Project Proposal/Initiative Name

OWASP Security Pre-accelerator Start-up Program

Project-Initiative Proposal Leaders

Marco Morana, OWASP Chapter London
Neill Gernon, OWASP Chapter Dublin

Initiative Overview

The focus of this initiative is to create open source material such as documentation manuals, wiki page resources and piloting data that can be used by the application security community for the management of a security pre-accelerator program. The goal of this pre-accelerator program is to catalyse innovation in application security by promoting the use of OWASP resources (e.g. security testing tools, technical documentation, training modules) within the start-up community and in a roadmap of a creation of possible start-up whose business plan includes the use of these OWASP resources. The pre-incubator phase is the preliminary phase that leads to incubation of a possible start-up. This is the phase where ideas brainstorm and are validated with a Proof of Concepts PoCs and working software tools and prototypes. These PoCs might be funded by non-profit (e.g. academics) and for profit entities (e.g. vendors) and validated by the open source community. At a later stage some of these validated PoC might help the pre-incubator teams to seek funding for a security start up can create an opportunity for employment in the application security industry.

Goals

The goal of the pre-incubator is to create opportunities to transform ideas into validated concepts and onto POC (proof of concept) prototypes. To pursuit innovative ideas and development of (PoCs) Proof of Concepts of web and mobile applications that use both OWASP open source tools as well as commercial APIs. The pre-incubator will offer a structured place to work to pre-incubate ideas into working prototypes using OWASP funded projects with backing of corporate sponsorship also provided through OWASP. These PoS will be released to the open source community for validation and use as a free resource.

Benefits for OWASP

The OWASP pre-incubator security start-up project empowers OWASP to leverage academic institutions and corporate sponsors to promote projects for the development of open source tools, improve visibility to application security and foster the creation of team of software developers interested in experimenting with OWASP open source tools for the creation of new software products. By spearheading the incubation of new software prototypes OWASP will create the opportunity for software developers, software and application security testers and consultants to become self-sufficient in supporting the further development of software and services as a security start-up. These security start-ups will have the opportunity to

DISCLAIMER: This material is to be considered property of the author(s) of the proposal Marco Morana and Neill Gernon and the information should be confidential information and cannot be released to general public or used by any organization or commercial entity without permissions of the authors

leverage OWASP resources for their security consulting, application security training and secure software development services in full respect of legal agreements for the use of open source licenses when these are used in their commercial services or products.

OWASP won’t be involved in the creation of the start-up but in the funding and mentoring support of the creation of open source projects that are delivered by the teams enrolled in the pre-incubator start-up program. OWASP through his local chapters will provide in-person mentoring to help mature the PoC from pre-incubation phase to incubation based by providing connections to seek funds for incubate start-ups whose business plan include either the use of open source for their consulting services or further development of products that use open source libraries

Expectation from OWASP

1. Assist as an advocate in the distribution of this programme to other sources that wish to replicate a pre-accelerator (e.g. Universities, government organizations);
2. Assistance to advocate, refer and gather future non-profit as well as corporate sponsors who wish to participate in the funding of the prototypes being developed with the pre-accelerator as proof of concept of R&D to be released as open source;
3. General open source community support to promote program to community people (individuals not working on behalf of company's) who may wish to create a product prototype;

Funding

Expenses for running the initiative for security incubator start-up development, including piloting the initiative logistics- management, administration, creation of website creation of guidelines and manuals (*)and funding for the prototype development is £10,000 total. Disbursements are provided based upon expenses in preparation of the following events:

1) Pilot-Launch Event - £500
2) Pilot-Workshops Event- £1500
3) Pilot- Hackathon Event - £2500

(Note: please refer to the project description for the details of these activities)

In addition the funding will be allocated for the development of the following documentation artefacts:

1) – Programme Guideline, Manuals & Wiki Page-£2000
2) – Development of working Prototype- -£5000 (**)

*The *programme structure and manual and the prototype* are provided by OWASP as resource so it can be run by other university, corporate and start-up communitys.*
***The working prototype* is based upon use of OWASP resources and commercially available software development tools including vendor APIs and software**

DISCLAIMER: This material is to be considered property of the author(s) of the proposal Marco Morana and Neill Gernon and the information should be confidential information and cannot be released to general public or used by any organization or commercial entity without permissions of the authors

OWASP Security Start-up Pre-acceleration Initiative: Project Description

Project Milestones

The OWASP pre-incubator security start-up project includes the following milestones;

1) **OWASP Security start-up pre-incubator process guide** that document the process the WHAT that is a guide that can be followed by a non-profit entity such as OWASP, University, and Government Agency to run a security start-up pre-incubator program. We will document all steps of the process that can be followed to create pre seed funding security start-ups which can be replicated by following this program including the different stages that lead from opportunity to idea concept to creation of the open source prototype to the start-ups itself. The guide provide guidance on the goals of the various activities such as hackatons (e.g. goal is to experiment with OWASP open source tools, templates for the development of working prototypes) create and sign legal contract agreements, creation and validation of PoCs Proof of Concepts
2) **OWASP Security start-up pre-incubator process manual that teaches** the HOW that is how to engage with the start-up community locally (start), organize meetings, hackatons, select ideas for prototypes development, mentoring and prepare business plans for participation to security incubators start-ups (end);
3) **OWASP Security start-up pre-incubator wiki site** to manage the steps of the startup security pre accelerator process and document the proof of concept prototypes that can go on to be fully incubated start-ups; This wiki site will be created as OWASP branded pre-accelerator web site and will help it to be taken forward and used by OWASP chapters in different areas/countries. This will give the OWASP pre-accelerator an identity which will help adoption, recognition and community credibility;
4) **Documented results of piloting with a start-up pre-incubator real case** that includes using the process guide the manual the wiki site to run a real case of pre-incubator program by running it at one of the established start up campuses in London such as Level39, Google Campus or other pending on availability and agreements
5) **OWASP open source working software prototype/PoC** of an open source application security software/technology. This prototype/PoC is produced by following the several steps of the pre-accelerator security incubator program and is produced by the initiative participants as residents in the pre-accelerator working space and validated by the open source community. *The scope of the prototype is to validate a proof of concept of a new idea that makes either web or mobile applications more secure.* This prototype is released as open source to the community

Project Stages

There are 3 stages within the Initiative:

1) Open/Announce Event (page 3)
2) Lean Prototyping Workshops (page 4)

3) Cyber Security Hackathon (page 5)

Non-Commercialization Constraints

This initiative will not be made into a commercial initiative for profit. It will continue to be an open source framework to be used at corporate, university and start-up ecosystem level to help drive security innovation and create a cluster of security prototypes that can be taken on at a later and separate stage for growth funding and commercialisation.

Stage 1- Open & Announce Event:

Engage with prospective participants (design, business and tech entrepreneurs/academia students) through open event discussing how the programme works and the overall opportunities within security for start-ups/entrepreneurs. Panel will hold security leaders from corporate.

Milestones/goals

(a) Organise community: *Engage and propose program with key collaborators/partners*> start-up hubs that we wish to work with to facilitate venue and entrepreneurs (IDEA London/Google Campus/Rainmaking Loft), key university's to facilitate with access to student talent (Kings & UCL) along with key meet up groups that can contribute with talent such as Developer groups on Meetup.com.

(b) - Promote: Once a specific date, time and venue has been agreed with the key collaborators we push promotion of kick off/launch event with collaborators and independently promote to our contacts and community through general promotion streams> social sites, posters in start-up hubs/university's, announce with meetup.com group partners (i.e. - developer groups) that have community relevant to our program (they can announce in email etc.). *Do everything to promote the event/program.* Having organised community in section (a) above will allow this to be promoted well through partners. *Community should understand the overall proposal and an overview of the program process.*

(c) - Engage: Host the kick off open to community event which will have the partners and the collected community attending. The focus is on *identifying opportunities that start-ups have within security* and making sure that the community *understand the process and how the pre-accelerator will work.*

-Structure of event follows: 1. Presentations from corporate security leaders on problem/opportunity areas. 2. Presentation of pre-accelerator program and how it will run. 3. Open engaging audience discussion and q&a.

-Registration & Signup participants: People interested in participating in the initiative will be invited to sign up to the pre-accelerator program through a registration page which would be announced through partner’s pre-launch event or on the night itself. Registration done through *launchrock.com* (capturing emails for registration). Other tools like eventbrite can be used to promote signup and get commitment.

-Further opportunity sharing: On the night of the kick-off event we announce this event will be followed by an add on workshop continuing to explore pain points, needs for innovation, (API) opportunity's and problems within security.

Example: "problems/trends/opportunities in Authentication" presented by Marco Morana (2 hour live workshop at chosen London venue). Present, discuss and q&a format. The result here is that start-ups/initiative attendees would have greater knowledge on the pain points within business before starting to explore the potential solutions.

This exploration and opportunity focused dialog can continue multiple times if required also through live, interactive webcasts via online tools. I.e. google hangout

Stage 2- Lean Prototyping workshops:

Following our open event and engaging workshop to discuss opportunities we are now at the stage where our potential participants have signed up to our pre-accelerator and are up-skilled and have some additional insight to problems and key areas of focus. Lean Prototyping workshops will start off by defining and building the right multidisciplinary teams before starting the iterative stages of opportunity analysis, rapid concept development and validation. More on Lean Prototyping, here.

Milestones/goals

(a) - Build Teams: We will split up into individuals that attended together - let groups stay together and for other individuals that showed up on their own > split into design, business and tech people. Also split into idea stage or opportunity seekers. Then co-ordinate a varied mix of people. *A starting point is to get each person in the room to introduce themselves - name, background, interests etc.*

(b) - Opportunity Analysis: Once teams are formed, kick off and start workshop.

1. Openly discussion on “what is” happening within the chosen section of security - 10min
2. Individually**,** participants map details of experiences for "what is" happening within chosen section of security - 10min
3. Openly discuss opportunities & create group Map - 10min *highlight key problem areas and discuss*

(c) - Rapid Concept Development:

1. Individually sketch out the possibilities for "what if" we created this concept to solve this problem, Crazier ideas the better taking inspiration for key problem areas. - 10min.
2. One person at a time - presents ideas and discuss with team. All comments/perspectives count. Evolve ideas as people contribute
3. Individually, Evolve & sketch 1 idea - 10min

Each person presents your idea to team - 5min / Discuss with team - 5min and gets feedback.

4. Team Recap - 20 second rapid pitch per person for all the concepts in the group.

Score the concepts through NAF (novelty, attractiveness, feasibility) 1-10 for each! Highest score gets additional time to iterate and create a more robust concept iterating on the key features using the previous framework of "what is" - "what if" - team compare, discuss and evolve concepts on features with scoring of NAF along the way.

(d) - Validation & Testing

Concepts at this stage will be well articulated, constructed and visible in format.

1. Now apply this to be re formatted and fitting to paper prototyping applications such as pop-app / proto.io etc.
2. Test with chosen users, validation from corporate sponsor and feedback on product proposition to make key changes.

DISCLAIMER: This material is to be considered property of the author(s) of the proposal Marco Morana and Neill Gernon and the information should be confidential information and cannot be released to general public or used by any organization or commercial entity without permissions of the authors

2. Apply business model canvas to construct business case & continue experiment + Javeline.com

Stage 3-Cyber Security Hackathon

At this stage the foundation has been laid and we now have established teams that have an early stage lean prototype that has had some testing and continuous validation from our security sponsorship partners. We now start to add design and code to the early stage concepts to get to a POC (proof of concept) prototype. The hackathon will allow a burst of effort to finish this prototype.

Format: 2 day hackathon with a 1 week gap between the end of hackathon and final prototype changes (pitches made to corporate security leaders/sponsors). This is to allow final prototype changes following end of day validation.
Process: 2 day hack, pitches, feedback, 1week change period, re-pitches > announce teams that will progress to funding stage.
Sponsors: Sponsors and senior corporate leaders will attend sections of the hackathon to engage, validate and inspect the prototypes and judge the final propositions.

Milestones/goals

(a) Format overview

This will be the kick off morning overview of what has been done so far and what we're looking to achieve over the next 2 days. Plus - an incentive to finish well can include access to sponsor resources, potential funding and guidance and encouragement from security leaders.

(c) Hackathon

This is where the teams get into adding design & code to their prototypes. Simply this is an undefined structure and they get coding/designing after the initial opening morning. Advice and validation is giving when required at sections thorough out the hackathon.

(d) Validate Hackathon Prototype

Having mentors on site and different times during the 2 day hackathon will be useful and each time can ask for validation and advice on what ever areas the feel are most challenging.

API - Hackathon

API's: If certain corporate sponsors wish to open up and provide information and access to APIs then teams can work on products with APIs. This should be discussed at project 1 at the open events and if APIs are provided then teams can start working on some ideas through project 2 within the lean prototyping workshops. This can be run as an add-on section to gather developer and product/UI/UX people to work on prototypes.
9.30-10.00 - Intro/API workshop
10.00-13.00 - Hackathon
13.00-14.00 - Lunch
14.00-17.00 - Hackathon
17.00-18.00 - Pitch/Judge/Awards
This can be an add-on API specific hackathon day

DISCLAIMER: This material is to be considered property of the author(s) of the proposal Marco Morana and Neill Gernon and the information should be confidential information and cannot be released to general public or used by any organization or commercial entity without permissions of the authors