The OWASP Application Security Code of Conduct for Certifying Bodies

(The OWASP "Red Book")

Version 1.1 (20th July 2011) Draft

Introduction

As understanding of application security becomes a critical part of an individual's skill set, organizations are eagerly seeking guidance in identifying knowledgeable individuals in application security. We believe that Certifying Bodies can play a role to empower organizations to identify security-minded individuals. While OWASP will ***never*** endorse or support any particular certification, we offer this code of conduct to help guide Certifying Bodies to better serve organizations that are ready to embrace an application security certification.

Code of Conduct

1. **The Certifying Body MUST NOT misrepresent the Certifying Body's certification as endorsed or supported by OWASP.**

   While OWASP recognizes the need of organizations to identify individuals with an understanding of application security, OWASP will not endorse any certifying body or their certification. One of the bedrock principles of OWASP is to maintain a vendor-neutral position and any endorsement of a certifying body or their certification is in direct contradiction of this core value. We respect your desire to fill a void in the application security space and expect that you will in turn respect our core values and brand name.

2. **The Certifying Body MUST include a visible disclaimer if the Certifying Body's certification is "based on OWASP materials".**

   OWASP will not allow our brand name to be used in the certification title. However, we welcome a Certifying Body to leverage tools, documents, guidelines, and standards that are freely available from OWASP[i]. We recognize that in such cases, a Certifying Body may wish to inform their audience that their certification is "based on OWASP materials". We are honored by your desire to leverage OWASP materials, but we ask that you honor the OWASP name and clearly disclaim that your use of OWASP materials does not represent an endorsement or association with OWASP.

Recommendations

A. **The Certifying Body SHOULD collect and publish feedback from certification applicants, recipients, and organizations recognizing the certification.**

   Certifications represent the Certifying Body's assertion that the recipient meets some minimal criteria, as defined by the Certifying Body. Organizations depend on that assertion when recognizing a Certifying Body's certification. We believe that organizations need feedback to effectively determine the value of a certification. We do not suggest what feedback should be solicited, nor the exact form or method for this publication; only that it represents your desire to honestly communicate the value and esteem or your certification.

B. **The Certifying Body SHOULD utilize questions, answers, evaluation material and processes that are open and freely available to the general public.**

   Organizations around the world are depending on certifying bodies to help identify individuals that understand application security. Supplying open questions and answers allows organizations

to evaluate for themselves whether or not a certification adequately satisfies their need. We ask you publish the bank of all questions and answers for any examination-based certification. We do not specify the exact form or method for administering the exam nor for publishing the questions and answers; only that it represents your desire to enable organizations to understand and evaluate the substance of your examination as it pertains to their organizational needs. OWASP suggests that the certifying body uses questions and answers developed by the OWASP community.

C. The Certifying Body 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 improve the state of application security in the world.

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

OWASP has a lot to offer certifying bodies. 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 classrooms. We even have packaged curricula, eLearning, and educational materials that are available for potential applicants to use and modify free of charge. Certifying bodies are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

References

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

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

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 Jason Taylor and Jason Li for creating this document, and to all the participants in the work session on Certification 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