NetSPI™

Thick Client Application Penetration Testing Checklist

NetSPI uses multi-vector pentesting to identify vulnerabilities within thick client applications deployed on Windows, Linux/ Unix, and macOS. NetSPI's approach to thick app penetration testing includes reviewing server-side and client-side controls, data communication paths, data storage, and authorization/ authentication best practices.

Our thick application testing methodology pulls from best practices and test cases within the OWASP Top 10, NIST, PCI DSS, and similar sources. Tools we use include decompilers, proxies, packet sniffers, disassemblers, debuggers, and many more. Our testing methodology features:

- Examination of how thick applications interact with their environments to identify the exposure of sensitive information. It is not uncommon to discover critical secrets (i.e. passwords and encryption keys) in registries, file systems, source code, and elsewhere.
- Discovery of bypasses to application logic using an array of tools and reverse engineering techniques, which can lead to compromise of the application account and data security.
- Testing of network communications for exploits that can lead to compromise of application servers and integrity. The OWASP Top 10 doesn't only apply to web applications – areas of the greatest risk are just as severe in thick applications. Injections, XML External Entities, Broken Access Controls have been proven by our team to be commonplace.

While each thick application is unique and requires extensive manual testing, there are common areas of risk our testers focus on. The following is our thick application penetration testing checklist, which outlines key areas of focus for NetSPI's pentesters during engagements.

Thick Client Application Penetration Testing Checklist

- ☐ **Assembly Controls:** Protections applied to compiled code.
- ☐ **Cryptography:** Implementations of encryption and handling of secrets.
- ☐ **Password Management:** Storage and handling of passwords, both cleartext and encrypted.
- ☐ **Sensitive Information Disclosure:** Data leaked throughout the application environment.
- ☐ **Excessive Privileges:** Ensure that the principle of least privilege is applied to accounts, registries, and the file system.
- ☐ **Authentication and Session Management:** Ensure that authentication solutions are secure.
- ☐ **Account Management:** Proper restrictions for accounts residing on the application's system.
- ☐ **Authorization Controls:** Application logic surrounding authorization.
- ☐ **GUI Controls:** Vulnerabilities arising from weak client-side controls including authentication, authorization, and business logic bypasses.
- ☐ **Web Service Controls:** Identify vulnerabilities that allow users to escalate privileges, manipulate data, and gain access to restricted functionality or data.
- ☐ **Network Traffic Analysis:** Secure implementations of server communications.

NetSPI™

Virtual Desktop Environment Checklist

- ☐ **Group Policies:** Permissions on the system that limit user access to commands, applications, files, and directories.
- ☐ **Virtual Environment Breakouts:** Security misconfigurations within the virtualization platform that allow access to the system on which the application resides.
- ☐ **Network Controls:** Restrictions on unintended and excessive egress and ingress network communications.

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.