2014 OWASP PROJECT HANDBOOK

2014 OWASP PROJECT HANDBOOK

Prepared by: Samantha Groves, OWASP Projects Manager

January 2014

TABLE OF CONTENTS

01 ACKNOWLEDGEMENTS

1. ACKNOWLEDGEMENTS

We would like to thank the many dedicated individuals who have worked tirelessly to volunteer ideas, suggestions, content, and design suggestions to the development of this handbook. We could not have completed this document without your contributions to this initiative. Thank you.

02 OVERVIEW

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. OWASP Projects provide 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.

• **Code Library Projects:** These projects provide libraries/frameworks that can be leveraged by developers to enhance the security of their applications.

• **Operational Projects:** These projects are a bit different than the types above. They were created to offer OWASP operational support. Some examples of operational projects include the OWASP Media Project whose contributors work on managing the OWASP YouTube channel along with working towards developing media content for the Foundation.

As with all OWASP groups, 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.

03 PROJECT REQUIREMENTS

3. PROJECT REQUIREMENTS

Starting an OWASP project is a very easy process. You simply have to submit an application to start your project, and work on it under the OWASP Projects umbrella. Additionally, projects and their leaders are expected to not only know and follow OWASP Project policies and guidelines, but they are expected to uphold the OWASP core values, as well. The OWASP core values are: 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 to submit an application.

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 unless they are operational projects. 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

endeavor. Project Leaders must use the appropriate project designation to refer to their project and must not abuse the OWASP brand. Project Leaders must also conduct themselves according to the OWASP Code of Ethics, and must follow OWASP Project policies and guidelines, at all times (Appendix 8.3).

3.5 OWNERSHIP

OWASP does not require a transfer of ownership of your project as all OWASP Projects must be offered under an open source license. Open Source means that the content must be made freely available and may be redistributed and modified by anyone. Every Project Leader and contributor owns their own contributions; however, he/she must accept that all contributions made to an OWASP Project must be open source. Project owners who own all copyrights to a project outside of OWASP, and no longer wish to be involved with the day to day management of a project, are welcome to donate their work to OWASP. Please contact the OWASP Project Manager for information on how to best donate your project to OWASP.

3.6 PROJECT OPERATIONAL REQUIREMENTS

At a minimum, all OWASP Projects need to have a project name, a Project Leader, a project description, a project community friendly license choice, and a project roadmap. Below you will find a short summary of what is expected for each of these operational requirements.

PROJECT NAME

A project name will include the OWASP brand name by default. A Project Leader can choose to omit the OWASP brand name from their project name, but the Leader must inform the OWASP Project Manager before it is omitted. Otherwise, the project will be set up using 'OWASP' as a prefix to the project name in the original application.

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.

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 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 plan. 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. It is recommended that Project Leaders have at least 4 yearly milestones in their roadmap.

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 and operational projects, or a GNU General Public License variant for tools and code projects.

04 PROJECT LEADER EXPECTATIONS

4. PROJECT LEADER EXPECTATIONS

All OWASP Project Leaders are expected to act with integrity, openness, and abide by the OWASP Core Values and OWASP Code of Ethics. All Project Leaders should treat everyone within and outside the OWASP community with respect, and this includes board members and employees. Leaders should work towards collaborating in a professional manner with all involved in the face of conflict. Please remember we are all here to make the world a better place through software security by making it more visible to the world. The majority of the OWASP community is made up of volunteers, and we must all respect each other's contributions and opinions even if we disagree.

Aside from the behavioral expectations OWASP has of its Leader, there are a handful of operational OWASP Project policies and guidelines that Leaders must abide by. You can find a brief summary of each, below.

4.1 OWASP PROJECT SPENDING POLICY

The project spending policy is a series of guidelines aimed at assisting OWASP Project Leaders with OWASP Project spending related questions. Generally, it is perfectly fine to spend project funds on things such as stickers, swag, marketing or other support services. It becomes tricky when looking at whether you can spend your project's funds on another project though - technically, those are not a Project Leader's personal funds for his/her projects. A Project Leader is a steward for the funds of the project that he/she is the leader of.

If a Project Leader finds that their project funds would be of better use in another project, then we recommend those funds get donated back to the general project fund. This way, anyone can request reimbursement for expenditures for other projects from the general project budget. This shows a fairness toward all projects and more transparency in the allocation of funds.

In order to avoid any problems or misunderstandings in the future, we have developed the project spending guidelines. The aim is to provide clear expectations of how OWASP Projects should spend project funds, and what are appropriate project expenses. Please see Appendix 8.6 for a full list of the guidelines.

4.2 OWASP GRANT FUND SPENDING POLICY

OWASP has grown considerably over the past few years, and this means that our project inventory has grown as well. We currently manage over 100 open source projects under the OWASP brand umbrella. OWASP prides itself on being able to spend resources in the pursuit of potential grant funding opportunities for our projects. However, our recent successful grant proposals have added several restrictions in the way we can spend grant awarded funds as an organization. Any funds that come into OWASP have an obligation to be spent in support of the mission. Additionally, there are specific guidelines that the IRS has on expenditures that fall into the category of grants.

Grants are defined as any funds that OWASP gives (for travel or other items) without receiving anything in return. For example, when we pay for travel for Project Leaders or community members to speak at our events, this is not

a grant because we are receiving a service in exchange for covering the costs of travel. In contrast, if we pay for a Project Leader to attend an AppSec conference where we are allowing one individual from the industry to come to our event for free, and we cover the cost with no expectation of performance or work, this is a grant. We need to then show that we have criteria that were used to determine who received the funding and the amount they received, in this case.

In order to avoid any problems or mis-understandings, we have developed a few guidelines to provide clear expectations of how grant awarded funds are to be managed and spent by all OWASP Projects. Please see Appendix 8.5 for a full list of the guidelines.

4.3 OWASP PROJECT SPONSORSHIP OPERATIONAL GUIDELINES

The Project Sponsorship Operational Guidelines aim to inform project sponsors of what they can expect if they donate funds, or other resources, to an OWASP Project. Additionally, they outline what Project Leaders can offer sponsors in exchange for donating funds to their OWASP Project. In order to avoid future misunderstandings, we have developed these guidelines to provide clear expectations of how sponsors and projects are expected to interact when funds are given to a project for product development. Please see Appendix 8.7 for the guidelines.

05 OWASP PROJECT LIFECYCLE

5. OWASP 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 for projects who take on these added responsibilities. Each of these stages is described in greater detail in the sections that follow.

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

OWASP INCUBATOR PROJECT STAGE

OWASP LAB PROJECT STAGE

OWASP FLAGSHIP PROJECT STAGE

5.1 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 gives Project Leaders the opportunity to leverage the OWASP brand name and resources 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.

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 as an Incubator Project.

Once a Project Leader has completed at least one version of a concrete deliverable, the project is eligible for graduation into the OWASP Lab stage. Note that graduation to the OWASP Lab stage is optional, and a Project Leader that has completed at least one concrete deliverable may continue in the OWASP Incubator stage.

5.2 LAB PROJECTS

OWASP Lab Projects represent projects that have produced a deliverable of significant value. Leaders of OWASP Lab projects are expected to stand behind the quality of their project as these projects should 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 Lab Project Leader is producing deliverables that are ready for mainstream usage.

OWASP Lab Projects are meant to be a 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 that is required to enter the OWASP Lab stage. To enter OWASP Lab, projects must be actively maintained, they must meet the OWASP Lab project standards, and they must seek to provide value to OWASP consumers.

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

5.3 FLAGSHIP PROJECTS

The primary goal of the OWASP Flagship Project stage is to identify, highlight, and support mainstream OWASP Projects that make up a complete software security solution. Selection of Flagship Projects is driven by the OWASP Community, and eligible projects are selected from the OWASP Lab Project pool by the Technical Project Advisory Group. 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 software 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 Lab 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 software security.

06 OWASP PROJECT STAGE BENEFITS

6. OWASP PROJECT STAGE BENEFITS

The requirements laid out for the various stages of project maturity can be arduous. As all Project Leaders are volunteers, OWASP recognizes the need to offer incentives for both the Project Leader and the project itself to help it move forward. The following section provides a list of standard resources made available to Project Leaders based on their project's current maturity level.

6.1 STARTING A PROJECT: INCUBATOR STAGE 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, Resource Procurement Support, Project Review Support, WASPY Award Nominations Opportunities, OWASP Projects Track Participation, Opportunity to use Project Fund Bucket for Project Development, and Community Engagement and Promotional Opportunities.

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 unless it is pre-approved by the Foundation. These funds are meant to be used towards project expenses. For a more information on our project spending policy, please view Appendix 8.6.

RESOURCE PROCUREMENT SUPPORT

Here at OWASP, we have an opportunity to work with many contractors and experts from different industries and fields. The OWASP Operations team are a hub of contacts, and we can help find resources for Project Leaders when needed. Simply contact the OWASP Project Manager for assistance on leveraging the OWASP network.

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 can retain the services of volunteer 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 Software 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 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 Project Manager, and they take place at our global AppSec conferences every year.

INTRA-OWASP PROMOTION

Additional promotional opportunities are available via a number of our marketing channels, OWASP activities, and even via other projects within OWASP. For example, the OWASP Web Testing Environment (formerly the OWASP LiveCD), the Podcast series, the AppSec Tutorial Series, and Media 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 on who to promote rests with those community members.

OPPORTUNITY TO SUBMIT PROPOSAL FOR PROJECT DEVELOPMENT FUNDING

All OWASP Projects will have an opportunity to submit a proposal for funds that can 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 this year, and there is a proposal submission requirement before any Leader can be awarded these funds. Please note, that Flagship and Lab projects will get a preference for funding, and funds will be awarded based on an appropriate justification need, and on a first come, first serve basis.

COMMUNITY ENGAGEMENT AND PROMOTIONAL OPPORTUNITIES

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.

6.2 BENEFITS OF GRADUATING: OWASP LAB STAGE

A Lab 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. As an OWASP Lab Project, Leaders get preference for promotional opportunities over Incubator Project Leaders. Projects can expect to be highlighted or "featured" for several reasons, including but not limited to:

- New project inception

- Recent project graduation

- Recent release

- High levels of contributor activity

- Strong positive feedback responses

- 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. Additionally, there is opportunity to be highlighted in our OWASP Connector Newsletter that is sent to over 43,000 subscribers.

RESOURCE PROCUREMENT SUPPORT

The OWASP Project Manager will give preference to Lab Project Leaders over Incubator Project Leaders when there is a need for resource procurement support. Simply contact the OWASP Project Manager for assistance on leveraging the OWASP network. Please note, the Project Leader must be aware that all resource costs will need to come out of their individual project budget. Please ensure that your project has enough funds before spending funds or hiring a resource.

OWASP OPEN SOURCE SHOWCASE & OWASP PROJECTS TRACK TRAVEL FUNDING ASSISTANCE

All 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 Project Manager, and they take place at our global AppSec conferences. OWASP travel funding is 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 Open Source Showcase and/or Projects Track modules. Preference is also given to Lab Project Leaders over Incubator Project Leaders.

OPPORTUNITY TO SUBMIT PROPOSAL FOR PROJECT DEVELOPMENT FUNDING

All OWASP Projects will have an opportunity to submit a proposal for funds that can 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 this year, and there is a proposal submission requirement before you can be awarded these funds. Please note, Lab Projects will be given

extra consideration over Incubator Projects due to increased level of commitment. Funds will be awarded based on an appropriate justification need, and on a first come, first serve basis.

6.3 BENEFITS OF GRADUATING: OWASP FLAGSHIP STAGE

A Flagship project will continue to receive the same benefits that OWASP Lab 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 grant proposals 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. All projects have an opportunity to seek out and submit grant proposals; however, Flagship Projects will get preference due to our limited resources.

PROJECT PROMOTION SUPPORT

As an OWASP Flagship Project, Leaders get preference for promotional opportunities over Incubator and Lab Project Leaders. 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. Additionally, there is opportunity to be highlighted in our OWASP Connector Newsletter that is sent to over 43,000 subscribers.

OPPORTUNITY TO SUBMIT PROPOSAL FOR PROJECT DEVELOPMENT FUNDING

All OWASP Projects will have an opportunity to submit a proposal for funds that can 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 this year, and there is a proposal submission requirement before you can be awarded these funds. Please note, Flagship Projects will be given extra consideration over Incubator and Labs projects due to their increased level of commitment. Funds will be awarded based on an appropriate justification need, and on a first come, first serve basis.

07 PROJECT REVIEWS

7. 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 Projects Infrastructure. Projects can be reviewed when an Incubator Project is ready to graduate into the OWASP Lab designation, and project releases can be reviewed if the Project Leader wants the quality of their product to be vouched for by OWASP. The goal of a review is to establish a minimal baseline of project characteristics and product quality.

7.1 PROJECT REVIEWERS

The Reviewer Pool is made up of a group of individuals that aim to ensure there are qualified reviewers making quality reviews of OWASP Projects.The Reviewer Pool is made up of individuals hand selected by our OWASP Technical Project Advisors. These individuals have proven themselves dedicated to executing quality reviews of projects. Starting in 2014, members of the Reviewer Pool will be asked to fill in their user profile, which will be visible to all 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 should gain added recognition in OWASP.

7.2 PROJECT 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 types of reviews OWASP can provide for Project Leaders: Project Graduation Reviews and Project Feedback Reviews.

PROJECT GRADUATION REVIEWS

Project Leaders can submit an application for a project review to assess whether they can graduate to the next stage in the OWASP Project Lifecycle. These reviews are conducted in the same way the Feedback Reviews are. The only difference is that the project might be able to graduate to the next stage if their project assessment is positive.

PROJECT FEEDBACK REVIEWS

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 due to the high number of projects in our inventory.

7.3 PROJECT ASSESSMENTS

There are several assessments our reviewers use to determine the quality, health, and usability of a project. These assessments were developed over a 6 month period of time by our OWASP Technical Project Advisory Team. The Technical Project Advisors were recruited as volunteers to help the organization review and update the assessment criteria and project graduation process. After months of testing different assessment criteria and processes, the advisors determined that projects need to be assessed in three primary areas by both a dedicated reviewer and the community at large. Below you will find the three assessments our reviewers use to determine the quality, health, and usability of a project. When reviewing a project, all of the assessments must be used to determine a more accurate and well rounded picture of the current state of the project.

PROJECT HEALTH ASSESSMENT

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 by submitting a request for review using the OWASP contact us form. 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 concepts:

- Project Maintenance: These questions assess whether the Project Leader is keeping his/her project materials up-to-date.

- Quality Expectations: These questions assess whether the project product is of value to users and the software security industry.

- Project Best Practices: These questions are meant to assess whether a project, and its Leader, are following OWASP best practices.

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. This assessment is qualitative in nature; therefore, the outcome is subjective to the unit of measurement used, the reviewer. This is why reviewer selection for each project is crucial.

PROJECT QUALITY ASSESSMENT

The quality assessment is used to determine how good the product produced by the project is. It is meant to determine whether the product is easy to use, and whether users can find materials to help them use the product. Moreover, this assessment is meant to determine whether the product has continued support and whether the Project Leader is maintaining the product and improving upon it regularly. This assessment is conducted by the same two (2) reviewers that conduct the Project Health Assessment. Please note, this assessment is qualitative in nature, as well. Therefore, the outcome is subjective to the unit of measurement used, the reviewer.

PROJECT USABILITY AND VALUE ASSESSMENT

The Project Usability and Value criteria were created during the 2013 Project Summit as a means of properly determining product value to users. The Project Health and Quality Assessments were created before the Summit. However, during the Summit, it was determined that there needed to be some way of measuring product value to

users that was separate from the assessments the reviewers conducted. Only then could we have a well rounded picture of the current state of a project. This is where this particular assessment was developed and why.

The Project Usability and Value Assessment is a survey aimed at capturing the value a product is providing to its users. It is based on the four (4) OpenSAMM business functions and twelve (12) Security Practices. The survey is to be sent out to product users, and the assessment will only be complete after at least 10 users finish the survey. After this assessment is complete, the (2) reviewers selected to assess the project will take the results, and use the feedback to complete the qualitative project quality and health assessments. The aim is to have quantifiable metrics that demonstrate usability and value based on actual user input, and a qualitative assessment of health and quality based on expert opinion.

08 APPENDIX

8. APPENDIX

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

8.1 OWASP PROJECTS HISTORY

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.

COMMITTEE DISSOLUTION

In early 2013, the OWASP Board of Directors made the decision to do away with all of our OWASP Committees. The committee structure was completely dissolved mid 2013, which meant that the GPC would no longer be final decision makers on OWASP Projects related matters.

TECHNICAL PROJECT ADVISORS

Faced with the need for experienced technical expertise for project reviews, the OWASP Projects Manager, Samantha Groves, recruited six (6) experts from different areas of the software security community. The aim was to build a grow of Technical Project Advisors that would help develop the assessment criteria and process OWASP would use to determine project health, quality and usability for the purpose of improving overall product quality throughout our projects inventory. The assessment criteria and process has been created, and we plan on implementing it thoroughly in 2014.

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 2013

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.

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 GRANT FUND SPENDING POLICY

OWASP has grown considerably over the past few years, and this means that our project inventory has grown as well. We currently manage over 100 open source projects under the OWASP brand umbrella. OWASP prides itself on being able to spend resources in the pursuit of potential grant funding opportunities for our projects. However, our recent successful grant proposals have added several restrictions in the way we can spend grant awarded funds as an organization.

In order to avoid any problems or mis-understandings, we have developed a few guidelines to provide clear expectations of how grant awarded funds are to be managed and spent by all OWASP Projects.

GUIDELINES

1. All grant applications submitted to a grant awarding body on behalf of an OWASP Project must be submitted to the OWASP Projects Manager for approval before they are submitted to the grant awarding organization.

2. All grant funds awarded to an OWASP Project must be spent in accordance to the project plan and budget submitted to the OWASP Projects Manager, and the grant awarding organization, prior to the award of the funds.

3. All expenses to be made using grant awarded funds must be pre-approved by the OWASP Projects Manager.

4. Awarded grant funds may not be used, re-allocated, or given away to any other initiative or OWASP Project for any reason.

5. It is the Project Leader's responsibility to make sure he/she is working with the OWASP Projects Manager to manage grant related expenses and spending.

6. It is the Project Leader's responsibility to make sure they are delivering the product outlined in the grant proposal using the funding made available by the grant awarding body.

7. In the event that the awarded project terminates its activities, the OWASP Projects Manager will notify the sponsor or grant awarding organization, and inform them of the cease of activity. The grant awarding organization can then decide to either take back the funds, or donate them to another project, to the general OWASP Project fund, or to another part of the OWASP organization that accepts sponsorships.

8.6 PROJECT SPENDING POLICY

Below you will find a series of guidelines aimed at assisting OWASP Project Leaders with OWASP Project spending related questions. In order to avoid any problems or misunderstandings in the future, we have developed these guidelines to provide clear expectations of how OWASP Projects should spend project funds, and what are appropriate project expenses.

GUIDELINES

1. OWASP Project funds are to be spent on project related expenses ONLY. If your project has more than one Project Leader, then all Project Leaders must agree to the expense before the purchase.

2. Before a purchase is made, the Project Leader must make sure that his/her project actually has the funds to cover the purchase. The easiest way to do this is to communicate your purchase needs to the OWASP Projects Manager, or you can look at the running funds list provided by the Foundation.

3. Project expenses exceeding $500 USD must be communicated to the OWASP Projects Manager before the purchase.

4. All project expenses will be managed via a reimbursement process. Once a purchase is made, the purchaser must submit a reimbursement request using our reimbursement form. Note: A receipt is required for the reimbursement process to be successful.

5. Appropriate Project Expenses encompass the following: Graphic Design; Technical Contractor; Web Design; Printing; Software Purchase; Hardware Purchase; Intern Stipends; Team Travel Expenses (for project related work ONLY); Venue Hire (project related work only); Food and Drink (if used to meet with other Project Leaders, contributors, OWASP staff, or an OWASP related function); Project Contractor. Please check with the OWASP Projects Manager before you move forward with a purchase if your expense falls outside of the items listed above.

6. All OWASP Projects are started with the understanding that they will be volunteer run, and they must remain volunteer run.

7. In the event that a project's Leaders decide they would like to hire a contractor to work on a particular aspect of the project, then the Project Leaders must manage the recruitment and payment on a task/work assignment basis. Contractors must be paid upon satisfactory completion of the task/work assignment. Additionally, the OWASP Projects Manager must be be informed that project funds will be used to hire a contractor for project development.

8. Hiring Project Leaders as Contractors: If a project's Leaders decide to hire another Leader as a contractor for a project task/work assignment, then the OWASP Projects Manager must be informed before work begins. Leaders must demonstrate to the OWASP PM that they have searched for 3rd party contractors, before the decision was reached to hire the Project Leader(s) as contractors.The contracted Leader(s) will be paid upon satisfactory completion of the work.

9. As of Jan 01, 2014, OWASP will add a disclaimer to the donation page which states that the Foundation reserves the right to reallocate funds to the general Foundation income account. For all money received for projects prior to Jan 1st - OWASP will make best efforts to contact donors in respect to their donor intent before reallocating funds in the instance of inactive projects.

8.7 PROJECT SPONSORSHIP OPERATIONAL GUIDELINES

The set of guidelines below aim to inform project sponsors of what they can expect if they donate funds, or other resources, to an OWASP Project. Additionally, they outline what Project Leaders can offer sponsors in exchange for donating funds to their OWASP Project.

In order to avoid any problems or misunderstandings, we have developed these guidelines to provide clear expectations of how sponsors and projects are expected to interact when funds are given to a project for product development.

GUIDELINES

1. Any company or individual can donate funds to a project in exchange for the placement of one sponsorship logo on the OWASP project page and product they have sponsored.

2. There is no limit or minimum amount that a company or individual can give in funds to an OWASP Project. However, the minimum amount required to have a company logo on the OWASP Project wiki page and product is $1000 USD.

3. Sponsors that donate less than $1000 USD will have their company name, and website url added to the project wiki page and product. No logo will be placed for donations below this amount.

4. A sponsor can choose to donate to the overall OWASP Projects budget. If the sponsor chooses to donate to the overall Projects budget, then one logo of their choosing will be placed on the OWASP Projects wiki page under the 'Sponsors' tab. The minimum amount required to have their company logo on the OWASP Project page is $1000 USD.

5. If a sponsor is donating funds to a specific project, then the logo must be placed in the 'Acknowledgements' tab under the 'Project Sponsors' heading using the new OWASP Projects wiki template.

6. Sponsor logos must NEVER be placed anywhere other than within the 'Acknowledgements' tab under the 'Project Sponsors' heading on the project wiki page.

7. Logos must be created using the following specifications for placement on the wiki page:

Resolution: 72dpi

File Type:.PNG or .JPEG

Size: No longer than 300 x 300 px

8. Sponsor logos on the product: All sponsor logos must be placed on a page/section/location that is separate from the content of the product. They must contain the company logo, their name, and their website url. The aim is to have a separate section on the product that clearly lists sponsor information. Template acknowledgement copy: “OWASP does not endorse vendors, but we would like to acknowledge the following contributions....”

9. Logos must be created using the following specifications for placement on the product:

Resolution: 300dpi

File Type: .EPS

Size: No smaller than 5in x 5in

10. All sponsorship logos will be placed on the project product and wiki page for one year or until the next major release. All legacy projects will be given one year to comply with these guidelines starting on January 01, 2014.

11. Logos must be sent to the OWASP Project Leader for inclusion on the OWASP Project wiki page and product. It is the responsibility of the Project Leader to make sure all of his/her project sponsors are properly represented on the OWASP Project wiki page and product.

12. All additional contributors get their name, email address, company name (if desired), and a link to one external website (no logo). No logos should be added for individuals who only contribute time, or for any other sort of contribution.

13. Project Sponsorship Rejection: A Project Leader can decide to accept sponsorships or not, but this must be across the board. In essence, a Project Leader must agree to accept all sponsors, or he/she must agree to deny all sponsorship support. However, if a Project Leader wants to reject a specific sponsor (not across the board) then an exception will have to be requested from the Board of Directors.

14. If a Project Leader fails to follow these guidelines, the OWASP Projects Manager will notify the Project Leader of the infringement. If the infringement continues, the Project Leader may face the removal of all Project Leader privileges until further notice.

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 urge approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas.