OWASP Project Hosting Solution Request for Proposals

Background

The OWASP Foundation came online on December 1st 2001. It was established as a 503(c) non-profit organization in the United States on April 21, 2004 to ensure the ongoing availability and support for our work at OWASP. OWASP is an international organization and the OWASP Foundation supports OWASP efforts around the world. OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem, because the most effective approaches to application security include improvements in all of these areas. Our central wiki can be found at http://www.owasp.org.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security. OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. Similar to many open-source software projects, OWASP produces many types of materials in a collaborative, open way. The OWASP Foundation is a not-for-profit entity that ensures the project's long-term success.

Since its inception as a repository for application security knowledge and information – OWASP has grown into a haven for security research tools and libraries aimed at helping organization improve the application security stance. Many of OWASP's first successful projects were documentation projects and as a result, our current infrastructure was designed around hosting projects in wiki format. However, many of our projects are now code-based tools or libraries and our current wiki infrastruction does not give us the flexibility necessary to manage these projects in a cohesive, reliable manner.

The OWASP Global Projects Committee is currently looking for proposals to provide a cohesive project hosting framework for developers and users.

Description

Our envisioned project hosting solution encompasses not just basic project management tools, but also an infrastructure to implement and/or support our broader needs to publicize and promote OWASP projects.

Basic Project Hosting Services

The following features are typical project hosting features that are relatively self explanatory and we assume will generally be part of any project hosting service proposal. Should any of these features not be available, please explicitly note the feature in the proposal.

- Issue Management
- Software Configuration Management (e.g. CVS, Subversion, Git, etc)
  - Anonymous Read Access
  - Authenticated Commit Access
  - Granular Access Control for Committers (e.g. folder-level, file-level, branch-level)
- Continuous Integration Build
- Support for various languages including, but not limited to, C/C++, Java, .Net, ASP, and PHP
- Project Metrics/Statistics for:
  - Downloads
  - Code Commits
  - Active Committers
  - Community Feedback Ratings
  - Average Issue Resolution Time
  - Open/Resolved Issue Counts

Project Content Presentation Services
The following features are related to how OWASP projects are presented and consumed to their user community. In general, while project services and templates would be standardized and provisioned by the GPC, we would like the use of such services in an individual project to be managed by the project owner so that they can be relatively self sufficient.

OWASP Branded Project wiki home page
Currently, the OWASP wiki hosts everything from chapter meeting notes, to informational articles, to project home pages. This has provided project leaders with the flexibility to create their own content as necessary to document and promote their project. However, the uncoordinated structure means that there is often no centralized place for project information. We have tried to address this by creating a standardized wiki template[1] but this template is tedious and time consuming to maintain manually. Additionally, project leaders can create wiki pages that end up clobbering or colliding with other projects or initiatives.

We would like to have project home pages that are isolated from each other and provides some consistent structure for basic project metadata, while providing project leaders the freedom and flexibility to create web content for their project as appropriate.

Mailing Lists / User Groups
All OWASP projects have individual mailing lists that are manually provisioned using OWASP's MailMan instance. The mailing list administrator must be manually set whenever a new project leader or core contributor arises. While the infrastructure is solidly in place, the process adds extra overhead to project management. Additionally, project leaders who want specialized mailing lists (e.g. announcement-only lists for patches) or other special requests add to the overhead.

We would like a service that provides some level of self-provisioning of mailing lists for projects. This provisioning can be a service that provisions default mailing lists automatically at project creation or provides project owners the ability to self-provision desired mailing lists within their project namespace.

Downloads Page
There is currently no consistent mechanism for OWASP projects to provide project downloads. In some cases, leaders will upload project releases to the OWASP wiki as "media files" and reference them in the wiki. In other cases, they will provide links to external sites where project releases can be downloaded. The inconsistency makes it difficult for users to find OWASP project releases and also makes it impossible for us to track the popularity (e.g. number of downloads) of OWASP projects.

We would like to have a project release download mechanism for projects that allows us to track download statistics and also provides users a consistent place to find project releases. Furthermore, this download mechanism must support the ability to make large files available for download. For example, the OWASP LiveCD distribution is several gigabytes in size.

Native Language Documentation
The current OWASP wiki is not conducive to publishing native language documentation, such a JavaDoc or PHPDoc, for our code-based projects.

We would like the project hosting service to support publication of such documentation under a project's namespace as appropriate.

Project Management Services
The following features relate to the ability of OWASP (and the GPC in particular) to leverage the project hosting solution in support of the OWASP mission. We recognize that these features may not be available "out-of-box". We would service providers to indicate how they envision their service could be used to support such features if not already implemented. Customization work can be included in service proposals.

Customizable (OWASP Branded) Projects Portal
With over 160 projects, we have a need to balance the visibility of projects on our main page to promote both mature projects and those that are still growing. Currently, OWASP projects are listed on the project page in a somewhat ad-hoc manner that unfairly benefits established projects. The sheer volume of projects also makes it extremely difficult for potential users to navigate and find projects of interest.

We would like for any project hosting service to support the ability to have a customizable, dynamically driven projects portal. This portal would highlight projects on a rotating basis on customized selection criteria. The portal should also allow users to search and navigate projects based on function, category, classification (e.g. Incubator, Labs, Mainstream, etc) and other similar project metadata. Ideally, the infrastructure would support tagging projects with relevant keywords which can then drive dynamic views of the portal.

---

[1] See https://www.owasp.org/index.php/Projects/Live_CD

Metrics Reporting

One of the reasons for gathering the metrics noted above (e.g. downloads, user activity, community ratings, etc) is to help determine projects in need of attention and identifying projects that have reached a minimal level of maturity. In support of this goal, we would like any project hosting solution to support the aggregation and reporting of accumulated project metrics.

Per Project Feature Settings

OWASP hosts a variety of projects including documentation projects, tools, and code libraries. Not every project will need native language documentation publication features or continuous build integration.

We would like for any project hosting service to support adding or disabling features that are relevant to a specific project.

Review Process

OWASP projects are periodically reviewed by community members for maturity, quality, usability, etc. We would like for any project hosting service to support a project review process by tracking progress and lifecycle of formal reviews. Such a process may include capturing and publishing feedback and quality metrics.

Hardened Security

As OWASP is an application security community, it would be hypocritical of us to use a project hosting service that was not secure. We would like for any project hosting service to have a concrete security plan for a reliable, hardened hosting solution. Additionally, we would appreciate (but do not require) the opportunity for our community to test the security of any hosting solution in a controlled environment to provide constructive feedback to the provider should their service be chosen.

Evaluation Criteria

The above features indicate our ideal goal for a project hosting service solution. We recognize that not all features are necessarily feasible or economical and fully expect that there may be some customization work to be done (either by the provider or by us). All proposals will be given consideration, though preference will be given to those proposals which satisfy a majority of our feature requests. Additionally, as OWASP is a 503(c) non-profit organization consisting almost exclusively of volunteers, proposals that offer services or products as donations to the organization will be given preference. Any provider that donates such services would be recognized as an OWASP Corporate Sponsor and such services may be tax-deductible.

Timeline

Date	Milestone
May 1st, 2011	RFP Initially Published
May 31st, 2011	Deadline for Proposal Submissions
June 6th-10th, 2011	Project Hosting Proposal Review period
June 15th, 2011	Announcement of Proposal Selection
June 30th, 2011	Contract Signed by OWASP
July 1st, 2011	OWASP Projects Chosen for Pilot
August 1st, 2011	Project Hosting service ready for pilot use
September 20th, 2011	Pilot projects migrated, projects portal prototyped
November 1st, 2011	OWASP Project Hosting Service formally launched

How to Submit

Please send all proposals, via email to projects@owasp.org. Proposal documents should be attached to the e-mail in PDF format and should include at minimum:

- Pricing options (if variable) for different time periods (6 months, 1 year, 2 year, etc)
- Requested Features Supported
- Customization Support Options (if available)
- Anticipated Service Level Agreement

The submission deadline for proposals is **May 31st, 2011**.