

## Objective

AppSec Consulting will certify applications' security by following a standardized procedure. Applications and their components will be reviewed to ensure that they are in compliance with various security parameters.

## Scope

The certification will look at security implementations of different aspects of the application and will cover

- Application Configuration
- Authentication
- Authorization
- Data validation
- Data privacy
- Session management
- Exception handling
- Information Leakage

The certification does not presume any specific vendor's technology that might be included in the application architecture. The checks are generic and can apply to any platform or language.

## Certification Procedure

The certification process involves performing a thorough audit of the application to identify existing and potential issues. AppSec Consulting has developed extensive checklists that comply with [OWASP](#)<sup>1</sup> and [NIST](#)<sup>2</sup> standards and the security of the application will be verified against these. Each certification area will typically consist of multiple tests to evaluate different aspects of that function. Every identified issue will be assigned a threat rating of Low, Medium or High based on the DREAD<sup>3</sup> method.

Supporting documentation will be required from the client for some of the items in the checklists while others will be verified by conducting a vulnerability assessment of the application. The assessment will be conducted using commercial and open source tools as well as manual testing techniques. AppSec Consulting will provide a list of required documentation at the start of the certification process.

## Remediation

Items that receive a DREAD threat rating of Medium or High will require remediation by the application owners. AppSec Consulting will usually suggest solutions for remediation that can be used by the customer. The remediation must be verified before the application is certified. The timeline for the verification will be determined when the report is presented at the end of the first vulnerability assessment.

<sup>1</sup> Open Web Application Security Project

<sup>2</sup> National Institute of Standards and Technology

<sup>3</sup> A standardized method for evaluating risk from threats



## AppSec Certified™ Security Certification

### Validity

The certification will be a snapshot in time and will be for a specific version of the application and its components. Changes to the application, its components or the environment will invalidate the application's security certification.

### Platform

For AppSec Consulting to certify an application as secure, the entire suite of tests must be performed. It is strongly recommended that the vulnerability assessment of the application be performed in a testing environment that mirrors the production environment with the same application code base.

