The OWASP Application Security Code of Conduct for Development Organizations

(The OWASP "Gray Book")

Version 1.13 (26th June 2012)

Introduction

Software applications are at the heart of most information systems and business processes. Organizations rely on these applications to undertake their business and process valuable data, yet the applications often have weak, or poorly selected, security mechanisms. Organizations that want to develop software must ensure that the users of their code are protected. Development organizations may be developing their own software or producing software for use by others. OWASP has unparalleled resources available to help organizations acquire, develop and operate applications securely.

Code of Conduct

1. **The Development Organization MUST have an application security awareness program for software developers and managers.**

   Training is a fundamental starting point for any software security initiative. The application security training for software developers, architects, managers, and other information technology staff should be tailored to the student's role. The training should include guidance on the importance of application security to the business as well as both conceptual and technical information. It must be linked with the organization's standards, technologies, controls, processes, compliance requirements and the relevant risks.

2. **The Development Organization MUST identify and mitigate application security risks as a core part of their software engineering process.**

   The identification and mitigation of application security risks must be addressed through activities that fit into each development team's engineering processes. Commonly they would include steps to assess threats, define security requirements, develop secure architectures and undertake secure coding practices. OWASP does not specify what these should be precisely nor how they should be performed; each organization/team can define what fits their risks, process and culture.

3. **The Development Organization MUST independently verify that appropriate security controls are present, rugged, and used properly in every application.**

   Whatever security controls are identified, development teams must get independent assurance there are processes in place to verify them. This verification is likely to include security code review, security testing, security architecture review, threat modeling, code release integrity checks, configuration checks, audits, vulnerability management, etc. These activities are most cost effective when performed throughout the development lifecycle, as opposed to a big review before delivery. As risks change over time, and as code undergoes changes, it is also important these activities continue and are managed throughout operational life of the application as well.

Recommendations

A. **The Development Organization SHOULD build application security into software acquisition processes.**

   Software development utilizes frameworks, modules, libraries, components and other code from third parties. Some development may be sub-contracted or outsourced. The organization should

have a process to define security requirements, ensure integrity in the supply chain and to evaluate software before purchase or use; this may require some contract language. We do not suggest what this language should contain, but point to our Software Security Contract Annex[i] as a possible starting point.

B. The Development Organization SHOULD be an OWASP Supporter.

The main benefit of becoming an OWASP Supporter[ii] is to demonstrate your belief that application security is important and that you are working to build a robust information-age economy and providing a suitably skilled workforce that attracts investment. In addition, your support goes directly to help researchers drive progress in application security to help protect the entire information technology ecosystem.

C. The Development Organization SHOULD assign a liaison to OWASP.

OWASP has a group that focuses on improving application security in organizations that undertake development. The group collaborates via email and at OWASP events worldwide. We expect the liaison to monitor the list and participate as much as they care to. The organization can define their level of participation.

D. The Development Organization SHOULD encourage relevant trade organizations to focus on application security.

Improving application security across a whole sector benefits all organizations by increasing the skills of the available workforce and by raising standards in the software supply chain. It could also reduce the risk of increased legislation and regulation. We believe that organizations in all sectors have the ability to influence their peers and raise standards in their markets. They can influence their own trade organizations to focus on application security and hopefully get in line with the OWASP Code of Conduct for Trade Organizations ("The OWASP Purple Book")[iii].

E. The Development Organization SHOULD leverage OWASP by attending our events, using our materials, and asking our experts for help.

OWASP has a lot to offer organizations that undertake development. We have freely available tools, documents, guidelines, and standards. We have worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in training courses. We even have packaged curricula, eLearning, and educational materials that are available for development teams to use and modify free of charge. Organizations are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

References

i. Software Security Contract Annex, OWASP
https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

ii. Membership, OWASP
https://www.owasp.org/index.php/Membership

iii. OWASP Code of Conduct for Trade Organizations ("The OWASP Purple Book")
https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#tab=Trade_Organizations

OWASP Application Security Codes of Conduct

In order to achieve our mission, OWASP needs to take advantage of every opportunity to affect software development everywhere. At the OWASP Summit 2011 in Portugal, the idea was created to try to influence educational institutions, government bodies, standards groups, trade organizations and groups active in the application security space. We set out to define a set of minimal requirements for these organizations specifying what we believe to be the most effective ways to support our mission. We call these requirements a "code of conduct" to imply that these are normative standards, they represent a minimum baseline, and that they are not difficult to achieve.

Organizations wishing to announce their compliance with this Code of Conduct should read the associated information on statements of compliance:

https://www.owasp.org/index.php/OWASP_Codes_of_Conduct#compliance

Special thanks to Jeff Williams and Colin Watson for creating this document, ??? and ??? for reviewing it, and to all the participants in the working sessions on Outreach to Educational Institutions, and Minimal AppSec Program for Universities, Governments and Standards Bodies at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.

https://www.owasp.org/index.php/OWASP_Codes_of_Conduct

About OWASP

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

https://www.owasp.org