OWASP
Open Web Application
Security Project

OWASP GUIDEBOOKS

PROJECT CHARTER 2013

Project Charter Document History

Document Revisions

Author	Release Date	Reason for Changes	Version #	Approval
Samantha Groves	October 2013	Updates	2.0	Samantha Groves

Summary of Changes

Version	Release Date	Summary of Changes
2.0	October 2013	Minor edits to all sections, proofreading, and layout adjustment.

Distribution History

This document has been distributed to the following people:

Author	Title	Company	Distribution Date	Distributed Version #
			October 2013	2.0

Table of Contents

1. Executive Summary

The OWASP Foundation proposes to initiate the OWASP Guidebook Project, which involves the updating and consolidation of The Development Guide, The Code Review Guide and The Testing Guide. These three books were developed in the past by OWASP volunteers as separate projects. These three projects make up the foundation of a security development life cycle for web applications. The Development Guide provides developers with specific instructions on writing secure code in their applications. Once that code is written, the Code Review Guide and the Testing Guide provide systematic steps in performing security assessments of a completed project, both from a code review and a penetration testing perspective. The aim of the OWASP foundation is to consolidate these three guides into one easily accessible book. It is our goal to help governments, businesses, developers, designers and solution architects to produce secure web applications.

2. General Project Information

Project Title: OWASP Guidebooks Project

Project ID: OGP

Sponsoring Organization: Department of Homeland Security and Georgia Tech Institute

Sponsor Representative: Deborah Bryant

Prepared by: Samantha Groves, OWASP Projects Manager

Version: 2.0

3. Project Stakeholders

Below is a list of all applicable project stakeholders.

Position	Name	Organization	E-mail
Project Manager: Program Manager Role	Samantha Groves	OWASP	Samantha.Groves@owasp.org
Project Manager/Leader/ Testing Guide	Andrew Muller	OWASP	Andrew.Muller@owasp.org
Project Manager/Leader/ Testing Guide	Matteo Meucci	OWASP	Matteo.Meucci@owasp.org
Project Manager/Leader/ Development Guide	Andrew van der Stock	OWASP	vanderaj@owasp.org
Project Manager/Leader/ Code Review Guide	Larry Conklin	OWASP	Larry.Conklin@owasp.org
Project Manager/Leader/ Code Review Guide	Eoin Keary	OWASP	Eoin.Keary@owasp.org

4. Project Purpose

Security is an essential component of any successful web application, whether the site is an open source project, a web service using straight through processing, or critical infrastructure process designed to provide critical services to local or global communities. Hosting companies (rightly) shun insecure code, and users shun insecure services that lead to fraud. The aim of these guides is to help governments, businesses, developers, designers and solution architects to produce secure web applications consistently and thoroughly. If done from the earliest stages, secure applications cost about the same to develop as insecure applications, but are far more cost effective in the long run. Unlike other forms of security (such as firewalls and secure lockdowns), web applications have the ability to make a skilled attacker rich, or make the life of a victim a complete misery. The guidebooks aim to provide a comprehensive manual for designing, developing, and deploying web applications thereby decreasing the risk of developing insecure applications.

4.1 Business Issues

At this highest level of the OSI software map, traditional firewalls and other controls simply do not help. The application itself must be self-defending. The Guides will be written to cover all forms of web application security issues, from old hoary chestnuts such as SQL Injection, through modern concerns such as AJAX, phishing, credit card handling, session fixation, cross-site request forgeries, compliance, and privacy issues. The Development Guide is aimed at architects, developers, consultants and auditors and is a comprehensive manual for designing, developing and deploying secure Web Applications and Web Services. The finished guides will be promoted and be freely available to everyone for download and consumption.

4.2 Business Objectives

The business objectives section of this charter illustrates the correlation of a project business objective to that of an element within the overall strategic plan of the sponsoring organization. Every objective should relate to at least one strategic element.

Strategic Plan Element	Project Business Objective
Development of Open Source Materials	All Guides are open source and freely available to all.
Promote the use of Open-Source Technologies	Most of the technologies reviewed or mentioned in the guides are open source.
Development of Open Source Security Capabilities	The guides instruct readers how to best develop web applications using a holistic approach towards software security.

5. Project Overview

5.1 Project Description

The primary aim of the OWASP Guidebooks Project is to deliver three books based on the original Development Guide, Code Review Guide, and Testing Guide. Moreover, a major goal of this project is to develop a high quality deliverable, reviewed by industry peers using OWASP Project assessment quality criteria. We aim to complete this project by allocating and seeking out funds to help our project managers/leaders successfully complete a high quality guide for the OWASP Foundation.

5.2 Scope

The major measurable outcome that will result from completion of the OWASP Guidebooks Project are three (3) new release candidates of each guide that will be published and promoted within the community. All three guides will be consolidated into one book which will encompass the entire product development cycle for creating and testing applications.

The project aims to change software security as it will aid developers and testers, among other stakeholders, with understanding modern issues related to web application security. Based on leading practice and written by many experts, the OWASP Guidebooks will provide guidance to the software industry. Previous editions have made a significant impact within the industry over a period of 5 to 6 years, and we estimate that the updating and consolidation of these guides will continue to positively impact the industry for years to come.

5.3 Assumptions

1. Project Leaders will have enough free time to complete the books.
2. Our budget estimates are accurate.
3. The long project timeframe will mitigate the risk of low volunteer writer availability.
4. OWASP will continue to assist project work.
5. OWASP will have a dedicated Projects Manager to assist with Program activities.

5.4 Constraints

1. We are using volunteer writers to produce the content, and their time to work on this project is limited.
2. We are using volunteer project managers/leaders to produce the content, and their time to work on this project is limited.
3. We must produce the 3 updated guidebooks with the funds raised.
4. Project team is located across the globe so decisions/tasks may take longer to complete.
5. Consensus on decisions may take longer to complete as team is located across the globe.

6. Project Requirements & Deliverables

The major goal of this project is to develop a high quality deliverable, reviewed by industry peers using OWASP Project assessment quality criteria. OWASP aims to update their development, testing, and code review guides to encompass more up-to-date best practices and technologies. In order to do this, the project team will have to conduct an audit of the existing guides, figure out what is still relevant and what must be re-written, find writers and assign chapters to each, have a technical editor review the content, and have the final content professionally designed.

7. Project Management Milestones & Deliverables

A peer review of the updated and new sections of the OWASP Guidebooks will be required at the proposed 50% milestone. During this management stage, the OWASP community will be consulted for reviewers. This is where we suggest DHS consider their involvement, if at all possible, as we highly value the input and advice DHS representatives can offer to the project. The 50% milestone review will focus on accuracy and quality that will be agreed upon before project initiation,. At the 100% milestone review, a professional technical writer will be resourced to further establish accuracy, and ensure a high quality deliverable for the project.

The five specific project milestones are: Review of Current Material; Technical Authoring; Technical Editing; Graphic Design and Wikification; Promotion of Finished Guidebooks.

8. Project Budget & Costs

Budget Definitions

- Personnel - salaries, benefits and associated fringe costs
- Other Direct Expenses - communications/marketing, travel, meeting expenses, project space
- Purchased Services - consultant and/or third-party contractor costs
- Indirect Expenses - administrative expenses related to overall operations

Budget Category	HOST Support	OWASP Foundation	Total
Personnel			
Other Direct Expenses	$10,000		$10,000
Purchased Services	$15,000*	$10,000**	$25,000
Indirect Expenses			
Grant Total	$25,000	$10,000	$35,000

** airfare + hotel funding for core team to meet and work on the project.

* Graphic Design Services to create images of the software engineering diagrams necessary. The diagrams, in their native format, must be licensed to OWASP so we can reuse them as open source.

* Additionally, the funds will be used for purchasing project management, writing, and other necessary software.

9. Personnel & Other Resources

Below you will find a breakdown of the resources needed to reach completion for the project.

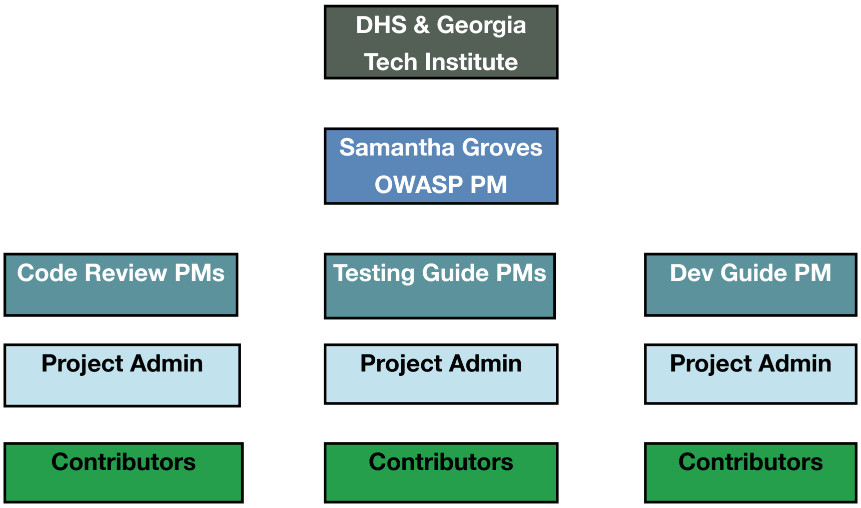
Resources	Description
Project Team	We need a dedicated Program Manager, Project Managers, Writers, Graphic Designers, Technical Editors, and Project Proofreaders.
Additional Funds	We required additional funding, which DHS provided, to hire out the majority of the writing, editing, design, and print work.
Administrative Support	Three project administrators were recruited to help keep project documentation filed, and to help the project managers with administrative work.
Equipment	Computers for each project participant: Provided by each participant.
Software Tools	Atlassian PM software and Scrivener writing software.
Project Summit Planning	Dedicated resource to plan project summit, arrange attendance for each contributor, and allocate funds where necessary.

10. Project Risks

1. We rely primarily on volunteer contributions for the project management and writing work.
2. Our project will be delayed if we do not have the funds necessary to proceed.
3. Project deadline might have to be extended due to the volunteer resource needed to complete crucial work.

11. Project Organization

11.1 Project Organization Chart



DHS & Georgia Tech Institute

Samantha Groves OWASP PM

Code Review PMs

Testing Guide PMs

Dev Guide PM

Project Admin

Project Admin

Project Admin

Contributors

Contributors

Contributors

11.2 Stakeholder Roles & Responsibilities

Stakeholder Title	Name	Roles and Responsibilities
Primary Organization	OWASP	Provide resources to deliver final product.
OWASP PM	Samantha Groves	Primary Responsibility for delivery of final product.
Project Project Managers	Larry Conklin, Eoin Keary, Andrew van der Stock, Andrew Muller, and Matteo Meucci	Delivery of 1 of 3 guidebooks.
Sponsoring Organizations	DHS & Georgia Tech Institute	Funding

12. Associated Documentation

1. Q1 Report to DHS
2. Q2 Report to DHS
3. Q3 Report to DHS
4. Project Gantt Chart
5. Original Grant Proposal