Blueinfy

# Agile Penetration Testing Methodology

Agile Security Testing is crucial in today's fast-paced development environments, where frequent releases and continuous integration are the norm. As organizations adopt agile methodologies to deliver software quickly, security must be integrated into every stage of development. Agile Security Testing ensures that vulnerabilities are identified and addressed early, without disrupting the development cycle. By embedding security testing into each sprint, teams can maintain high-speed delivery while ensuring that applications are robust, secure, and compliant. This approach not only reduces risks but also improves the overall quality of the software, allowing businesses to innovate confidently and securely.

Blueinfy has developed a strategic security approach, leveraging agile penetration testing principles, as part of its Agile Security Testing service: -

## Initial Comprehensive Penetration Test

On initiation of the client association, Blueinfy performs a full scope in-depth penetration test of the application to identify pre-existing vulnerabilities and to assess the application's security posture comprehensively. This initial assessment provides a detailed report outlining vulnerabilities, their potential impacts, and remediation recommendations.

## Ongoing Agile Penetration Testing

With every sprint/release cycle, the below methodology is followed to ensure security along with deployments: -

**Export from Ticketing System:** The company exports data from their ticketing system (in Excel format), including use cases, changes, and user stories related to each agile release.

**Review of Changes:** The Blueinfy team, with full knowledge of the application and security expertise, reviews the export to identify changes that may introduce security risks.

**Targeted Security Assessment:** Blueinfy conducts focused manual penetration tests on the specific changes highlighted, targeting areas with potential security impacts.

**Integration into Agile Workflow:** Blueinfy integrates its testing process into the company's agile workflow, ensuring seamless collaboration without disrupting the development cycle.

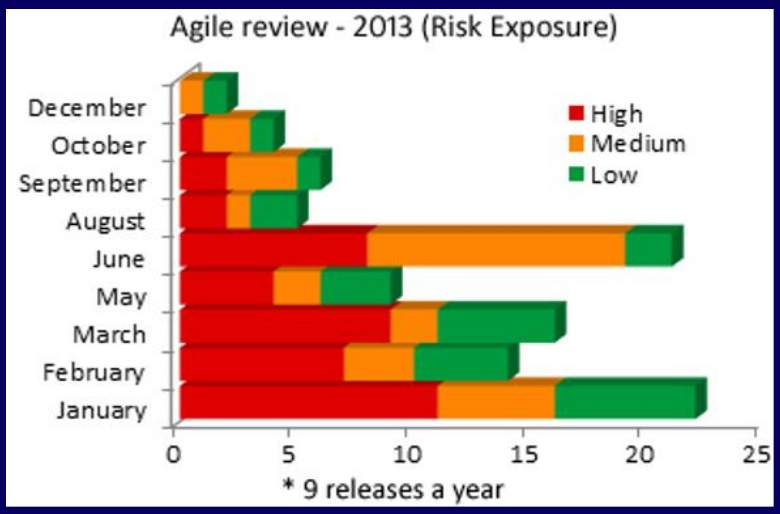
**Rapid Feedback:** Blueinfy provides quick, actionable feedback on vulnerabilities or risks identified in each agile release cycle.


contactus@blueinfy.net

**Iterative Testing:** This process is repeated iteratively, ensuring that security assessments remain aligned with the continuous pace of development and changes within the application.

## Enhanced Reporting and Management Tracking

To enable effective tracking and management of security performance, Blueinfy delivers detailed reports on vulnerabilities, trends, and the status of issues, which are updated regularly to reflect the latest changes. A security dashboard has been developed, offering management a clear, real-time view of the application's security status, including trends and actionable insights. As an example, following graph is provided:




The iterative nature of testing allows for continuous improvement and adaptation of security practices in response to evolving threats and development changes.

## Key Differences between Traditional Penetration Testing v/s Agile Penetration Testing

| Aspect | Traditional Penetration Testing | Agile Penetration Testing |
|---|---|---|
| Frequency | Conducted periodically (annually or biannually) | Continuous process integrated throughout the software development lifecycle |
| Scope | Focuses on the overall application | Allows for feature-specific testing as new functionality is developed |
| Methodology | Incorporates a mix of automation and manual testing | Relies more on manual testing techniques focusing on the enhancements for a sprint |
| Timing | Done at the end of the development process, before product launch | Performed at frequent intervals throughout development |
| Benefits | Provides a comprehensive report and overall security posture of the application | Offers real-time visibility, agility, and early identification of vulnerabilities |

## Actionable Report with Zero False Positives

A key deliverable of the assessment is a highly actionable, well-structured report designed to drive immediate remediation. The report is curated to maintain zero false positives and includes the following critical components: -

- Executive Summary
- Description of Discovered Vulnerabilities
- Risk Rating (curated after business impact assessment and industry security standards like CVSS/CWE/CVE)
- Evidence of Vulnerabilities (screenshots, HTTP traffic, vulnerable parameter, exploit vector, tool results, reproduction steps etc.)
- Exploit Evidence of Vulnerabilities (if required)
- Mitigation Strategies and Defence Approaches (catered to help Developers)
- Report Readout and Guidance

## Tools

Blueinfy uses its own tools along with open source tools and products during the assessment process. Blueinfy has its own tools and utilities for performing manual penetration testing. Some of these tools are available at https://www.blueinfy.com/tools.html


contactus@blueinfy.net