Desktop/Plugin Penetration Testing Methodology

Our desktop/plugin pen testing methodology (which includes manual + automated) covers all static and binary analysis of the installer and the application including OWASP Desktop Top 10 categories. Below is the methodology that is used for a comprehensive security review of desktop applications/plugins: -

Application Enumeration and Profiling

During this phase, testers map the features of the application and enlist the types of data it processes to identify likely attack surfaces and sensitive flows (authentication, data storage, APIs, third-party integrations). This contextual profiling guides targeted test cases, helps prioritise high-risk areas, and ensures critical entry points aren't missed or misclassified.

Security Control and Test Cases

1. **Data Storage Security** – This category focuses on identifying vulnerabilities in how an application handles data storage. It includes checking for sensitive information like credentials, session, hard-coded secrets, API keys etc. in local storage, caching of data, and use of weak encryption methods, and persistence of data after logout or application uninstallation etc.
2. **Access Control and Execution Privileges** – This category focuses on ensuring that desktop applications and plugins operate with the least privilege principle. It includes validation of permission enforcement, improper privilege escalation, bypass of authentication or authorization mechanisms, insecure use of system APIs, and exploitation of debugging or developer options.
3. **Third-Party Dependencies** – This category focuses on identifying vulnerabilities in the libraries being used, particularly if outdated versions are implemented and ensuring that excessive permissions are granted to third party components etc.
4. **Code Integrity and Reverse Engineering** - This category focuses on protecting the application binaries and plugin executables from tampering and unauthorized analysis. It includes validation for code signing, binary hardening, obfuscation, checksum verification, and anti-debugging mechanisms to prevent reverse engineering or malicious code injection.
5. **API Layer Vulnerabilities** – This category focuses on validating the security of API interactions within desktop or plugin architectures. The methodology listed as the "API Penetration Testing Methodology" applies for this set of checks.
6. **Network Communication/Device & Platform Security** – This category focuses on the security of data transmission and the overall device/platform interaction. It includes checking for insecure transmission of data, certificate validation, possibility of MiTM attacks, and exposure of API endpoints etc.

contactus@blueinfy.net

The list provided is not limited to but represents core test cases, but the high level methodology varies based on the logic/business use case of the application being tested.

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, file path, 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

