WEB APPLICATION PENETRATION TEST

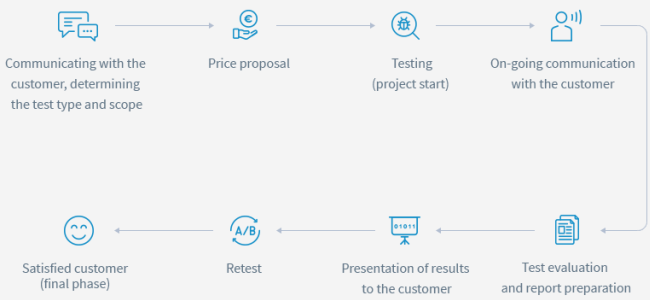
Web applications play an important role in today's business. These applications are often vulnerable to many types of attacks that may result in stolen data, or the execution of an malicious code with the permissions of the webserver.

Our team of professionals has experience of testing all kinds of web applications from small presentation websites, e-shops, CMS, e-commerce, API services, and Web Services to Internet banking and robust large portals.

We offer several types of web application penetration tests that vary in the scope and depth of the test. After discussing with the customer, we recommend the type and scope of appropriate test for the specific application.

This price is determined after customer consultation, which determines the scope, type of test, and other requirements from the customer.

The penetration test can be adapted to the CWE/SANS Top 25, ASVS, WASC 26 Classes Testing methodologies/standards.



GENERAL SERVICE OVERVIEW

The purpose of the web application penetration test is to discover vulnerabilities in web applications, demonstrate the exploitation of identified vulnerabilities, identify their risk, and recommend solutions to eliminate them.

The penetration test results in a report that does not contain any "false-positive" findings, but only verified vulnerabilities.

The penetration test can be performed using the BLACK BOX (no information about the tested environment), GRAY BOX (partial information about the tested environment) or WHITE BOX (full information about the tested environment, including the source codes of the application) method.

The cost of the penetration test depends on the size and complexity of the tested application.

WEB APPLICATION PENETRATION TEST ACCORDING TO OWASP TESTING GUIDE V4.0 METHODOLOGY

Deep penetration test according to the OWASP testing guide v4.0 methodology is designed for those who want to thoroughly test the security of their application in detail. It is suitable for large projects, critical web applications, and where strong emphasis is placed on security. The test is performed using commercial and open source tools, scripts, and tools written within the company.

The penetration test according to the OWASP testing guide v4.0 methodology includes:

- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing

- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for weak Cryptography
- Business Logic Testing
- Client Side Testing

WEB APPLICATION PENETRATION TEST ACCORDING TO THE OWASP TOP 10 2017

The OWASP Top 10 contains 10 vulnerability categories that are most common in web applications. These vulnerabilities are usually easy to identify and exploit. They pose a risk, since these vulnerabilities allow an attacker to steal data from the database or file system, gain control over a user account or execute (malicious) code of his choice with the permissions of the webserver.

The penetration test according to the OWASP Top 10 2017 consists of:

- A1 – Injection
- A2 - Broken Authentication
- A3 - Sensitive Data Exposure
- A4 - XML External Entities (XXE)
- A5 - Broken Access Control
- A6 - Security Misconfiguration
- A7 - Cross-Site Scripting (XSS)
- A8 - Insecure Deserialization
- A9 - Using Components with Known Vulnerabilities
- A10 - Insufficient Logging & Monitoring

AUTOMATED TEST

The test is performed using automated tools (scanners). After the automated test is completed, the results are manually verified and false-positive findings are removed. Automated tests only test basic security and are therefore only suitable for web applications that are not critical from a business perspective. The purpose of this test is to prevent attacks by inexperienced attackers (script-kiddies) or tools that constantly scan web applications and try to exploit any vulnerabilities.

AUTOMATED TEST WITH MANUAL TESTING

The test is performed using automated tools (scanners). After the automated test is completed, the results are manually verified and false-positive findings are removed. Unlike the "automated test," it's just the first phase of the test. The second phase of the test involves a manual identification of vulnerabilities from the OWASP TOP10 2017 over a limited time horizon, which depends on the size and functionality of the application. The purpose of this test is to prevent attacks by inexperienced attackers (script-kiddies), slightly experienced attackers, or tools that constantly scan web applications and try to exploit any vulnerabilities. This test is suitable for non-critical web applications.

MICROTEST (FLASH) TEST

This is a quick and time-limited test performed within few hours or days depending on the size and and functionality of a tested application. During the penetration test, vulnerabilities from the OWASP TOP10 2017 are sought to "find as many vulnerabilities as possible in a short time". The goal of the test is to quickly assess the security of the application.

LONG-TERM TEST (ADDITIONAL SERVICE)

With the emergence of new attack vectors, vulnerabilities and new security circumvention techniques, we offer the additional "long-term test" service after the penetration test. The long-term test consists of a short-term intensive test (for example one day duration) conducted every month for the duration of the service.