Deploying Secure Web Applications with OWASP Resources

Fabio E. Cerullo

OWASP Ireland, Ireland
fabio.e.cerullo@aib.ie

Secure applications do not just happen – they are the result of an organization deciding that they will produce secure applications. OWASP's does not wish to force a particular approach or require an organization to pick up compliance with laws that do not affect them as every organization is different.

However, for a secure application, the following at a minimum are required:

- Organizational management which champions security
- Written information security policy properly derived from national standards
- A development methodology with adequate security checkpoints and activities
- Secure release and configuration management

Many of the tools, documentation and controls developed by OWASP are influenced by requirements in international standards and control frameworks such as COBIT and ISO.

Furthermore, OWASP resources can be used by any type of organization ranging from universities to financial institutions in order to develop, test and deploy secure web applications. This presentation will introduce you to some of the most successful projects such as:

- OWASP Enterprise Security API which can be used to mitigate most common flaws in web applications;
- OWASP ASVS which is intended as a standard on how to verify the security of web applications;
- OWASP Top 10 which helps to educate developers, designers, architects and organizations about the consequences of the most important web application security weaknesses;
- OWASP Development Guide which shows how to architect and build a secure application;
- OWASP Code Review Guide which shows how to verify the security of an application; source code;

OWASP Testing Guide which shows how to verify the security of your running application.

Finally, as OWASP believes education is a key component in building secure applications, some of the initiatives being carried out by the OWASP Global Education Committee are going to be highlighted.