OWASP
The Open Web Application Security Project

Projects Handbook 2013

OWASP Global Projects Committee

Version: 2.0
Produced: Oct 9th, 2012

Table of Contents

1. Acknowledgements
2. Overview
3. Project Requirements
    - 3.1 Openness
    - 3.2 Innovation
    - 3.3 Internationalization
    - 3.4 Integrity
    - 3.5 Ownership
4. Project Lifecycle
    - 4.1 Incubator Projects
    - 4.2 Labs Projects
    - 4.3 Flagship Projects
5. Project Reviews
    - 5.1 Reviewer Pool
    - 5.2 Project Feedback Reviews
6. Project Processes
    - 6.1 New Project Application Process
    - 6.2 Project Donation Process
    - 6.3 Project Transition Process
    - 6.4 Project Abandonment Process
    - 6.5 Project Adoption Process
    - 6.6 Project Removal Process
    - 6.7 Incubator Graduation Process
    - 6.8 Project Review Processes
    - 6.9 Current Project Migration Process
7. Project Stage Benefits
    - 7.1 Starting a Project: Incubator Benefits
    - 7.2 Benefits of Graduating: OWASP Labs Stage
    - 7.3 Benefits of Graduating: OWASP Flagship Stage
8. Appendix
    - 8.1 June 2011 GPC Working Session
    - 8.2 List of OWASP Recommended Licenses
    - 8.3 OWASP Code of Ethics 2012
    - 8.4 OWASP Project Donation Contract
    - 8.5 OWASP Project Handbook 2013 Authors

1. Acknowledgements

This handbook was made possible thanks to the support from the following organizations:

These companies directly supported the June 2011 GPC Working Session (Appendix 8.1) where many of these policies were developed for OWASP Projects.

We would also like to thank the many dedicated individuals who have worked tirelessly to design, write, and complete this handbook. We could not have completed this project without your contributions to this initiative.

2. Overview

Projects are one of the primary methods by which OWASP strives to achieve its mission, which is to make application security more visible. The OWASP Projects Division provides a community based online platform that allows project leaders the opportunity to freely test ideas and theories in an open environment. Leaders are able to leverage the OWASP brand, and the help of a dedicated OWASP project manager to guide development.

The goal of an OWASP Project is to create a concrete deliverable - such as a document, a tool, or a code library - that furthers the OWASP mission. OWASP projects are divided into the following major categories:

- **Documentation projects:** These projects seek to communicate information or raise awareness about a topic in application security. Note that documentation projects can take any media form (e.g. CBT, videos, games, etc.) and are not limited to a print deliverable.
- **Tool projects:** Tool projects aim to create software that enables users to test, detect, protect, or educate themselves using a facet of application security.
- **Library projects:** These projects provide libraries/frameworks that can be leveraged by developers to enhance the security of their applications.

As with all OWASP initiatives, OWASP Projects are driven by volunteers, and they are open to everyone. This means that anyone can lead a project, anyone can contribute to a project, and anyone can use a project. This handbook is meant to be the primary reference for OWASP project leaders, and it should serve as a useful starting point for anyone that wishes to start their own project within the OWASP organization.

3. Project Requirements

Starting an OWASP project is very easy. Projects and their leaders are simply expected to uphold the OWASP core values: openness, innovation, internationalization, and integrity. Beyond these principles, a potential project leader with an idea only needs a project name, a project description, a project license choice, and a project roadmap.

3.1 Openness

OWASP Projects must be open in all facets, including source material, contributors, organizational structure, and finances (if any). Project source code (if applicable) must be made openly available, project communication channels (e.g. mailing lists, forums) should be open and free from censorship, and all project materials must be licensed under a community friendly license as approved by the Free Software Foundation (Appendix 8.2).

3.2 Innovation

All OWASP Projects are expected to be innovative, and address an application security concern. Projects can be ideas turned into a proof-of-concept, new implementations of familiar ideas or tools, or something altogether different. The OWASP philosophy is to try many things and fail fast! This means that we want project leaders to bring projects forward, no matter how large or small, and no matter how unlikely they may seem. Project leaders are encouraged to be forward thinking in their ideas and designs.

3.3 Internationalization

A project is internationalized when all of the project's materials and deliverables are consumable by an international audience. This can involve translation of materials into different languages, and the distribution of project deliverables into different countries. OWASP Projects are not expected to be internationalized from day one, but they are expected to keep the international audience in mind for future development. OWASP resources and assistance are available to help in translation efforts, but project leaders will need to ensure that their project is flexible enough to support internationalization.

3.4 Integrity

OWASP Projects must uphold the integrity of The OWASP Foundation, and must not unduly promote a specific company, vendor, or organization. While OWASP welcomes corporate sponsorship of a project, project leaders must ensure that any such relationship is disclosed, and that the project continues to be a vendor agnostic endeavour. Project leaders must use the

appropriate project designation to refer to their project (Section 4) and must not abuse the OWASP name. Project leaders must also conduct themselves according to the OWASP Code of Ethics at all times (Appendix 8.3).

3.5 Ownership

OWASP does not require a transfer of ownership of your project. Each project leader and contributor owns their own contributions, just like any other major open source project. Project leaders who own all copyrights to their project, and no longer wish to be involved with the day to day management of their project, are welcome to donate their copyright ownership to OWASP. Simply contact the OWASP Project Manager for more information on the processes involved.

4. Project Lifecycle

Projects, along with Global Conferences and Local Chapters, are the cornerstone of the OWASP organization. We want to provide a fostering environment for new ideas and energetic project leaders; however, our global consumers depend on OWASP to provide dependable, quality projects. The OWASP Project Lifecycle represents a balance between keeping a very loose structure around OWASP projects, and ensuring that OWASP consumers are not confused about a project's maturity and quality.

Our lifecycle stages allow consumers to easily identify mature projects, and projects that are proofs of concept, experimental, and classified as prototypes in their current state. The greater the maturity of the project, the greater the level of responsibility for the project leader. These responsibilities are not trivial as OWASP provides incentives and benefits (Section 7) for projects who take on these added responsibilities.

The OWASP Project Lifecycle is broken down into the following stages:

OWASP Incubator Projects

OWASP Labs Projects

OWASP Flagship Projects

Each of these stages is described in greater detail in the sections that follow. At a minimum, all OWASP projects have a project name, a project leader, a project description, a project license choice, and a project roadmap.

Project Name

A project name *may* include the OWASP name. If a project chooses to use the OWASP name, any project artifacts must clearly state the project's current lifecycle designation. For example, this notice can be on the cover page (documentation), in an 'About' dialog (tools), in comment header blocks (code), or some other prominent location.

Project Leader

A project leader is the individual who decides to lead the project throughout its lifecycle. The project leader is responsible for communicating the project's progress to the OWASP Foundation, and he/she is ultimately responsible for the project's deliverables. The project leader

must provide OWASP with his/her real name and contact e-mail address for his/her project application to be accepted, as OWASP prides itself on the openness of its products, operations, and members.

Project Descriptions

A project description should outline the purpose of the project, and the value it provides to application security. Ideally, project descriptions should be written in such a way that the start of the description can be used as a teaser or an excerpt (as commonly done for news articles and blog postings). This teaser will be seen and used in various places within the Projects Portal. Poorly written project descriptions therefore detract from a project's visibility, and project leaders should ensure that the teaser is concise and meaningful.

Project Roadmap

A project roadmap is the envisioned plan for the project. The purpose of the roadmap is to help others understand where the project is going. It gives the community a chance to understand the context and the vision for the goal of the project. Additionally, if a project becomes inactive, or if the project is abandoned, a roadmap can help ensure a project can be adopted and continued under new leadership.

Roadmaps vary in detail from a broad outline to a fully detailed project charter. Generally speaking, projects with detailed roadmaps have tended to develop into successful projects. Some details that leaders may consider placing in the roadmap include: envisioned milestones, planned feature enhancements, essential conditions, project assumptions, development timelines, etc.

Project License

A project must be licensed under a community friendly or open source license. For more information on OWASP recommended licenses, please see (Appendix 8.2). While OWASP does not promote any particular license over another, the vast majority of projects have chosen a Creative Commons license variant for documentation projects, or a GNU General Public License variant for tools and code projects.

4.1 Incubator Projects

OWASP Incubator projects represent the experimental playground where projects are still being designed, ideas are still being proven, and development is still underway. The “OWASP Incubator” label allows OWASP consumers to readily identify a project’s maturity. The label allows project leaders to leverage the OWASP name while their project is still maturing.

OWASP Incubator projects are given a place on the OWASP Projects Portal to leverage the organization's infrastructure, and establish their presence and project history. Many of the benefits and privileges afforded to projects are dependent upon metrics and statistics that are tracked by the OWASP Projects Infrastructure.

Incubator Project Deliverables

Leaders of Incubator Projects are expected to produce a draft or development release as a downloadable file on the project page within twelve (12) months of project inception. As previously mentioned, OWASP believes in pursuing ideas in a fail-fast manner. In order to avoid an excess of stagnant projects that never mature, projects will not be permitted to linger in an undeveloped state beyond this time period. If a project has not produced at least a draft or development release, the project will be removed from the OWASP Projects Portal. If a project leader subsequently produces a completed release and wishes to re-associate with OWASP Projects, then that project can be returned to the OWASP Projects Portal.

Once a project leader has completed at least one version of a concrete deliverable, the project is eligible for graduation into the OWASP Labs (Section 6.7). Note that graduation to the OWASP Labs is *optional* and a project leader that has completed at least one concrete deliverable may continue in the OWASP Incubator stage.

4.2 Labs Projects

OWASP Labs projects represent projects that have produced a deliverable of significant value. Leaders of OWASP Labs projects are expected to stand behind the quality of their projects as these projects have matured to the point where they are accepted by a significant portion of the OWASP community. While these projects are typically *not* production ready, the OWASP community expects that an OWASP Labs project leader is producing deliverables that are ready for mainstream usage.

OWASP Labs projects are meant to be the collection of established projects that have gained community support and acclaim by undergoing the project review process. These reviews are part of the **Incubator Graduation Process (Section 6.7)** that is required to enter OWASP Labs. To enter OWASP Labs, projects must be actively maintained, they must meet the OWASP Labs project standards, and they must seek to provide value to OWASP consumers.

In recognition of these qualities, such projects are afforded a number of benefits to help grow the project including but not limited to: graphic design support, technical writing reviews, and UI design reviews. In addition, OWASP Labs projects have a primary spotlight in the OWASP Projects Portal, and they receive increased promotional opportunities within the OWASP organization.

While projects that graduate to the OWASP Labs can remain there indefinitely, project activity is a prominently featured piece of metadata on the Projects Portal. As a result, Projects without periodic activity will be automatically tagged as inactive. As a result, project leaders are encouraged to maintain the level of excellence attributed to Labs projects.

4.3 Flagship Projects

The goal of OWASP Flagship projects is to identify, highlight, and support mainstream OWASP projects that make up a complete application security platform composed of OWASP Projects. Selection of Flagship projects is driven by the GPC, and eligible projects are selected from the OWASP Labs by the Global Projects Committee, in consultation with a working group of independent industry experts. This selection process generally ensures that there is only one project of each type covering any particular security space. These projects are selected for their superior maturity, established quality, and strategic value to OWASP and application security as a whole.

OWASP Flagship projects represent projects that are not only mature, but are also projects that OWASP as an organization provides direct support to maintaining. The core mission of OWASP is to make application security visible and so as an organization, OWASP has a vested interest in the success of its Flagship projects. Since Flagship projects have such high visibility, these projects are expected to uphold the most stringent requirements of all OWASP Projects.

Selection for OWASP Flagship designation is by invitation only. A Labs project leader can present their case for why they think their project deserves Flagship status. However, there is no deterministic process to be designated a Flagship project. There are no steps to be followed that guarantee Flagship status. This status is reserved for the strategic use of OWASP to identify a platform that supports the OWASP mission to improve the state of application security.

5. Project Reviews

OWASP recognizes the need for project consumers to quickly ascertain the maturity of a project. Project reviews are not mandatory, but they are necessary if a project leader wishes to graduate to the next level of maturity within the OWASP Global Projects infrastructure. Projects can be reviewed when an Incubator project wishes to graduate into the OWASP Labs designation, and project releases can be reviewed if they want the quality of their deliverable to be vouched for by OWASP. The goal of a review is to establish a minimal baseline of project characteristics and release quality.

Project Health Reviews

Project health reviews are not mandatory, but they are necessary if a project wants to graduate to the next level of maturity. The project leader can submit an application for a project health review using the Incubator Graduation Form found on the OWASP Global Projects Portal. After the application is received, the project will be assigned two (2) reviewers that will help assess the project.

The review centers around the following core questions:

1. Is the project actively maintained?
2. Does it meet quality expectations?
3. Does it follow OWASP Project best practices?
4. Does it support the OWASP mission and objectives?
5. Does the project have one accepted OWASP reviewed deliverable on record within the new project's infrastructure?

These questions were designed to distil the core characteristics of a healthy OWASP project, as any concern about a project's quality can be aligned to one of the above questions.

Deliverable/Release Quality Reviews

Deliverable/Release quality reviews are not mandatory either, but they are necessary if a project wants to graduate to the next level of maturity. The project leader can submit an application for a project review of this type using the Deliverable/Release Reviews form found on the OWASP Global Project Portal. After the application is received, the project will be assigned two (2) reviewers that will help assess the deliverable or release.

As there are 3 project categories that exist within the OWASP project landscape, each category has its own set of criteria that a release must meet if they are to have a successful review that OWASP will vouch for.

Document Project Assessment Criteria

1. Does the project have a publicly accessible bug tracking system established, and source

code repository?
2. Is the document in a format which can be converted to an OWASP book?
3. Does the project release/deliverable have a table of contents that links all the wiki content together?
4. Is the project release/deliverable available for download on the OWASP Project wiki page?
5. Has all release/deliverable content been reviewed by a technical editor to ensure that English grammar is correct, understandable, and the content flows well?

Tool Project Assessment Criteria

1. Does the project have a publicly accessible bug tracking system established, and source code repository?
2. Does the project include online documentation built into the tool?
3. Does the project include build scripts that facilitate building the application from source?
4. Does this project have an easy to use installer (Goal: Fully automated installer) (or stand alone executable version)?
5. Is the tool/deliverable user friendly and easy to use?

Library Project Assessment Criteria

1. Does the project have a publicly accessible bug tracking system established, and source code repository?
2. Does the project include online documentation built into the library?
3. Does the project include build scripts that facilitate building/adding to the application from source?
4. Does this project have an easy to use installer (Goal: Fully automated installer) (or stand alone executable version)?
5. Is the library/deliverable user friendly and easy to use?

To facilitate the review, the OWASP Global Projects team will help the project leader allocate reviewers. The results of these reviews are published openly, and are available to project consumers.

5.1 Reviewer Pool

The Reviewer Pool is a mechanism to ensure there are qualified reviewers making quality reviews of OWASP projects.The pool is set of veteran reviewers who have proven themselves dedicated to executing quality reviews of projects. Any reviewer that has completed ten (5) project reviews in the last twelve (12) months is eligible to join the Reviewer Pool. Members of the GPC and the Board are also automatic members of the Reviewer Pool, as are any paid

professional project reviewers retained by the OWASP Foundation.

Members of the Reviewer Pool will be asked to fill their user profile, which will be visible to OWASP consumers as a testament to why their reviews have merit and relevance. Members of the Reviewer Pool serve a critical role in ensuring the quality of projects, and will gain added recognition in OWASP.

5.2 Project Feedback Reviews

Project Reviews provide a way to look comprehensively at the overall maturity of a project. Additionally, there is significant value in allowing projects to solicit *general* feedback to improve the quality of their projects. There are two ways the OWASP Global Projects Portal goes about giving feedback: Project Review and User Feedback.

Project Review
Project leaders can submit an application for a project review to assess the quality of their project, and to get general professional feedback from the OWASP Community. Reviews of this type can only be done every six (6) months.

User Reviews
The Projects Portal allows users to leave generic feedback for both individual releases, and the overall project. These feedback responses are provided to project leaders, and are also used as part of the overall evaluation of project maturity.

6. Project Processes

While the OWASP Project Lifecycle may seem unwieldy, the goal of the lifecycle is to *simplify* OWASP project management. The following sections below outline our streamlined processes that exist to help projects move smoothly through the OWASP Project Infrastructure.

6.1 New Project Application Process

The New Project Application Process is how a brand new idea becomes an OWASP Project. Such projects are labelled as OWASP Incubator projects. The process involves submitting the proposed project name, project leader information, project description, project roadmap, and selecting an appropriate open-source license for the project using the New Project Application Form on the Projects Portal.

Once a request has been submitted, the proposal will be made open to the community for review and feedback for a period of seven (7) days. Unless there are any critical objections or concerns that the project violates OWASP principles, the project will be automatically created in the OWASP Projects Infrastructure. The infrastructure will create the following items for the project:

- An initial project home page
- A profile on the Projects Portal populated with the supplied information
- A mailing list (or forum topic once available)
- A code repository (List of suggestions on which to use)
- An issue tracker (List of suggestions on which to use)
- Any relevant user accounts for the project leader (@owasp.org email address, wiki account, project SVN account, etc)

An announcement will be made regarding the new Incubator project and the project leader will have twelve (12) months to produce a functional deliverable.

6.2 Project Donation Process

The Project Donation Process is used for a project that has an existing functional release, but is not currently associated with OWASP. This process is the primary mechanism by which individuals or organizations can transfer the ownership of their project's copyright to OWASP. Please note that an individual or organization does not have to transfer copyright ownership in order to share their existing project with OWASP. This process is in place for those entities wishing to tranfer copyright to the OWASP Foundation. In order to accomodate for these two cirumcstances, OWASP project donation types fall into two categories: partnerships and endowments.

Partnerships occur when the project owner has decided to adopt OWASP principles and processes for their project. Such owners wish to continue their leadership and involvement with the project, but want their project to be included in the OWASP Project landscape. OWASP welcomes all such project owners as partnerships are the most common type of project donation.

Endowments occur when the project owner has created a project and wishes to completely turn over the project to OWASP. Such owners feel their project has some value, but do not wish to stay involved in the process. As a result, they would like someone at OWASP to “adopt” the project. In order to properly adopt such projects, owners may need to assign OWASP certain rights in order for the organization to properly accept the project. Though these situations are rare, OWASP welcomes all project endowments and will work with any such project owner to ensure a smooth and proper transition.

The donation process requires submitting the project name, project description, project roadmap, an appropriate open-source license choice, and the type of donation. In addition, the latest functional release should be uploaded along with the request. These items can be submitted through the Project Donation Form on the Projects Portal.

Once a request has been submitted, the proposal will be made open for review and feedback for a period of seven (7) days. Unless there are any critical objections or concerns that the project violates OWASP principles, the project will be created in the OWASP Projects Infrastructure and the project owner will be provided the same project setup and resources as in the New Project Application process. Note that endowments may be held for additional review in order to ensure that OWASP can properly make use of the project.

The project owner will be expected to migrate their project to the OWASP Projects Infrastructure and utilize these resources. OWASP understands that long standing projects may have established communities that make migration difficult or inappropriate. Exceptions to this policy will be made on a case-by-case basis. In such cases, project owners will need to work with the OWASP Global Projects team to ensure the appropriate project artifacts and details are regularly synchronized to the Projects Portal. At minimum, a project home page and profile entry will still exist for the project even if the project is not hosted on the OWASP Projects Infrastructure.

Once the project has been migrated and the donation is complete, an announcement will be made regarding the project donation.

6.3 Project Transition Process

The Project Transition Process is used to transition leadership of a project to a new project leader. This is a simple automated process to transfer the relevant accounts, mailing lists, and other project resources to the new project leader. The current project leader should log into the

Projects Portal and submit a Project Transition Request identifying the new project leader. The proposed leader will receive a request to confirm their new role. Upon receiving the new leader's confirmation, the Projects Infrastructure will transfer the project to the new leader. An announcement will be made regarding the leadership transition.

6.4 Project Abandonment Process

The Project Abandonment Process was put in place for those occasions where a project leader is no longer able to manage their project, and has not been able to find a suitable replacement for the leader role. Project abandonment can also occur when the project leader feels his/her project has become obsolete. Under these cirucumstances, the acting project leader is encourage to submit the Project Abandonment Form found in the Projects Portal. Once a request has been received, the project in question will be archived and labeled as an Archived project. Please note that anyone within the OWASP community can adopt an Archived project so please make sure that you are willing to have others take over your endevour if you wish to go through the project abandonment process.

6.5 Project Adoption Process

The Project Adoption Process is for *inactive and orphaned* projects. Any OWASP community member may volunteer to adopt an inactive or orphaned project by submitting a Project Adoption Request through the Projects Portal. Upon receiving an adoption request, the global projects team will contact the current leader of the inactive project in question. An inactive project leader can relinquish leadership of the project to the new proposed leader through the Project Transition Process. If no reply is received and no constructive activity is detected within thirty (30) days of contacting the inactive leader, the OWASP project manager will transition the project to the proposed adopting leader. An announcement will be made regarding the project adoption.

6.6 Project Removal Process

The Project Removal Process occurs periodically through automated and manual review. The purpose of this process is to migrate projects that have been identified for removal off of the OWASP projects infrastructure. Possible reasons for removal include (but are not limited to) inappropriate evolution of a project that results in contradicting OWASP core values, abuse of OWASP project services or infrastructure, expiration of Incubator projects that have not developed into a functional product after a year of inception.

Any project can be "flagged" by anyone that questions the appropriateness of a specific project. OWASP will periodically examine projects that are excessively flagged.

OWASP global projects team will flag Incubator projects without a submitted release that have exceeded their time in the Incubator. Such project leaders will be warned in advance of this

deadline. Upon the deadline, if no updates have been submitted, the OWASP Project Manager will archive the project. Additionally, the global projects team will periodically review a random sample of Incubator projects to ensure that submitted releases are indeed “functional”.

A project that has been previously removed from OWASP cannot be submitted again through the New Project Application Process by the same project leader. If a project leader wishes to associate a removed project with OWASP, the leader may submit a completed release to the OWASP global projects team for evaluation.

6.7 Incubator Graduation Process

The Incubator Graduation Process is an *optional* process undertaken at the *request* of a project leader using the Incubator Graduation Form. The purpose of this process is to move a project from the OWASP Incubator into the OWASP Labs. In order to be considered for OWASP Labs, an Incubator project must have an OWASP reviewed deliverable/release, and obtained an aggregate of at least two (2) positive responses for each of the core project review questions.

The review centers around the following core questions:

- Is the project actively maintained?
- Does it meet quality expectations?
- Does it follow OWASP Project best practices?
- Does it further the OWASP mission?
- Does the project provide value?

Reviews must be performed by a member of the Project Reviewer Pool, and their review must answer affirmatively to each of the core Project Review questions. If a project leader has requested to graduate from the OWASP Incubator stage, and the project fulfills all other graduation requirements *except* for the Reviewer Pool review, OWASP will ensure that the project receives a timely review. In such cases, the OWASP global projects team will make a call for reviewers from our review pool. If no reviewer can be found within fifteen (15) days, the global projects team will, at its discretion, *pay* for a professional, third-party reviewer to complete the review.

Upon confirmation that a project fulfills the requirements of the graduation process, a project will graduate from the OWASP Incubator stage to the OWASP Labs stage. An announcement will be made regarding the project graduation through our marketing channels.

As entrance into the OWASP Labs provides greater benefits and visibility, the global projects team expects that project leaders will aspire to graduate from the Incubator as quickly as possible. If a project leader makes a graduation request that is not successful, the project leader will *not* be permitted to make another graduation request for the project for a period of three (3) months. Due to this restriction, we encourage all project leaders to be certain that their project is

in good order prior to making the graduation request. This rule is in place to prevent undue strain on the Reviewer Pool and our OWASP resources.

6.8 Project Review Processes

OWASP offers two types of reviews for projects: Deliverable/Release Review and Project Health Review. Project reviews are not mandatory, but they are necessary if a project leader wishes to graduate to the next level of maturity within the OWASP Global Projects infrastructure. Projects can be reviewed when an Incubator project wishes to graduate into the OWASP Labs designation, and project releases can be reviewed if they want the quality of their deliverable to be vouched for by OWASP. The goal of a review is to establish a minimal baseline of project characteristics and release quality.

6.9 Current Project Migration Process

The Existing Project Migration Process is a one-time process. It was developed to help transition OWASP projects from the projects infrastructure that uses Assessment Criteria v2 to the new OWASP projects infrastructure that uses the Incubator, Labs, and Flagship designations. As part of the June 2011 GPC Working Session, the GPC performed a complete inventory of all known OWASP Projects. During this inventory, each project was evaluated and assigned a provisional state in the OWASP Projects Lifecycle. These provisional assignments were made effective upon the launch of the new OWASP Projects Infrastructure (September 2011).

Certain projects were identified during the inventory as having never created a functional release despite being over a year old. Such “graveyard” projects were removed from the system and were treated as if they had undergone the Project Removal Process.

Projects provisionally placed in the OWASP Labs and projects that are provisionally designated as Flagship projects had six (6) months to confirm their status by fulfilling the appropriate requirements. Projects that are provisionally placed in the OWASP Incubator can graduate to the OWASP Labs at any time by undertaking the Incubator Graduation Process (Section 6.7).

7. Project Stage Benefits

The requirements laid out for the various stages of project maturity can be arduous. Since, all project leaders are volunteers, OWASP recognizes the need for incentives for both the project leader and the project itself. The following section provides a list of standard resources made available to project leaders based on their project's current maturity level.

7.1 Starting a Project: Incubator Benefits

Aside from leveraging the OWASP brand, we can offer a number of benefits to an OWASP project leader for starting a project. These include: Financial Donation Management, Technical Writing Support, Graphic Design Support, Professional Project Review Support, WASPY Awards Nominations, OWASP Projects Track Participation, Opportunity to get $500 for Project Development, and Community Engagement and Support.

Financial Donation Management

As part of the project home page provided by the OWASP Projects Infrastructure, all projects can solicit financial donations. While these financial resources are available to project leaders, there are strict rules for what these funds can be used for. In particular, these funds *cannot* be used to pay project leaders or contributors for their time spent working on the project. These funds are meant to be used towards project expenses.

Project Review Support

OWASP recognizes that project leaders often have difficulty objectively reviewing their own projects. The goal of a project review is to enable project leaders to receive constructive, objective feedback on how to improve their projects. OWASP Global Projects can retain the services of volunteer professional project reviewers from the OWASP community. As our reviewer pool is made up of unpaid volunteer staff, we are only able to review a project every 3 months. Please note, this service is still under development for the coming year.

WASPY Awards Nomination

Project leaders have the opportunity to participate in the annual WASPY Awards. WASPY Awards are given to those projects that have provided outstanding contributions to the OWASP Community and the Information Security Industry over the year. Any OWASP project can be nominated to receive an award and have their name put into the nominee pool.

OWASP Open Source Showcase & OWASP Projects Track Participation

This opportunity is open to all Open Source Projects. All Incubator project leaders and contributors are welcome to apply for the OWASP Open Source Showcase and the OWASP Projects Track event modules. These event modules are managed by the OWASP Global Projects Group, and they take place at each global AppSec conference every year starting in 2013.

Intra-OWASP Promotion

Additional promotional opportunities are available through a number of other initiatives, activities, and even other projects within OWASP.

For example, the OWASP Web Testing Environment (formerly the OWASP LiveCD), Podcast, AppSec Tutorial Series, and CBT projects all interact with other OWASP projects. These types of projects can provide cross-promotion opportunities for other projects.

Likewise, there are multiple teams working on internationalization that support ongoing translation efforts. These teams can provide translation services that will help projects reach wider audiences.

OWASP also holds and participates in many industry and community events, including local chapter meetings, regional events, and outreach activities. Projects can gain increased exposure through OWASP presence at these events.

Note that while OWASP encourages project leaders, translation team members, chapter leaders, conference planners, and outreach leaders to consider promoting mature projects, the final decision rests with those community members.

Opportunity to submit proposal: Award of $500 for Project Development

All OWASP projects will have an opportunity to submit a proposal for $500 stipend that will be used for development of the project. There are restrictions to the use of these funds. Stipends cannot be used to pay project leaders or contributors for work done. Acceptable expenses include travel, marketing, advertising, technology, and development expenses. There is a set amount set aside from the Foundation for this award every year, and there is a proposal submission deadline for the year. Please note, this offering is still under development for the coming year.

Community Engagement and Support

Last but not least, project leaders get first hand access to industry experts, and a wealth of knowledge and support from over 32,000 global OWASP members and supporters.

7.2 Benefits of Graduating: OWASP Labs Stage

A Labs project will continue to receive the same benefits that OWASP Incubator projects receive (please see above), along with the additional benefits outlined below:

Project Promotion Support

OWASP recognizes that project leaders want to obtain visibility for their endeavors, and there are a number of ways that can be achieved through our Global Projects infrastructure. Projects can expect to be highlighted or “featured” for several reasons, including but not limited to:

1. New project inception
2. Recent project graduation
3. Recent release
4. High levels of contributor activity
5. Strong positive feedback responses
6. Press Coverage

If selected, projects will be highlighted through the Global Projects Portal and our social networking infrastructure as these are the primary methods we use to promote the visibility of OWASP projects.

Technical Writing Support

If needed, OWASP can provide a project leader with assistance in locating and hiring a professional technical writer to *review* project documentation. The project leader must ensure that the cost of the Technical Writer come out of the individual project budget.

Graphic Design Support

As with technical writing, OWASP can provide a project leader with assistance in locating and

hiring a professional graphic designer. The goal of graphic design is to enable project leaders to create polished, professional looking projects. The project leader must ensure that all graphic design costs come out of their individual project budget.

OWASP Open Source Showcase & OWASP Projects Track Travel Funding Assistance

This opportunity is open to all Open Source Projects. All Labs project leaders and contributors are encouraged to apply for the OWASP Open Source Showcase and the OWASP Projects Track event modules. These event modules are managed by the OWASP Global Projects Group, and they take place at each global AppSec conference every year starting in 2013. OWASP travel funding is also made available to those project leaders that are in need of assistance. Preference is given to project leaders that are traveling from the region closest the the AppSec event in question, and preference is also given to project leaders that have not participated in the OSS and Projects Track modules.

Opportunity to submit proposal: Award of $500 for Project Development

All OWASP projects have an opportunity to submit a proposal for $500 stipend that will be used for development of their project. There are restrictions to the use of these funds. Stipends cannot be used to pay project leaders or contributors for work done. Acceptable expenses include travel, marketing, advertising, technology, and development expenses. There is a set amount set aside from the Foundation for this award every year, and there is a proposal submission deadline for the year. Labs projects will be given extra consideration over Incubator projects due to increased level of commitment. Please note, this offering is still under development for the coming year.

7.3 Benefits of Graduating: OWASP Flagship Stage

A Flagship project will continue to receive the same benefits that OWASP Labs projects receive (please see above), along with the additional benefits outlined below:

Grant Finding and Proposal Writing

OWASP will assist Flagship projects with finding and developing a grant proposal to help fund their product development. Projects must have an active project leader willing to take responsibility for helping complete the proposal. Additionally, the project leader must be willing to take the lead on delivering the project outlined in the proposal if we are successful in securing

grant funding.

Yearly Marketing Plan Development

OWASP will help projects with the Flagship designation by helping the active project leader plan, develop, and execute a yearly marketing plan.

Opportunity to submit proposal: Award of $500 for Project Development

All OWASP projects have an opportunity to submit a proposal for $500 stipend that will be used for development of their project. There are restrictions to the use of these funds. Stipends cannot be used to pay project leaders or contributors for work done. Acceptable expenses include travel, marketing, advertising, technology, and development expenses. There is a set amount set aside from the Foundation for this award every year, and there is a proposal submission deadline for the year. Flagship projects will be given extra consideration over Incubator and Labs projects due to their increased level of commitment. Please note, this offering is still under development for the coming year.

8. Appendix

In this section, you will find examples, forms, and extra information relevant to the OWASP Projects infrastructure.

8.1 June 2011 GPC Working Session

Since the inception of the Global Projects Committee (GPC) at the 2008 OWASP Summit, our goal has been to foster an environment where OWASP Projects can grow and mature. As application security awareness rises, the knowledge and capabilities provided by OWASP Projects becomes increasingly important. To that end, we must balance the history of OWASP Projects as a loosely managed collection of random application security projects with the necessity to provide clarity and assurance to a world that has come to depend on many of these OWASP Projects.

Over the last three years, the GPC made great strides towards this goal, but virtual meetings have their limitations, and progress slowed significantly. Following the initial 2008 Summit, the GPC met in person only once during the 2009 Mini-Summit. During this session, we met with renewed rigor and were able to take advantage of the Summit to outline an overall OWASP Project Lifecycle, along with an ambitious but achievable agenda for the remainder of the year. The argument could be made that the productivity of a week at the Summit matched or exceeded the productivity of the GPC during the entirety of the previous year. Recognizing the value of in person meetings, the GPC requested support for two in person meetings during the 2011 year as part of our overall 2011 budget, which was approved at the May 2011 Board meeting.

The GPC held the first of these working sessions in the three days leading up to OWASP AppSec EU in Dublin, Ireland. The GPC Working Session took place from June 6th – 8th at the Trinity Capitol Hotel, *separate* and *away* from the official conference venue. This separation was deliberate to minimize distractions and maximize productivity of the GPC. During this session, the GPC met for over 30 hours and accomplished a variety of goals including:

1. Designated the phases of the *OWASP Projects Lifecycle*
2. Outlined vision for *OWASP Enterprise Edition* support
3. Established processes for moving from phase to phase
4. Completed inventory of OWASP Projects and assigned initial phase
5. Targeted projects to pilot *OWASP Flagship* designation
6. Drafted mapping of Flagship projects to OpenSAMM categories
7. Created of Project Health Evaluation criteria
8. Selected of Projects Hosting Infrastructure provider

Many of these accomplishments were uncompleted goals from the *original* GPC charter. The working session also resulted in several deliverable artifacts which are enclosed with these proceedings. We hope that these proceedings demonstrate the value of in person committee working sessions and provide the framework and precedent for other committees to pursue their own working sessions. For the full report, please see the GPC Full Working Session Proceedings Document.

8.2 List of OWASP Recommended Licenses

Here you will find a list of OWASP Recommended Licenses that you can choose from for your project. Choosing one of the licenses below is not mandatory. We only ask that you choose a community friendly license.

<table>
<tr><th></th><th colspan="3">Allow commercial uses of your work?</th></tr>
<tr><th></th><th colspan="2">Yes</th><th rowspan="3">No</th></tr>
<tr><th></th><th colspan="2">Allow modifications of your work?</th></tr>
<tr><th></th><th>Yes, no restriction except attribution</th><th>Yes, as long as modification are also opensource</th><th>No</th></tr>
<tr><td>Tool Project (Non-WebBased)</td><td>GPL 3.0 (requires that modifications to your code stay open source, thus prohibiting proprietary forks of your project)</td><td rowspan="3">Apache 2.0 (fewest restrictions, even allowing proprietary modifications and proprietary forks of your project, and more up-to-date than BSD license)</td><td rowspan="4" colspan="2">Sorry, such licenses are not opensource and are not elegible to become an OWASP Sponsored Project. If this is really what you want, consider using CC-BY-ND or CC-BY-NC-ND. See http://creativecommons.org/choose for more information and note that they label these two license as "not a Free Culture License".</td></tr>
<tr><td>Tool Project (WebBased)</td><td>AGPL 3.0 (prevents GPL's SaaS loophole)</td></tr>
<tr><td>Library Project</td><td>LGPL 3.0 (similar to GPL but modified for use with libraries that may be called by other proprietary programs)</td></tr>
<tr><td>Document Project (includes E-Learning, presos, books, etc)</td><td>CC-BY-SA 3.0 (like GPL but for documents. Alternately you can use FDL, but projects like Debian and Ubuntu don't accept it)</td><td>CC-BY 3.0 (like Apache but for documents)</td></tr>
</table>

8.3 OWASP Code of Ethics 2012

Each of us is expected to behave according to the principles contained in the following Code of Ethics. Breaches of the Code of Ethics may result in the foundation taking disciplinary action. (Membership Revocation)

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Promote the implementation of and promote compliance with standards, procedures, controls for application security;
- Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;
- Discharge professional responsibilities with diligence and honesty;
- To communicate openly and honestly;
- Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Foundation;
- To maintain and affirm our objectivity and independence;
- To reject inappropriate pressure from industry or others;
- Not intentionally injure or impugn the professional reputation of practice of colleagues, clients, or employers;
- Treat everyone with respect and dignity; and
- To avoid relationships that impair — or may appear to impair — OWASP's objectivity and independence.

8.4 OWASP Project Donation Contract

The OWASP Foundation

Project Donation License Agreement

Thank you for your interest in The OWASP Foundation (the "Foundation"). In order to clarify the intellectual property license granted with contributions of software from any person or entity (the "Contributor"), the Foundation would like to have a Project Donation License Agreement on file that has been signed by the Contributor, indicating agreement to the license terms below. This license is for your protection as a Contributor of software to the Foundation and does not change your right to use your own contributions for any other purpose.

If you have not already done so, please complete this Agreement.

Please read this document carefully before signing and keep a copy for your records.

Full name: _____

E-Mail: _____

Telephone: _____

Country: _____

You and the Foundation hereby accept and agree to the following terms and conditions:

1. The donation of your project means that you agree to hand over all past, present and future contributions of source code and documentation to the Foundation, however submitted to the Foundation, excluding any submissions that are conspicuously marked or otherwise designated in writing by You.

2. You hereby grant to the Foundation a non-exclusive, irrevocable, worldwide, no-charge, transferable copyright license to use, execute, prepare derivative works of, and distribute (internally and externally, in object code and, if included in your Contributions, source code form) your Contributions. Except for the rights granted to the Foundation in this paragraph, You reserve all right, title and interest in and to your Contributions. OWASP will always release a free and open version of anything we distribute that includes your Contributions.

3. You may continue to be involved in the donated project, but you may no withdraw your project from the OWASP Foundation once the project donation process has been completed. The project donation process is complete once the Foundation receives as signed version of this form from you.

4. You represent that you are legally entitled to grant the above license. If your employer(s) have rights to intellectual property that you create, you represent that you have received permission to make the Contributions on behalf of that employer, or that your employer has waived such rights for your Contributions to the Foundation.

5. You represent that, except as disclosed in your Project Donation submission(s), each of your Contributions is your original creation. You represent that your Contribution submission(s) include complete details of any license or other restriction (including, but not limited to, related patents and trademarks) associated with any part of your Contribution(s) (including a copy of any applicable license agreement). You agree to notify the Foundation of any facts or circumstances of which you become aware that would make Your representations in this Agreement inaccurate in any respect.

6. You are not expected to provide support for your Contributions, except to the extent you desire to provide support. You may provide support for free, for a fee, or not at all. Your Contributions are provided as-is, with all faults defects and errors, and without warranty of any kind (either express or implied) including, without limitation, any implied warranty of merchantability and fitness for a particular purpose and any warranty of non-infringement.

Please sign: _____ Date: _____

8.5 OWASP Project Handbook 2013 Authors

Jason Li

Jason has led security architecture reviews, application security code reviews, penetration tests and provided web application security training services for a variety of commercial, financial, and government customers. He is also actively involved in the Open Web Application Security Project (OWASP), serving on the OWASP Global Projects Committee and as a co-author of the OWASP AntiSamy Project (Java version). Jason earned his Post-Master's degree in Computer Science with a concentration in Information Assurance from Johns Hopkins University. He earned his Master's degree in Computer Science from Cornell University, where he also earned his Bachelor's degree, double majoring in Computer Science and Operations Research.

Justin Searle

Justin is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and currently plays key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), National Electric Sector Cybersecurity Organization Resources (NESCOR), and Smart Grid Interoperability Panel (SGIP). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences, and is currently an instructor for the SANS Institute. In addition to electric power industry conferences, Justin frequently presents at top security conferences such as Black Hat, DEFCON, OWASP, and AusCERT. Justin co-leads prominent open source projects including the Samurai Web Testing Framework, Middler, Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

Keith Turpin

Over the years Keith has held a number of positions at The Boeing Company including: Application Security Assessments team leader, Team Leader for IT Security International Operations, Team Leader for Information and Supply Chain Security Assessments, engineering systems integrator, software developer and senior manufacturing engineer on the 747 airplane program.

He represented Boeing on the International Committee for Information Technology Standard's cyber security technical committee and served as a U.S. delegate to the ISO/IEC sub-committee on cyber security. He is a member of the (ISC)2 Application Security Advisory Board, and the Director of the HPPV Northwest regional engineering competition.You can see his OWASP project on secure coding practices here:
http://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
The presentation on his OWASP project at AppSec USA 2010 can be found here:
http://vimeo.com/17018329
You can see the video of his AppSec USA 2009 presentation on Building Security Assessment Teams here:
http://vimeo.com/8989378

Nishi Kumar

IT Architect Specialist, FIS
Nishi Kumar is an Architect with 20 years of broad industry experience. She is part of OWASP Global Industry Committee and project lead for OWASP CBT (Computer based training) project. She is a committed contributor of OWASP. She has spearheaded Secure Code Initiative program in FIS Electronics Payment division. As part of that program, she has delivered OWASP based training to management and development teams to various groups in FIS. She has been involved with PA-DSS certification of several applications in FIS. Since joining FIS in 2004 she has worked as an architect and team lead for several financial payment and fraud applications. She has hands-on accomplishments in design, development and deployment of complex software systems on a variety of platforms. Prior to joining FIS Nishi Kumar has worked for Pavilion, HNC, Fair Isaac, Trajecta, Nationwide Insurance and Data Junction as Senior Software Engineer, Architect and in Project Management roles. Nishi can be reached at: nishi787(at)hotmail.com

Brad Causey

Brad Causey is a Web Application Security, Forensics, and Phishing specialist working in the financial sector. He frequently contributes to various open source projects, and participates in training and lectures at various educational facilities.

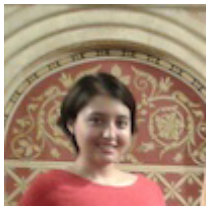
Brad Causey is also an OWASP GPC member, the President of the OWASP AL Chapter, and the President of the AL IISFA Chapter.

Chris Schmidt

Chris is currently the Project Leader for the OWASP ESAPI Projects and also serves on the OWASP Global Projects Committee. He has been involved with OWASP for 4 years and has spoken at many OWASP events about the benefits of the Enterprise Security API as well as participated in Leadership discussions amongst the organization.

During the day, Chris is an Application Security Engineer and Senior Software Engineer for Aspect Security where he has been since fall 2010. Prior to joining the team at Aspect Security he spent 5 years as 'Black Ops Beef' for ServiceMagic Inc with the official title of Software Engineer. Before getting involved in software professionally, Chris worked in hardware as a Senior Field Service Engineer providing hardware and software support for PC’s, Servers, Midrange Systems and Peripherals for 9 years.

In addition to his professional career he is also a musician with several ongoing projects and enjoys cold beer and long walks in the park.



Samantha Groves: OWASP Project Manager

Samantha Groves is the Project Manager at OWASP. Samantha has led many projects in her career, some of which include website development, brand development, sustainability and socio-behavioral research projects, competitor analysis, event organization and management, volunteer engagement projects, staff recruitment and training, and marketing department organization and strategy implementation projects for a variety of commercial and not-for-profit organization. Samantha earned her MBA in International Management with a concentration in sustainability from Royal Holloway, University of London.