COMMITTEE 2.0 - PROJECT REVIEWS PROPOSAL

August 14, 2015

OVERVIEW

The following proposal describes the mission and objectives of Project Reviews Committee 2.0. This new committee structure was approved by the board on July 2014(http://owasp.blogspot.com/2014/07/owasp-committees-20.html) which allows and empowers project leaders to work more efficiently on objectives determined by the mission and vision of OWASP.

The Objective

- Create and propose a clear and unbiased process to review projects, depending on their matureness and type (Code/Tool/Documentation)
- Community engagement to create and establish a continuous review processes
- Communicate with project leaders regarding the status of their project
- Promote projects that have requested a review and evaluation of their status
- Execute Periodic reviews, depending on the activity level and type of the project
- Identify and highlight incubator/lab projects which are excelling in innovation and progress
- Provide functional testing to code and tool projects (Smoke testing)
- Provide Static Analysis Code review to proactively alert Project leaders of potential security bugs in their code
- Annual Content Auditing to identify missing areas and content around security issues

The Opportunity

- Periodic clean-up of inactive projects
- Clean Wiki and up-to-date project inventory based on reviews and evaluation
- Provide Project leaders a platform to promote their projects
- Provide the community with updated resources
- Identify and analyze bottle necks in the development process of projects

The Solution

- For Code and tool project, we have setup all projects in Openhub to measure the activity level using(https://www.openhub.net/orgs/OWASP)

- Quarterly reviews on activity level of Incubator projects
- Project health review on quarterly basis
- Proposal for creating review methodology for Document projects

THE PROPOSAL

Several projects start under the OWASP umbrella as incubators, many fail, and some survive and become valuable tools to the open source community. In order to identify and promote the projects, it is essential to have a proper review process within OWASP. At this moment of writing, there is a basic, semi-automated process to review projects set in motion by the Project Task Force. This task force initiated a more robust review process 8 months ago, however, with the approval of a committee, we are moving forward with an official proposal in order to establish a more legal entity within OWASP to execute project reviews.

Our mission is to incorporate strategic, approved methodologies by the OWASP community. Right now there is no official and clear process how a project moves from incubator to flagship phase. One of the major problems is the lack of reviewers, therefore the task force came up with some basic process to clean-up the inventory of projects based on:

- Activity level of a project using automated SaaS such as Openduck
- Activity level on wiki page(updated information)
- Statistic information(wiki page update) (Key Indicators)
- Health criteria developed by the former Technical advisory board to measure the activity level conform OWASP principles

Even though these methodologies help us to identify active projects, it does not solve more complex issues with regards of how to identify the quality of projects, especially Document ones. Furthermore, the Project task force submitted a proposal to the community including feedback, to establish a proper process to review documents.

Execution Strategy

Our execution strategy incorporates automated tools that help us quickly categorize those projects that are inactive and lack the minimum quality standards, such as,

- Code project is not able to build (Team City, IDE's to build projects).: For this purpose, Jason Johnson helped us setup a TeamCity server to automate the builds. Right now we are in the process of configuring the projects that can be properly build through this server/ Otherwise this is tested by using a IDE such as Eclipse or Visual Studio
- does not even have an open repository available to the community : Using Openhub we were able to configure 88 projects that have an open repository
- Does not have an open source license
- No commits in over a year(code/tools)
- No active project leader
- Vendor neutrality issues

This provides the minimum standards to allow a project be active however, other criteria that determines if a project can become LAB or Flagship has been established partially through the Project Health criteria (https://docs.google.com/spreadsheet/ccc?key=0AllOCxlYdf1AdG5NZGhzTjZpT1RDcnRibjd0aXhfOUE), however

some of these are not simple to measure and they need a second review from the community to establish a better approved methodology.

We want to propose and create official guidelines that will help Project leaders understand their responsibilities and manage their expectations when starting and maintaining a project

TECHNICAL REVIEWERS

Another part of the committee's mission is to establish an independent, committed strong body of technical reviewers that can help us evaluate and provide feedback to projects. This has been one of the most difficult parts in the process due to the lack of commitment. Therefore we might look to establish strategic partnerships with other organizations that can help us accomplish this goal, such as, establishing a good relation with IEEE and look for volunteers willing to help us review documentation or request a specific grant to accomplish this by hiring technical reviewers. As mentioned before, the main problem is lack of commitment due to the amount of hours involved in the review process.

MEMBERS

Right now, the active members of the project task force are:

- Committee lead: Johanna Curiel
- Kait-Disney Leugers (Staff)
- Gary Robinson (Adviser)
- Jason Johnson (Technical Adviser/contributor)
- Jim Manico (Adviser)

CONCLUSION

This proposal aims to create a committee that can establish a more accurate review system within OWASP. Especially, it aims to improve the quality of projects and offer a platform for development and support to project leaders in their mission to make their projects valuable tools to the open source community.

We hope that with the official establishment of a committee, we are able to create the necessary process and allocate the necessary resources (staff, materials, etc.) to create a better platform to the review projects.