HOST Grant Funding Application

Introduction

Georgia Tech Research Institute (GTRI), through funding by the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T) , Cybersecurity Division is responsible for carrying out key components of the Homeland Open Security Technology program (HOST).

The HOST program was created to identify new, emerging and undervalued open source solutions to cyber security challenges and to share that information broadly; to make strategic investments in projects with high-impact potential; to encourage innovation by enabling cross-industry collaboration. The Investment component of the program is intended to contribute seed investment in advanced research and development activities that support national cybersecurity objectives and have the potential to create sustainable project communities.

The Investment program is seeking grant applications for projects which fall within its mission.

General Guidance

As a general rule, any effort that contributes to an open source approach to cybersecurity will be considered. Ideal applications would include projects which are:

- Open source (either code or content)
- Built upon existing open source work or projects already underway
- Affiliated with an organization or community that can sustain the effort after the funding is expended

Reference projects: Recent program investments have included contributions to the development of Intrusion Detection Systems (IDS) and government certification of open source security standards. Other projects now under consideration include piloting deployment of OSS security systems in a municipal government environment; development and publication of guides to best security practices for web applications.

Case Study

All funded projects will participate in pre- and post-project surveys and a case study for the purpose of information sharing.

For additional information please email your inquiry to HOST-investment@gtri.gatech.edu

HOST Investment Funding Questionnaire
OWASP ESAPI Libraries Project

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

1 – Sponsoring Organization

- OWASP ESAPI Reboot Project
- OWASP Foundation
- Samantha Groves
- Samantha.Groves@owasp.org
- +44 07838455215
- 9175 Guilford Road; Suite 300; Columbia, MD 20640
- OWASP ESAPI wiki page

2 – Project Summary

In 200-400 words, please write a summary of your project.

The OWASP Foundation proposes to initiate the OWASP Enterprise Security API (ESAPI) Reboot Project. The original OWASP ESAPI Project was a free, open source, web application security control library that made it easier for programmers to write lower-risk applications. The ESAPI libraries were designed to make it easier for programmers to retrofit security into existing applications. This project was first developed in the past through volunteer contributions, and has continued to be updated sporadically by the OWASP community since its inception. ESAPI is one of OWASP's most widely used and distributed projects, and it is currently in a position where it needs to be updated and re-vamped.

In April 2012, the OWASP Foundation made the decision to fund the redesign and redevelopment of ESAPI, which is why the OWASP ESAPI Reboot Project was created. The OWASP led, reboot redesign initiative will focus on gathering key players in the application security and development communities to design, develop, and distribute a new version of the ESAPI libraries.

The funding is needed as the original OWASP ESAPI Project has simply reached a point where a more dedicated team is needed to complete the work required to create an updated, high quality deliverable. Our primary objectives are to redesign the ESAPI project framework, develop new and updated ESAPI documentation, to release a high quality OWASP product, and to market the finished deliverable to increased adoption. The amount requested is $25,000 USD. The project would begin immediately after receiving funds, and we estimate that the time to completion will be 15 months.

3 – Problem Statement

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

ESAPI was originally designed for a previous web application landscape. However, the IT and security

worlds have changed much since it was first conceived in 2006, and ESAPI needs to embrace these changes. One such change involves componentization. The web is becoming a modular framework where components are dropped in and out ad-hoc depending on the need of the application and its users, at any given point in time. ESAPI needs to embrace this paradigm, and alter its design to work in that philosophy. Another problem is the current platform. Web application has changed a great deal in the last decade, and the browser is no longer the only consumer of content from web applications. We need to extend ESAPI to take mobile clients and web services, as well as the more traditional browsers into consideration. Footprint is another one of our problems that we hope to address with this update. The #1 complaint for ESAPI has always been the number of direct and indirect library dependencies. There is a lot of implied trust being passed to a lot of code that is simply never used by ESAPI users. This builds on the componentization aspect of the effort, and enables us to have tighter control on what code we are using. Integration is another concern that has come up over the years. Currently it is far too difficult to integrate ESAPI into the big frameworks. There is no clear path to integration. The new ESAPI needs to address this concern and ease the path to integration with the top frameworks.

In addition, ESAPI lacks sufficient “overview” and “how-to” documentation. While ESAPI has lots of excellent detailed API documentation, there is very little documentation that provides the big picture of how applications should use ESAPI. Often ESAPI provides multiple ways to solve the same problem, and sometimes this can be detrimental to those trying to learn how to use it. “How-to” type documentation would help address this learning gap.

Another major problem we hope to address with the OWASP ESAPI Reboot project is the multiple language issue. Currently, there are multiple language versions of ESAPI that are in various states of development. Shortly after the 2.0 release of ESAPI for Java became generally available, it quickly became apparent that the development of all the other various programming language implementations were lagging behind. At last count, there were implementations for ESAPI in more than a dozen different programming languages, most of those which were based on the 1.4 ESAPI for Java release which had some significant design vulnerabilities. Moreover, some security controls are completely missing from some language implementations. We hope to correct these issues during the first stage of development.

One last major issue involves the ESAPI extensions. There are some security controls in ESAPI that are really just proof-of-concept or “toy” examples. The “E” in ESAPI is supposed to stand for “Enterprise”; toy examples need not apply. Every security control should have at least one minimally useful reference implementation for each security control. Also, the ESAPI security configuration mechanism needs to support a clear separation of duties. Operations staff or corporate security need to be able to “lock down” certain properties to enforce specific corporate security policy, while allowing the development staff to control other properties. Currently this is very difficult to enforce because all the security settings are in a single ESAPI.properties file. We plan to rectify this issue during development as well.

Lastly, there are miscellaneous ESAPI bug fixes that need to be addressed. Most of the ESAPI implementations have open issues, some of which are serious. These need to be fixed and closed during development.

4 – Solution Statement
In 250-750 words, please describe the solution(s) this project will deliver:

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

We plan to amend and fix the current ESAPI project framework to create a more up-to-date, high quality deliverable. In addition, we plan to create new ESAPI documentation to match the new framework, and we plan to market the finished deliverables to increased adoption.

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

Yes, our solution does involve a handful of technical innovations. One of the current technical innovations is the implementation of an extensive, but consistent set of security controls across a broad and diverse set of programming languages. These languages include: Java, C#, PHP, ColdFusion CFML, C, C++, Perl, JavaScript, Python, and many more. One important detail to point out is that our security controls will be written and vetted by developers with extensive experience in application security. This will help the project with quality and accuracy control.

What social benefit is expected to accrue to cyber security as a result of the solution and how would it accrue based on the scope of the project?

The social benefits of web applications, and the work needed to secure them, is very underestimated. Most of world is run on applications found on the internet as they are able to support critical infrastructures more easily on a global scale. We at OWASP believe it is paramount to help secure these systems from attacks no matter where their origin is. Our goal with the OWASP ESAPI Reboot Project is help programmers write lower risk applications by providing them with an up-to-date web application security control library, that enables them to retrofit security into existing applications.

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

The OWASP ESAPI Reboot Project is not contingent upon the completion of other related projects; however, there are four project stages within the overall project that are important to address. The third stage of the project involves the development of ESAPI documentation. The deliverable will be an ESAPI reference manual based on the updated framework. The Fourth project stage will involve our global adoption initiatives. In this stage, we plan on developing and implementing the project's marketing initiatives with the aim of increasing the adoption of the ESAPI deliverable. These two stages will begin once updating of the ESAPI framework has been completed.

Goals:
Our goal is to update the current ESAPI libraries, and fix any known bugs within the ESAPI framework.

Moreover, we aim to produce a high quality deliverable with reference documentation and marketing materials.

- Updated ESAPI Libraries
- Fix any known bugs in existing framework
- ESAPI Reference Manual
- ESAPI Marketing Initiatives (Includes tutorial video series)

High quality, meaning peer-reviewed.

The previous editions of the ESAPI libraries were very well received with thousands of users consuming the deliverables. The goal of this project it to update these libraries to reflect the current state of software development.

5 – Context

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

Describe the technical environment in which the problems exist.

Following the original mission statement of OWASP, ESAPI has a definite web application slant to it. However, in the last several years, the world has expanded beyond web applications viewed in browsers. It has become apparent that developers writing mobile applications or stand-alone server applications also need help in addressing the overwhelming number of security issues that they face. Future versions of ESAPI will attempt to take these additional contexts into account.

What is the specific problem or core issue this solution would address?

Refreshing the current ESAPI framework, and updating the ESAPI libraries with more current information and code, will make them far more applicable for today's modern applications. The original goal of the OWASP ESAPI project was to help programmers write lower risk applications by providing them with a web application security control library that enables them to retrofit security into existing applications. We plan on developing and updating those libraries as we feel this will facilitate security implementation at the programmer level, thereby helping decrease the major web application breaches we so commonly see today.

How does the problem or issue relate to your organization and why is your organization qualified to undertake this project?

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. OWASP is more than qualified to undertake this project as the organization, and its many industry contributors, have been involved with developing communications that help in securing web applications for more than 11 years. In addition, the ESAPI project has already been developed, and has been a very successful project throughout the years. The ESAPI libraries have been used by thousands, and OWASP hopes to update the framework in the hopes of continuing to provide value to the information security community.

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

Connect each step of your work with your goals.

The primary objectives for the OWASP ESAPI Reboot project are to gather key players in the application security and development communities to design, develop, and distribute a new version of the ESAPI libraries. OWASP feels that this project will allow us to distribute up-to-date content and information to the developer community thereby allowing ESAPI to continue to create value for its consumers. Moreover, a major goal of this project is to develop a high quality deliverable, reviewed by industry peers, using OWASP project quality criteria.

The first stage of this project involves a review of the current version of ESAPI to help the development team understand the current landscape. This stage will also help the team pinpoint any shortfalls, and evaluate the removal, or addition of controls to the ESAPI core. The team will define the 50% and 100% milestones for the project during this stage as well. Defining the milestones will help the project team keep track of the management stages and their project accomplishments. The second stage will involve an OWASP Hackathon event. The ESAPI:Rebooted Hackathon will be a 2-day event held after the first stage of the project is completed. The primary goals of the hackathon are to foster new development and contributions from the development community, and extend the reach of ESAPI into additional platforms. Developers attending the hackathon will compete to create ESAPI-Enabled components (leveraging the new API). The core team will be responsible for ensuring the API is ready before the hackathon, and for providing end users with the API.

The remaining stages will focus on the documentation and marketing initiatives of the project. The third stage will involve developing the technical requirements for the documentation deliverable. This will involve creating a reference manual that matches the updated configuration of the ESAPI libraries. Authors will be selected and allocated based on skill and experience to design and develop this deliverable for the project.

The last stage involves the marketing plan. The goal of this stage is to provide an itinerary of deliverables the help the updated ESAPI libraries with promotion. The aim is to increase adoption of the deliverable.

There are four major goals we hope to accomplish with the OWASP ESAPI Reboot Project. We feel that by dividing the work into these four management stages, the project team will be in a better position to allocate resources to the different work initiatives throughout the lifecycle of project.

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

Each management stage will have a 50% milestone review and a 100% milestone review. During the first stage, a peer review of the updated ESAPI framework and libraries will be required at the proposed 50% milestone. This 50% technical milestone review will focus on quality and content that will be agreed upon before project initiation. At the 100% technical milestone review, a professional technical project reviewer will be allocated to further establish accuracy, and ensure a high quality deliverable for the project. The Hackathon event will have it's 50% review before the event occurs, and the 100% review after the event. These reviews will be in the form of a meeting with the OWASP Project Manager to ensure all objectives are met. The project's reference manual and marketing initiatives plan will have their own 50% and 100% milestone reviews, as well.

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

The OWASP Foundation will lead this project and provide project management and project support resources to ensure completion and quality control of the OWASP ESAPI Reboot Project. OWASP will reach out to our community for volunteers and contributors. We will also review the deliverable at both the 50% and the 100% milestones for the technical, Hackathon logistics planning, manual design, and marketing initiatives work stages.

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

Yes, the OWASP Foundation has donated $5,000 to the OWASP ESAPI Reboot project.

7 – Projected Outcomes

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

How would you define success for this project?

The success of the OWASP ESAPI Reboot Project will focus on accuracy and quality that will be agreed upon before project initiation. The success criteria will be documented in the project product description and quality management strategy that will be created by the OWASP Project Manager with recommendations from the ESAPI Reboot project leaders.

In addition to the individual product descriptions, OWASP has defined requirement guidelines for a project release that are based on quality review by OWASP members. In order to have a release signed by OWASP:

- The project must be in good standing with the organization.
- The release to be approved must be submitted to the official OWASP Project Repository for archival

purposes.
• The release must have an aggregate of at least five (5) positive feedback responses by OWASP reviewers.

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

The most important measurable outcomes of the proposed OWASP ESAPI Reboot project are an updated version of the ESAPI libraries that are free to all who wish to use the information. The ESAPI Reboot team will also develop a tutorial series with subsequent marketing materials, and a reference manual that will compliment the updated libraries. All materials will be available free of charge under an open source license.

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

The OWASP ESAPI Reboot project will change software security as it will help developers by making it easier for them to write lower-risk applications. The current version of ESAPI has already accomplished this, but the libraries are outdated. They are in dire need of a redesign and an update. This is why OWASP feels that the ESAPI Reboot project is one of our most important initiatives for the next year. The original ESAPI libraries were designed to make it easier for programmers to retrofit security into existing applications. They served as a solid foundation for new development, and we believe it is important to continue to provide a quality, up-to-date service to the ESAPI consumer community.

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

The next steps following completion of the proposed ESAPI library updates are to design and develop an ESAPI video series that will focus on a set of easy to follow tutorials on implementing and using ESAPI controls in applications. Most importantly, OWASP plans to develop an ESAPI reference manual that will cover everything from installation to writing custom controls and components.

8 – Project Budget
An important component of your proposal is the preparation of an initial high-level budget that is reasonable. Please ensure that everything mentioned in the proposal is accounted for in the budget. Complete every field using your best judgment when projecting project expenses. Provide any detail in the notes section that you feel would be helpful to provide clarity.

If you anticipate support (including in-kind) from an organization other than HOST, please enter those amounts below and use the notes field to describe the nature of the in-kind description.

Budget Definitions
• Personnel - salaries, benefits and associated fringe costs
• Other Direct Expenses - communications/marketing, travel, meeting expenses, project space
• Purchased Services - consultant and/or third-party contractor costs
• Indirect Expenses - administrative expenses related to overall operations

Budget Category	HOST Support	OWASP Foundation (Reboot Initiative)	Notes	Total
Personnel	$0	$2000		$2,000
Other Direct Expenses	$12,000	$3,000		$15,000
Purchased Services	$5,000			$5,000
Indirect Expenses	$8,000			$8,000
Grand Total	$25,000	$5,000		$30,000

Host Support Budget Narrative

- **Other Direct Expenses:** This will cover the design and development of marketing/communications materials for the Hackathon event, along with marketing materials for the ESAPI Launch. This will also cover catering for the initial ESAPI updating meeting, and the catering for the subsequent ESAPI Hackathon where more of the OWASP community will be involved in development.
- **Purchased Services:** Services such as the following: graphic designer, reference manual editor, voice actor, video producer, audio producer, web developer (brochure site for ESAPI).
- **Indirect Expenses:** $1000 budget for each project stage to take care of extraneous expenses that come up during development; however, we feel that only 3 stages require this budget. These 3 major stages are: Hackathon (Major goal of Hackathon: foster new development and contributions from the development community, and extend the reach of ESAPI into additional platforms), Reference Manual Development, Marketing Initiatives Development and Launch. The $5000 is for operating expenses which includes: overall advertising, systems maintenance (for the ESAPI "site"), and ESAPI booth space at upcoming development conferences for promotion of project.

OWASP Foundation Support Budget Narrative

- **Personnel:** $500 stipend to be allocated to each primary project contributor for incidentals during development. These include office products, technology, food, unanticipated travel, or other expenses that occur. There are only 4 main contributors for this project, and they will lead the initiatives as a group.

- **Other Direct Expenses:** This is covering our OWASP Project Leader's primary travel expenses as they need to get together to update the ESAPI libraries, and to run the ESAPI Hackathon Event.

Budget Narrative

I am using this space to give my budget allocation a bit more detail for us. Keep in mind that I used the original ESAPI reboot proposal as the basis for this allocation. See here.

I am leaving this bit out of the proposal. This is mostly so we can agree on how we want to spend the money overall. Here is my breakdown:

Key
DE: Direct Expenses
P: Personnel
PO: Personnel covered by OWASP Funds
DEO: Direct Expenses covered by OWASP Funds
PS: Purchased Services
IE: Indirect Expenses

• ESAPI Redesign
- Project Leader Stipend for Incidentals (Throughout the Project): $2000 *PO*
- Extraneous Expenses Budget: $500 *DEO*
- Operating Expenses (Throughout the Project): $5,000 *IE*

• Hackathon Event
- Travel for Leaders: $2,500 *DEO*
- Marketing for the Event: $3000 *DE*
- Catering/Venue Hire: $3,000 *DE*
- Extraneous Expenses Budget: $ 1000 *IE*

• Documentation Sprint
- Authors, Graphic Designers, Editors, Publishers: $6,000 *DE*
- Extraneous Expenses Budget: $ 1000 *IE*

• Tutorial/Promotions Series
- Voice Actor, Video Producer, Graphic Designer, Audio Producer: $5,000 *PS*
- Extraneous Expenses Budget: $ 1000 *IE*

Please explain your approach for use of grant funds if not previously defined in your project approach, activities or other other sections of your application; how will funds for personnel be expended, staff or contract work? What services will be purchased? Are these one time expenses, or will the expense require an ongoing commitment to sustain the activity?

Submit Your Proposal

Please submit this completed proposal to: HOST-investment@gtri.gatech.edu After you submit your grant request proposal, we will send you an email within three days acknowledging receipt of your proposal. We carefully review every proposal. Within one weeks of receipt we will be in contact with you to schedule a time to review your proposal in greater detail.

Thank you for your interest in the program.