OWASP Alchemist

The Problem

A large majority of software projects do not incorporate security from the word go. Usually it comes as a later and lighter process in the SDLC, worse as an afterthought or a quick-fix! While it is easier to say and expect adoption of better and superior software security practices in an SDLC, the reality is a lot different. With the ever changing landscape of software development industry and the innovations that seep in every day, it is probably too much to keep up with them for the software community. It is a known and accepted truth that a later-in-the-cycle approach, worse a quick-fix approach, turns out expensive, ineffective and usually non-implementable often leading to frustration, wasted time and massive security holes.

How Alchemist helps solves this problem?

Alchemist intends to help solve this conundrum, by enabling a software development team in realization of highly secure and defensible application with built-in defenses/controls against security-related design, coding and implementation flaws. Alchemist is focused to present this solution by way of architecting a real-life high stakes software application in J2EE (Spring/Struts) with security built into it right from the inception, step-by-step as it falls under an SDLC. Although this project is more than useful for existing/already developed applications, Alchemist is not the ideal solution to retrofit security into existing applications. It is aimed at offering more to applications that are at least in development, most in design phase. Allowing for language-specific differences, Alchemist builds this application with a strong foundation of security architecture that covers following main practices:

- Security Requirements
- Threat Risk Modeling
- Use and Abuse Cases
- Secure Coding Guideline

Alchemist Roadmap

ALPHA RELEASE: A real-world banking application with 5 dynamic pages.

Provisional Release Date: 13th December 2010

Release Includes

- Design Patterns
- Security Requirements Document
- Threat Risk Model
- Use and Abuse Case Document
- Secure Coding Guide

BETA RELEASE: The banking application extended to 10 dynamic pages.

Provisional Release Date: 28th February 2011

Release Includes

- Incorporate suggestions and feedback from alpha release
- Fix reported bugs and flaws
- Updated Design Patterns, Security Requirements Document, Threat Risk Model, Use and Abuse Case Document and Secure Coding Guide

STABLE RELEASE: A real-world banking application with 13 dynamic pages.

Provisional Release Date: 16th May 2011

Release Includes

- Incorporate suggestions and feedback from alpha release
- Fix reported bugs and flaws
- Updated Design Patterns, Security Requirements Document, Threat Risk Model, Use and Abuse Case Document and Secure Coding Guide

Misc.

Licensing: GNU GPL

Project Leaders:

Bishan Singh (c70n3r@gmail.com)

Chandrakanth Narreddy (chandra.kanth@hotmail.com)

Naveen Rudrappa (Naveen.rudra02@gmail.com)