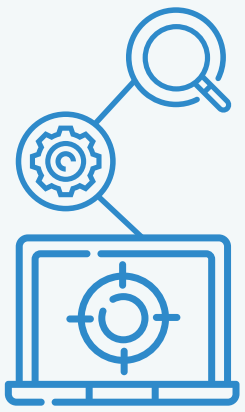
APPSEC TESTING APPROACHES

SCANNERS



Scanners work best when highly customized to a particular environment or application. They will find everything you program them to search for and nothing you don't. For this reason, while they are well-suited to looking for a specific, predefined set of vulnerabilities, they cannot find design and more complex logic issues that more manual human testing can uncover. Scanners can be particularly useful for in-house tasks such as a static code analysis of application source code.

SCALABILITY	COVERAGE	EASE-OF-USE	COST
• High for homogeneous environments	• Predictable and programmable	• Require customization • Triage of identified issues (removal of false positives) requires manual effort • Low signal-to-noise on automatic results	• Varies; can be free to expensive

AT A GLANCE

- **Programmable with consistent, scalable results**
- **Most powerful when customized**
- **Used in conjunction with FTEs who can filter results and remove false positives**
- **Can be free to expensive**

PUBLIC BUG BOUNTIES

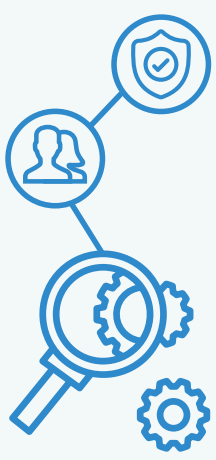
Public Bug Bounties offer human creativity and fast results. Application security teams can open a public-facing application to a bug bounty and attract many researchers to it in a short amount of time who will typically find most low-hanging fruit. It is a highly scalable means of manual testing, but researcher credentials and code coverage will be undefined and unknown. Bug bounties can be particularly helpful for security teams needing a quick review for obvious issues in public-facing applications or for those looking to establish a formal, public channel with external researchers.

SCALABILITY	COVERAGE	EASE-OF-USE	COST
• High	• Can potentially examine a large volume, but actual coverage will be undefined and unknown	• Fast, simple test initiation • Triage of identified issues will be manual; communication with researchers requires a high level of effort • Unpredictable signal-to-noise on reported results	• Variable, pay for each new bug found

AT A GLANCE

- **Human Creativity**
- **Globally sourced**
- **Unknown Researcher Qualifications**
- **Paid-by-finding**

PENTESTING AS A SERVICE (PTAAS)



Pentesting as a Service (PtaaS) provides on-demand manual penetration testing for web applications, mobile applications, APIs, external networks, and cloud services. Findings are delivered through a platform that integrates with developer tracking systems like JIRA and GitHub. A SaaS platform also facilitates collaboration between pentesters, security team members, and development teams to not only find but also fix issues.

SCALABILITY	COVERAGE	EASE-OF-USE	COST
• High	• Defined, focused and procedural (e.g., OWASP Top 10)	• Fast test initiation with streamlined researcher onboarding • Supported triage with ongoing developer-researcher communication • High signal to noise on reported results	• Predictable, fixed price

AT A GLANCE

- **Human Creativity**
- **Globally sourced**
- **Researchers vetted and credentialed Supported triage process**
- **Time-boxed and fixed price**