Build Security In, Before the Building Begins

The OWASP Secure Software Development Contract Annex helps software developers and their clients negotiate and capture important contractual terms and conditions related to the security of the software to be developed or delivered. Most contracts are silent on these issues, and the parties frequently have dramatically different views on what has actually been agreed to. Clearly articulating these terms is the best way to ensure that both parties can make informed decisions about how to proceed. There are currently versions in English.

Build security in using a contract:

- Define security-related life cycle activities
- Define security requirement areas
- Require security analysis and testing using an agreed-upon standard (such as the OWASP ASVS).

Contact a Qualified Attorney, but Bring the Contract Annex With you!

The OWASP Secure Software Development Contract Annex is guidance, but it's guidance that you should take with you when you talk to a qualified attorney to negotiate and capture important contractual terms and conditions related to the security of the software to be developed or delivered.

The Contract Annex is a starting point for your agreement. You may not like all the activities, or may want to propose more. You may want to assign responsibilities differently. The Contract Annex is not intended to exactly capture the needs of all software Clients and Developers. It is intended to provide a framework for discussing the key topics that are important to ensuring that software ends up secure. After you have a security discussion and reach agreement, you should tailor this agreement to match.

What are the Benefits of Negotiating and Capturing Security-Related Terms and Conditions?

There are many benefits to working through the OWASP Secure Software Development Contract Annex. The principal one is that it will make expectations clear between the parties involved. In some cases it will help to prevent lawsuits when difficult security problems surface in the software. Also, these are the same activities that are required by many legal and regulatory compliance reasons.

The goal of the Contract Annex is simply to ensure, at each stage of the lifecycle, that appropriate attention has been paid to security. An additional benefit is that this documentation can be collected together to form a "certification package" that essentially lays out the argument for why this software should be trusted to do what it claims it does.

Project Sponsors

The OWASP Legal project is sponsored by:

ASPECT SECURITY
Application Security Specialists