of the code's functionality and security posture.

Set up review environment

Prepare the environment for the review, including setting up static analysis tools, code linters, and any necessary plugins within the IDE. Ensure the environment mirrors the production setup as closely as possible.

Code familiarisation

Understanding the codebase structure, including critical modules, third-party libraries, and frameworks, is crucial for effective navigation and pinpointing areas that may require more detailed examination.

SmartView takes care of your reporting

Cognisys' SmartView Portal provides a centralised platform for clients to manage their projects and vulnerabilities efficiently. Through the portal, clients can track the status of each identified issue, assign tasks to team members, and monitor the progress of remediation efforts. This streamlined process ensures that vulnerabilities are addressed promptly and thoroughly, enhancing the overall security posture of the web application.

posture for web applications and an improved overall risk management strategy.

Why choose Cognisys' code review?

When it comes to securing your code, Cognisys stands out by offering a deep white box testing approach, detail-oriented review process that uncovers hidden vulnerabilities often missed by automated tools. Our expert team doesn't just skim the surface; we dive into the intricacies of your code to identify security gaps, logic flaws, and potential compliance issues.

With Cognisys, you're partnering with seasoned professionals who understand the nuances of secure coding practices and how they align with your business goals. We don't just find problems—we provide actionable insights and recommendations with code fixes to strengthen your code's resilience, ensuring your software is secure, reliable, and future-ready.

BACK TO CONTENTS