HOST Project Funding Questionnaire

Required Proposal Components

Please describe your project in narrative form using clear, simple prose. The topic statements listed under each section are required. You may include additional information as desired.

1 – Sponsoring Organization

- OWASP Guide Project
- OWASP Foundation
- Kate Hartmann
- Kate.hartmann@owasp.org
- 301-275-9403
- 9175 Guilford Road; Suite 300; Columbia, MD 20640

2 – Project Summary

In 200-400 words, please write a summary of your project. Include the amount of funding requested, the proposed start date and the estimated months required to complete the project.

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.

The funding is needed to secure resources for the re-development of the guides. Our primary objectives are to align the solutions to be complimentary, to release a high quality product, and to market them to increased adoption. The amount requested is $25,000 USD. The project would commence immediately, and we estimate that the time to completion will be eighteen months.

3 – Problem Statement

In 250-750 words, please describe the problem(s) this project will address:

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.

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.

Describe similar efforts that have been made in the past by your organization or other organizations to solve this problem and what results have been achieved. If past projects have failed, please explain why and how this project will be different.

1. The original OWASP Development Guide has become a staple diet for many web security professionals. Since 2002, the initial version was downloaded over 2 million times. Today, the Development Guide is referenced by many leading government, financial, and corporate standards and is the Gold standard for Web Application and Web Service security.
2. The testing Guide and the Code Review guide were last updated in 2008. This project will take the three most referenced security documents and update them to combat current issues. Additionally, collaboration of the project leaders to design a common numbering system across all phases will provide a powerhouse of reference material for today's security engineers.

4 – Solution Statement

Please describe your solution in detail, in both technical and non-technical terms.

We plan to redevelop and consolidate the guides to reflect modern threats, vulnerabilities and technologies.

Does your solution involve any technical innovations? If so, please explain what they are and what other innovations could be developed as a result.

The solution shall involve the latest approaches to building, defending and securing web applications and software. Many tools will be able to feed off this information and build test cases to reflect this body of knowledge.

What social benefit is expected to accrue to cyber security as a result of the solution and

how would it accrue based on the scope of the project?

The social benefit of secure application development is underestimated. Applications on the Internet control many of modern civilization's critical infrastructure and data. It is paramount to help secure such systems from attacks be it from organized crime or rogue nation states. Our goal with the OWASP Guidebook Project is to help those involved in creating secure systems by providing them with a comprehensive manual for designing, developing and deploying secure Web Applications and Web Services.

Are the innovations produced by this project contingent upon the successful completion of other related programs or projects? If so, how are they contingent and what are the projects?

Combining the Developers Guide, the Testing Guide and the Code Review Guide and bringing their content current in their guidance and their methodologies will make them applicable for today's modern applications. This project would also bring more unity between these three documents by providing continuity of application, thereby, providing a single source reference for all stages of the life cycle. The three guides will need to be updated and reviewed as separate guides, and then combined to create one piece of literature that encompasses the full web application development life cycle.

Goals:
Delivering high quality deliverable based on the three guides:

- Code Review Guide
- Testing Guide
- Development Guide

High quality meaning: Peer reviewed

The previous editions of all three guides were very well received and account for thousands of downloads. The goal of this project it to update these documents to reflect the current state of software development.

5 – Context

Describe the technical environment in which the problems exist.
What is the specific problem or core issue this solution would address?
How does the problem or issue relate to your organization and why is your organization qualified to undertake this project?

Statistics on vulnerable websites, exploits, compromises and defacements are staggering. Just some of the major web application breaches this year are: Sony, LinkedIn, Gawker, Git Hub, Apache, US Senate, Washington Post, AT&T and Electronic Arts. Simple patching of operating systems and firewalls do not fix the problem. Each web application is usually custom created, meaning these applications need to be individually tested and

re-programed to find and fix the vulnerabilities before they are exploited.

Combining the Developers Guide, the Testing Guide and the Code Review Guide, and bringing their content current in their guidance and their methodologies will make them applicable for today's modern applications. The goal of the OWASP Guidebook Project is to help architects, developers, consultants and auditors in designing, developing and deploying secure Web Applications and Web Services. This will help decrease the major web application breaches we so commonly see today.

OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problems because the most effective approaches to application security include improvements in all of these areas. OWASP is more than qualified to undertake this project as the organization, and its many industry contributors, have been involved with developing communications that help in securing web applications for more than 10 years. Moreover, the Developers Guide, The Testing Guide and The Code Review Guide are projects that have already been developed, and have been successful projects in isolation. They have been downloaded thousands of times throughout the years, and OWASP hopes to re-fresh the literature in the hopes of continuing to provide valuable information to the Information Security community.

6 – Activities

In 250-750 words, please describe (not just list) the activities of this project:

Connect each step of your work with your goals.

The major goals of the OWASP Guidebook Project are to deliver three books based on the original Development Guide, The Code Review Guide and The Testing Guide. Moreover, a major goal of this project is to develop a high quality deliverable, reviewed by industry peers using OWASP Project Release quality criteria.

The first step of our work will involve a review of the current versions of the documents. This will help us highlight any shortfalls in terms of modern technical advice or accuracy, and it will ensure the identification of accurate quality acceptance criteria. The second step will involve defining both the 50% and 100% milestones as a function of the identified sections to develop for each guide. Defining the milestones will help the project team keep track of the management stages and project accomplishments.

The next stages consist of the technical aspects of the project. The third step will involve designing the approach to each OWASP Guidebook chapter such that the format and nomenclature is consistent across a given guide. This will ensure accurate consolidation of the three original guides, and help communicate consistency throughout the literature. Next, authors for each section will be allocated based on skill, experience and willingness

to deliver a quality product. This ensure that the work is completed in a timely manner with special attention placed on quality assurance. The fifth step will consist of designing new sections for each guide taking into account contemporary development techniques and vulnerabilities found. Special attention will be taken not to neglect legacy issues affecting web applications and software. The purpose of this step is to ensure the OWASP Guidebook is updated accurately. The last stage will involve an OWASP peer review of the finished deliverable. This step aims to confirm quality and product relevance based on the experience and expertise of industry experts from around the world.

Describe the specific milestone activities that would be accomplished in this proposed project.

A peer review of the updated and new sections of the OWASP Guidebook 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, and documented in the product description and quality management strategy. 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.

What form of involvement and leadership position will your organization take in this project?

The OWASP Foundation will lead this project and provide project management and project support resources to ensure completion and quality control of the OWASP Guidebook Project. OWASP will reach out to our community for volunteers and contributors, and we will review the deliverable at both the 50% and the 100% milestone stages. We welcome the involvement from DHS in such areas.

Will your organization be donating funds or making any in-kind contributions to help facilitate this project? If so, in what manner and what amount?

Yes, the OWASP Foundation hopes to donate $10,000 to the OWASP Guidebook Project. Additionally, there is a possibility that OWASP may be able to raise more capital; however, this is dependent on the fundraising resources available to the organization during project initiation.

7 – Projected Outcomes

In 250-750 words, please list the concrete, measurable results and specific expected outcomes:

How would you define success for this project?

The success of the OWASP Guidebook Project will focus on accuracy and quality that will be agreed upon before project initiation. The success criteria will be documented in the project product description and quality management strategy. In addition to the individual product descriptions, OWASP has defined requirement guidelines for a project release that are based on quality review by OWASP members. In order to have a release signed by OWASP:

- The project must be in good standing with the organization
- The release to be approved must be submitted to the official OWASP Project Repository for archival purposes.
- The release must have an aggregate of at least five (5) positive feedback responses by OWASP reviewers.

What measurable outcomes are expected as a result of this project?

The major measurable outcomes that will result from completion of the OWASP Guidebook 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.

How might this project change cyber security within two years? Ten years?

The OWASP Guidebook Project will 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 Guidebook 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.

What next steps might follow the completion of the proposed project?

The proposed next steps following completion of the OWASP Guidebook Project are to have three published books with consistent visual and communication based branding. Most importantly, OWASP plans to implement references among all books that can be applied to the entire security life cycle in any environment.

8 – Project Budget

An important component of your proposal is the preparation of an initial high-level budget that is reasonable. Please ensure that everything mentioned in the proposal is accounted for in the budget. Complete every field using your best judgment when projecting project expenses. Provide any detail in the notes section that you feel is relevant.

If you anticipate support (including in-kind) from an organization other than HOST, please enter those amounts below.

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	10,000		
Other Direct Expenses	15,000*		
Purchased Services		$10,000**	
Indirect Expenses			
Grand Total	25,000		

* airfare + hotel funding for core team to meet as well as purchasing designated project management software

** 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

Submit Your Proposal

Please submit this completed proposal to the attention of: Deborah Bryant, at bryant.deb@gmail.com

After you submit your grant request proposal, we will send you an email within three days acknowledging receipt of your proposal. We carefully review every proposal. Within one weeks of receipt we will be in contact with you to schedule a time to review your proposal in greater detail.