SYNOPSYS®

www.synopsys.com |

Penetration Testing

Eliminate vulnerabilities in your server-side applications and APIs

We replicate the steps a threat agent can take to exploit your vulnerabilities, demonstrates the impact, and provides clear guidance to fix them.

The tools you need

We combine multiple testing tools like automated scans and in-depth manual tests to get the most comprehensive security assessment of your client-side applications. We're also able to perform various types of high-quality penetration tests across many different types of software at scale.

The experts you want

Our application penetration testers have extensive experience building software—not just trying to break it. They leverage this experience to pinpoint business-critical issues and provide actionable remediation guidance. As a result of our pen tests, you'll be able to view your applications through the eyes of both a hacker and an experienced developer to discover where you can improve your security posture.

The depth that works best for you

We offer two depths of penetration testing for you to choose from.

1. PEN TESTING-ESSENTIAL (PT-E)

Identifies high-risk vulnerabilities in web applications and web services, which automated scanners generally do not find. Includes automated scans as well as thorough manual testing focused on exploratory risk analysis. This is ideal for critical applications, especially those undergoing major changes.

2. PEN TESTING-STANDARD (PT-S)

In addition to everything Pen Testing-Essential offers, experts dedicate additional time and effort to exploring deeper business logic testing, which covers attacks outside of a canned list or attacks that may not have been considered otherwise.

Security testing that emphasizes an adversarial approach

4 steps to a successful pen test

1. **Reconnaissance.** We review your applications to find vulnerabilities.
2. **Scanning.** We probe for vulnerabilities using up to 20 different automated tools and manual techniques. We use targeted tools to effectively test application technologies/frameworks.
3. **Exploitation.** We perform deep exploratory risk analysis to bypass any existing security controls (such as WAF, Input Validation etc.) We attempt to abuse your business logic and user authorization to demonstrate exactly how security vulnerabilities could allow threat agents to gain access and cause damage.
4. **Remediation**. At the end of each assessment we will conduct a live read-out with the appropriate development team to review each vulnerability identified during the assessment, answer any questions that the team might have around each vulnerability and also discuss mitigation/remediation strategies.

92% of reported vulnerabilities are in applications, not networks.

-NIST

The Synopsys Difference

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software.

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com