aa teknoloji

# Application Security Testing

The application security testing service for detecting vulnerabilities in web, mobile, and API applications provides secure software development lifecycle support to development and security teams with a manual test-oriented analysis approach. It is supported by SAST, DAST, and SCA outputs.

## Application Security Challenges

The increasing speed, microservice architectures, and the need for continuous integration in today's software development processes turn security into an element that is pushed to the background. Organizations struggle to manage security sustainably between regulatory pressure and data breach risks.
Invisible security vulnerabilities in web, mobile, and API-based applications, especially authentication, authorization, and business logic flaws, pose serious risks. The lack of systematic execution in manual security tests makes detecting such critical vulnerabilities difficult; SAST, DAST, and SCA outputs strengthen this process as supporting factors.
The fragmented and manual progress of testing processes slows down scalable security evaluations and increases the risk of critical security vulnerabilities leaking into production environments.

⚠ Who can benefit?

- Early detection of security vulnerabilities for development and DevOps teams
- Integrated management of SAST, DAST, SCA, and manual testing processes
- Minimizing critical security vulnerabilities before production for organizations
- Centralized risk management in web and API applications for security teams

### Core Principles

**Early Detection**
Manual detection of security flaws at an early stage

**Integration**
Integrated management of SAST, DAST, and SCA processes

**Risk Mitigation**
Minimizing critical vulnerabilities prior to production

**Centralized Analysis**
Unified management of all application security risks

## Technical Specifications

### Access and Installation

- Secure access model for the testing environment
- Role-based test authorization architecture
- Rapid scope definition and commencement
- Testing support for multiple applications

### Authentication

- Multi-factor authentication support
- API testing and token-based secure access mechanism
- Controlled access with session management
- Role separation according to authorization levels

### Integrations

- Structure compatible with manual security test processes
- Supporting use of SAST, DAST, and SCA outputs
- Secure integration with external systems
- Centralized management support for security findings

### Test and Analysis

- Web, mobile, and API application support
- Analysis approach focused on manual penetration tests
- Vulnerability analysis aligned with OWASP standards
- CVSS and CWE-based risk assessment

### Reporting and Monitoring

- Real-time security finding reporting
- Detailed technical and executive report outputs
- Vulnerability lifecycle tracking
- Traceability via centralized dashboard

## How Does the Application Security Testing Service Work?

The application security testing service detects vulnerabilities with end-to-end analysis by placing manual security tests at the center of web, mobile, and API applications. The process is conducted in three main stages: discovery, analysis, and reporting, and it is supported by SAST, DAST, and SCA outputs.

### Workflow

**1. Discovery and Scoping**
- Application surface and attack area are determined.
- Web, mobile, and API components are inventoried.
- Authentication and authorization flows are examined.
- Test scope is correlated with the threat model.

→

**2. Security Analysis**
- Business logic and authorization flaws are tested.
- Manual penetration controls are performed according to OWASP scenarios.
- Attack scenarios are analyzed through impact assessment.
- Static, dynamic, and dependency analysis outputs are evaluated.

→

**3. Verification and Reporting**
- Findings are verified in a reproducible manner.
- Risk scoring and classification are performed with CVSS and CWE.
- Attack scenarios are verified in critical functions.
- Remediation recommendations are provided for security flaws.

**Continuous Security Approach**
Application security tests are continuously improved with regularly updated threat scenarios. Adaptation to new vulnerability types is achieved, the testing scope is expanded, and security assessments are made repeatable.

## Advantages

**Manual Security Tests**
Verifies business logic and authorization flaws that automated tools might miss, through manual penetration tests.

**SAST, DAST, and SCA Analysis**
Analyzes security vulnerabilities comprehensively across source code, running applications, and dependency layers to reveal risks.

**Risk-Based Prioritization**
Prioritizes critical security vulnerabilities by classifying findings based on CVSS and CWE, making it easier to take action.

**Single Point Security View**
Reports and makes traceable all security findings across web, mobile, and API applications from a centralized location.

aa teknoloji

AA Teknoloji is an AI-powered media technologies platform developed for modern newsrooms. Our integrated solutions, ranging from news workflow systems to digital archive solutions, real-time broadcasting infrastructure to multi-channel content management, accelerate the digital transformation processes of media organizations and offer scalable broadcasting operations.

For more information, visit aateknoloji.tr or follow the @aateknoloji LinkedIn account.