# Kaspersky Application Security Assessment

kaspersky

Whether you develop corporate applications internally, or purchase them from third parties, you'll know that a single coding error can create a vulnerability exposing you to attacks resulting in considerable financial or reputational damage. New vulnerabilities can also be generated during an application's lifecycle, through software updates or insecure component configuration, or can arise through new attack methods.

Kaspersky Application Security Assessment Services uncover vulnerabilities in applications of any kind, from large cloud-based solutions, ERP systems, online banking and other specific business applications, to embedded and mobile applications on different platforms (iOS, Android and others).

### Service Benefits

Kaspersky Application Security Assessment Services help application owners and developers to:

- Avoid financial, operational and reputational loss, by proactively detecting and fixing the vulnerabilities used in attacks against applications
- Save remediation costs by tracking down vulnerabilities in applications still in development and test, before they reach the user environment where fixing them may involve considerable disruption and expense
- Support a secure software development lifecycle (S-SDLC) committed to creating and maintaining secure applications

Combining practical knowledge and experience with international best practices, our experts detect security flaws which could expose your organization to threats including:

**Syphoning off confidential data**

**Infiltrating and modifying data and systems**

**Initiating denial of service attacks**

**Undertaking fraudulent activities**

Following our recommendations, vulnerabilities revealed in applications can be fixed, and such attacks prevented.

## Service Scope and Options

Applications assessed can include official web sites and business applications, standard or cloud based, including embedded and mobile applications.

The services are tailored to your needs and application specifics, and may involve:

- Black-box testing – emulating an external attacker
- Grey-box testing – emulating legitimate users with a range of profiles and analysis of application business logic
- White-box testing – analysis with full access to the application, including source codes; this approach is the most effective in terms of revealing numbers of vulnerabilities
- If Web Application Firewall (WAF) systems are used for application protection, they can be switched to monitoring mode or activated and respond to attacks (in this case, the work is performed in two stages: with protection disabled and in active mode to verify the identified findings).

## Results

Vulnerabilities which may be identified by Kaspersky Application Security Assessment Services include:

- Flaws in authentication and authorization, including multi-factor authentication
- Code injection (SQL Injection, OS Commanding, etc.)
- Logical vulnerabilities leading to fraud
- Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
- Use of weak cryptography
- Vulnerabilities in client-server communications
- Insecure data storage or transferring, for instance lack of PAN masking in payment systems
- Configuration flaws, including ones leading to session attacks
- Sensitive information disclosure
- Other web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and the OWASP Top Ten.

Results are given in a final report including detailed technical information on the assessment processes, results, vulnerabilities revealed and recommendations for remediation, together with an executive summary outlining management implications. Videos and presentations for your technical team or top management can also be provided if required.

# About Kaspersky's Approach to Application Security Assessment

Security assessments of applications are performed by Kaspersky security experts both manually and through applying automated tools, with full regard of your systems' confidentiality, integrity and availability and in strict adherence to international standards and best practices, such as:

- Web Application Security Consortium (WASC) Threat Classification
- OWASP Web Security Testing Guide
- OWASP Mobile Security Testing Guide
- Other standards, depending on your organization's business and location

Project team members are experienced professionals with a deep, current practical knowledge of the field, including different platforms, programming languages, frameworks, vulnerabilities and attack methods. They speak at leading international conferences, and provide security advisory services to major vendors of applications and cloud services, including Oracle, Google, Apple, Facebook and PayPal.

# Delivery Options

Depending on the type of security assessment service, the specifics of the systems in scope, and your requirements for working conditions, security assessment services may be provided remotely.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

**www.kaspersky.com**



#kaspersky
#bringonthefuture