The OWASP Application Security Code of Conduct for Standards Groups

(The OWASP "Yellow Book")

Version 1.1 (20th July 2011) Draft

Introduction

The world of information technology is driven largely by standards groups such as BS, ENISA, IETF, ISO, ITU, NIST, OASIS, PCI SSC, W3C, and many more. We believe that every technical standard that involves software in any way should take the time to consider possible application security risks and, if necessary, address them in the standard. OWASP is ready to work with standards groups and has considerable resources to help standards groups make good decisions and get application security right.

Code of Conduct

1. **The Standards Group MUST include an "Application Security" section in each software related technical standard.**

   We believe that the most important way to ensure that application security is considered during the development of any technical standard related to software is to require a section focusing on that topic. Even for standards that do not have any need for specific application security requirements, the process of considering possible application security implications and documenting the outcome is a critical part of the standards creation process.

2. **The Standards Group MUST provide OWASP a "notice and comment" period when releasing standards that include an application security aspect.**

   OWASP wants to help standards groups create strong standards that will secure technologies. Ideally, we would be involved from the beginning in the creating of the standard, but we believe it is critical that we have an opportunity to provide comments and guidance to help shape the final result.

Recommendations

A. **The Standards Group 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 help your constituents properly address application security in the projects affected by the standards you develop.

B. **The Standards Group SHOULD assign a liaison to OWASP.**

   OWASP has a group that focuses on improving application security in standards. 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 standards group can define their level of participation.

C. **The Standards Group SHOULD define or adopt a definition of Application Security.**

   Without a definition of application security, standards groups may struggle with whether a particular issue should be covered or not. We do not try to mandate a single definition of application security for all standards groups. Rather, we simply suggest that standards groups must have such a definition in place. We recommend using OWASP as a way to help figure out what that definition should encompass.

D. The Standards Group SHOULD leverage OWASP by attending our events, using our materials, and asking our experts for help.

OWASP has a lot to offer standards groups. We have freely available tools, documents, guidelines, and standards[ii]. We have worldwide events that are open to everyone and all the presentations are recorded. Participants are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

E. The Standards Group SHOULD involve a security expert early in their standard definition process.

Organizations creating standards may want to include a security expert to assist throughout the process of creating a standard. While OWASP does have experts with a very broad array of expertise, we may not understand your domain fully. However, we believe there is huge value in having a security expert available to assist with threat modeling, vulnerability analysis, risk assessment, and other security activities that should be applied during the creation of any technical standard.

References

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

ii. Projects, OWASP
https://www.owasp.org/index.php/Category:OWASP_Project

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.

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, Dave Wichers, and 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