THOUGHTS

on OWASP

Based on blog posts by

Dinis Cruz

beta version

Thoughts on OWASP

Dinis Cruz

This book is for sale at http://leanpub.com/Thoughts_OWASP

This version was published on 2014-04-07

Contents

Introduction

This book contains the blog posts written by Dinis Cruz on OWASP (and other philosophical ideas)

This section has the following chapters:

- Change Log[1]
- Why This book[2]

Table of Contents[3]

[1] /manuscript/0.Introduction/Change_Log.md
[2] /manuscript/0.Introduction/Why_This_book.md
[3] ../../Table_of_Contents.md

Change log:

Here are the changes made (per version):

v0.12 (07 April)

- Renamed all files (using FluentSharp script) so that they all have Underscores instead of spaces (making them easier to link in GitHub)
- Updated main README.md file. Added Table_of_Contents.md file for GitHub
- Added links to Table_of_Contents and all chapter README files

v0.11 (30 March)

- created GitHub repo https://leanpub.com/Thoughts_OWASP (and added all previous DropBox content to that repo)
- renamed ALL posts (to make it easier to read what they are about); set their extension to .md (for Markdown) and moved them into 'Chapter specific' folder (which works when there are no images)
- created the following chapters: "OWASP Organization" ,"OWASP Projects" ,"OWASP Summits" ,"OWASP Education" ,"OWASP MIA" ,"Philosophy", "Application Security Industry"

v0.10 (23 March)

- First release of book with raw import from blogger posts (no formatting or editing done)
- added cover to eBook version

Table of Contents[4]

[4] ../../Table_of_Contents.md

Why This book

I put this book together because I wanted to capture the evolution of my 'Thinking on OWASP'. Although I don't think that all my thoughts/ideas are correct or any good, I do feel that some are OK and deserve to be preserved and shared.

I also think that it is important for the new generations of OWASP Leaders to understand the past and to learn from what has happened before. Specially important is to learn from others mistakes (like mine).

Also captured in this book are a number of mine 'soul searching' and 'philosophy' based posts. I hope you like them :)

GitHub Repository

The content (and version control) of this book is managed using Git. The GitHub repository is the https://github.com/DinisCruz/Book_Thoughts_OWASP and you are free to fork it and use the content as you please

The selection criteria

The initial import from my blog was made of 76 blog posts which resulted in an book with 256 pages and 54,277 words. Part of that list where a number of posts that covered a wide range of OWASP topics (which is why I used the OWASP tag them on them), but since this is more of a 'ideas' book, I used the following criteria to trim the content (also note that most of this posts will exist on other books).

Here are the posts removed:

posts about specific OWASP projects

- "Another step in the use of ESAPI and AppSensor Jars from .Net/C# (using Jni4Net) "
- "Loading OWASP ESAPI jar and its dependencies from C# (using jni4net)"
- "Creating a clone of WebGoat on GitHub"
- "Help out with WebGoat .NET development"
- "Is this a safe way to do a .NET Server Redirects? (and deal with A10: Unvalidated Redirects and Forwards)"
- "O2 Script to create Google Static map with OWASP UK Chapter locations"
- "OWASP AppSensor and O2 Platform at Security B-Sides London"
- "Should Mass Assignment be an OWASP Top 10 Vulnerability?"
- "Stats used to support OWASP Top 10 entries (next version must publish them)"
- "Trying Google Groups as the OWASP O2 Platform mailing list"
- "WebGoat.NET in Action (and how I set-it up)"

posts about specific OWASP Events (most of which are now not relevant)

- "Call For Training - OWASP 2013 LATAM Tour"

- “OWASP Connector January 22, 2013”
- “OWASP Connector January 8, 2013”
- “OWASP is Hiring a FT Event Manager (35k USD)”
- “OWASP Royal Holloway Next Chapter Meeting - Thurs 10 May :30-9pm”
- “Presenting at OWASP Turkey Chapter on Sat 10th of November (on Secure Continuous Delivery)”
- “The Projects Summit 2013 is happening: GET INVOLVED!!!!”

misc topics

- “Great animation that shows how BootStrapToday works”
- “OWASP Press and using LeanPub with GitHub and DropBox”
- “SI Open Sources the Eclipse Plugin-development toolkit that I developed for TeamMentor”
- “SRE and Package HtmlAgilityPack Sanitizer as a stand alone module (at OWASP .Net)”
- “Submitting a request to the OWASP Platform”
- “To read: ENISA on ‘National Cyber Security Strategies’”
- “The Power of UnitTests when refactoring code (for example Security Pages)”
- “Using 99Designs for Design services”
- “What do the Twitter backups downloadable files look like”
- “Contract work to help with OWASP Wiki edits”

Table of Contents[5]

[5] ../../Table_of_Contents.md

1 OWASP Organization

This section has the following chapters:

- An Idea of a New Model for owasp[1]
- I wish that OWASP in 2014[2]
- Improved Wikipedia funding page why OWASP needs something similar and who buys OWASP Corporate Memberships[3]
- OWASP Board Election - Why I voted 'Abstain' and why you should go on the record with your vote[4]
- OWASP Executive Director Role (Not yet)[5]
- OWASP Principles based on NHS[6]
- OWASP Revenue Splits and the 'Non-profits have a charter to be innovators'[7]
- Proposed change for SoC - Use budget to pay for project related expenses[8]
- Remove all commercial non-OWASP logos from OWASP.org[9]
- Sarah Baso as OWASP Executive director, how it broke the model, structure and culture of OWASP employees[10]
- Why OWASP can't pay OWASP Leaders[11]
- Why the need to enable the use of OWASP chapter funds[12]
- Why NDAs have no place at OWASP[13]
- Me and Jim Manico[14]
- On John Wilander[15]

Table of Contents[16]

[1] /manuscript/1.OWASP_Organization/An_Idea_of_a_New_Model_for_owasp.md

[2] /manuscript/1.OWASP_Organization/I_wish_that_OWASP_in_2014.md

[3] /manuscript/1.OWASP_Organization/Improved_Wikipedia_funding_page_why_OWASP_needs_something_similar_and_who_buys_OWASP_Corporate_Memberships.md

[4] /manuscript/1.OWASP_Organization/OWASP_Board_Election_-__Why_I_voted_'Abstain'_and_why_you_should_go_on_the_record_with_your_vote.md

[5] /manuscript/1.OWASP_Organization/OWASP_Executive_Director_Role_(Not_yet).md

[6] /manuscript/1.OWASP_Organization/OWASP_Principles_based_on_NHS.md

[7] /manuscript/1.OWASP_Organization/OWASP_Revenue_Splits_and_the_'Non-profits_have_a_charter_to_be_innovators'.md

[8] /manuscript/1.OWASP_Organization/Proposed_change_for_SoC_-_Use_budget_to_pay_for_project_related_expenses.md

[9] /manuscript/1.OWASP_Organization/Remove_all_commercial_non-OWASP_logos_from_OWASP.org.md

[10] /manuscript/1.OWASP_Organization/Sarah_Baso_as_OWASP_Executive_director,_how_it_broke_the_model,_structure_and_culture_of_OWASP_employees.md

[11] /manuscript/1.OWASP_Organization/Why_OWASP_can't_pay_OWASP_Leaders.md

[12] /manuscript/1.OWASP_Organization/Why_the_need_to_enable_the_use_of_OWASP_chapter_funds.md

[13] /manuscript/1.OWASP_Organization/Why_NDAs_have_no_place_at_OWASP.md

[14] /manuscript/1.OWASP_Organization/Me_and_Jim_Manico.md

[15] /manuscript/1.OWASP_Organization/On_John_Wilander.md

[16] ../../Table_of_Contents.md

1.1 An Idea of a new model for OWASP

Here is a post/idea that has been 18 months in the making (in fact since I stepped down as OWASP board member on 12th Feb 2011[17])

I wrote the text below in response to Jim Manico owasp-leaders list "What is OWASP?" thread[18], and am quite happy with the OWASP model that I finally was able to document.

Well Jim, I think the problem is in the currently structure of OWASP, where even when there is no malice or vendor-bias by an OWASP leader, the end result comes out that way (and can be interpreted in the way you have recently).

The key problem is that the current 'Board, Committees and Project/Chapter leadership model', was created for another era when OWASP was much smaller , with a very different set of problems and with a much smaller WebAppSec industry. Unfortunately, I don't see a solution for the problem you describe (and others that OWASP has) until that structure is changed.

For a while there was the *'...is OWASP run by Aspect Security?'* now is the *'...is OWASP run by Trustwave?'* maybe next is the *'... is OWASP run by WhiteHat?'* . Until the Board and Committees stop being seen as positions of Power + Kudos + Reputation + Carrer Advancement + 'PressReleases created on appointment', this will not be resolved. For example, it is very damaging that OWASP leaders think that they need to be Board/Committee members to get things done. This is not only false, but it creates a power-vacum where other OWASP leaders think that _'something is being done' _or that _'its the other dude responsibility to do that!'. _

The reason why I left the Board 18 months ago was because I realised that the model that we had created for OWASP (which worked so well until then) was expiring and a new model was needed.

Jim description of *'OWASP is a non-profit community-service based organization'* is absolutely spot-on, and OWASP needs (in my opinion) a Board and 'Committees' (or what ever name they are rebranded as) that are focused on that simple but powerful word: **Community **(we will need some creativity on what body/group should have the operational parts of the current Committees that are currently working very well)

I think the time has come to handle most of the OWASP 'Power and Responsibilities' to the OWASP employees who know OWASP more than any of us. Maybe we have a system where operational questions (like budgets, salaries, structures, etc...) are voted by majority.

We really need to re-focus OWASP Leaders energy in getting things done and re-invent OWASP in a lean, open, collaborative and effective community (and organization).

OWASP will still need a Board (or whatever name that is rebranded as). But that Board should be 99% focused on Community issues (i.e. how to empower OWASP Leaders to be productive, creative, empowered, happy). And for the_ 'but OWASP legally needs a board' _crowd, the other 1% would be to accept the decisions taken by OWASP's leadership community and employees.

[17] https://lists.owasp.org/pipermail/owasp-leaders/2011-February/004664.html
[18] https://lists.owasp.org/pipermail/owasp-leaders/2012-October/007895.html

We probably will need to hire more employees to really make this work, and as per the model I'm proposing here, that decision should not be made by the 'Board or Committees'. That decision should be made by the current employees :)

The good news is that OWASP is in an strong financial position to make this work, the not so good news is that I don't think this will happen any time soon. And the hard decisions that only a 'truly independent voice' (i.e. the employees) would be able to make, will have to wait a couple more months/years.

I don't know the author or the source, but one of the best quotes I've heard is *"....sometimes the best way to find the solution for a problem is to redefine the problem..."* :)

Meanwhile ... OWASP is still an amazing organization, doing amazing stuff and making a difference in the WebAppSec world.

I just want us to REALLY make a difference. Using the mountain analogy in the Trillions video[19] , I want us to be climbing the BIG mountain (not the smaller one we have been climbing over the last 10 years)

I don't want to look back when I'm old to OWASP and say: _'we did well, but we missed our window of opportunity to change the world' _

I want to look back and say: *"We did out best, and changed the world"*

[19] http://vimeo.com/7395079

1.2 I wish that OWASP in 2014 ....

In 2014, it would be amazing if OWASP has:

- an environment where:
  - developers collaborate with security professionals
  - 'Secure coding questions' can be asked and answered
  - browser and framework vendors/creators come together to work on the hard problem of 'web security'
  - governments, companies and 'web players', come together to define (and present) action-plans, standards and deliverables
  - the latest research is presented and the new generation of security-focused developers/researchers can find home(s) to develop, nurture and present their ideas
- OWASP projects (tools, documents, services) that:
  - have so much quality that they are '*best in class*' and raise the bar for the whole industry
  - are funded because: a) they add really value, and b) users want/need the next versions/features/bug-fixes (see OWASP Project Partnership Model[20])
  - generate enough revenue that allows full-time staff (devs, qa, documentation, etc...) to be paid at fair market value (for their skills). With a cavet that OWASP cannot pay its leaders[21]
  - are easily consumed by other tools (the project's materials and capabilities)
  - add so much value to companies, that they become OWASP Paid Corporate members, not because it is the '*right thing to do*' but because they get so much value from it that they don't want the '*OWASP train*' to slow down
  - have a lot of resources available to them (with real/tangent benefits for being an 'OWASP project')
  - are given a 'fair change' to succeed and mature (with 'non performing/accepted' projects quickly removed), taking into account that a lot of projects are just an (healthy) way to create 'OWASP Leaders'
  - can be consumed from the developer's IDEs and integrated into the multiple SDL phases/activities
  - can be consumed from 'cloud services'
- multiple ecosystems[22] targeted to specific languages, frameworks and communities
- OWASP chapters that deliver regular training sessions and 'hands-on' workshops to its community
- universities that teach OWASP materials (and that share them for others to use)
- colleges/schools that use OWASP materials to create a new generation of developers and security professionals that have passion, love to hack and respect the art of 'creating secure code'
- OWASP conferences that bring together the OWASP leaders (in a very non-cost-effective way) so that those leaders can work together, present their ideas and meet its users
- OWASP conferences/chapters that do presentations under a TED-like format (15m max), with its videos reaching wide audiences
- OWASP conferences/chapters that publish: books of its presentations, academic papers, panel's conclusions/recommenda plans
- co-organised events at non-OWASP conferences (specially on developer-focused large conferences)

[20] https://docs.google.com/document/d/1ea4jWVDziLcZMTJUC5qW5psWYROpB-oPlqyl4Ei2xHA/edit?hl=en_US&authkey=CKycuTY&pli=1
[21] http://diniscruz.blogspot.com/2012/04/why-owasp-cant-pay-owasp-leaders.html
[22] https://www.owasp.org/index.php/Security_Ecosystem_Project

- lots and lots and lots of OWASP booths at non-OWASP events (in fact every 'mid size' OWASP chapter should do it at local conferences/events)
- a '*owasp leader hospitality program*' that looks after OWASP leaders when they travel (to OWASP events)
- very small (if any) instances of *'OWASP leaders burned out*' cases (this usually happens to conference's organisers)
- strong demands on its project leaders/contributors to present regularly at OWASP conferences and chapters
- an 'project reviewers/users' community that works with OWASP projects in reviewing, mentoring and using those projects
- a 'serendipity' social graph engine that connects OWASP leaders/contributors with each other (when they are traveling around the world)
- multiple mobile apps that make OWASP 'goodness' easy to find and consume
- very few barriers of entry for new ideas to occur (and projects and chapters to be created)
- low tolerance for non performing activities, projects, chapters or 'leaders' (i.e. when something is not working, remove/clean/break it very quickly it)
- an army of editors for the OWASP Wiki, with very high rigour and quality-requirements for its content
- a much bigger OpsTeam (OWASP Operational Team) that makes this all possible, empowers OWASP's leaders and makes the hard decisions required to keep OWASP's community working
- a much more transparent and open OpsTeam where 99% of emails and other OWASP related activities are published and easily consumed (think email boxes published with read-only/viewing privileges)
- a model where OWASP leaders are empowered to make financial decisions/commitments and spend the available OWASP funds in the way they believe is best, with no (very little) questions asked and very fast approval cycles (see the GSD project[23] for details)
- a reputation-based trust model where OWASP leaders/contributors are highly respected (and valued) by its peers, employees and industry (think StackOverflow points/badges solution)
- a high standard for '*what is an OWASP leader*' based on respect, talent, energy and deliverables
- a model where it doesn't matter what title an OWASP leader has, but what has he/she created or delivered
- a number of certifications based on the model described in the OWASP Red Book[24] , and wide adoption of the other books: Green, Blue, Yellow, Purple and Gray
- lots and lots and lots of writing on OWASP's and WebAppSec ideas, topics, strategies, etc... (both in agreement and disagrement on what is happening). The resulting arguments (both pro and con) should then be consolidated in easy to consume and distributed packages
- large number of isolated 'owasp houses' where it is possible to go and spend dedicated time just coding, learning, collaborating, debating, fixing apps, breaking apps, writing SAST/DAST rules, etc...
- Invested in Developing Software Security Talent[25] under Mark's or similar programs
- The OWASP CheatSheets[26] are available in a number of formats (book, tablets, mobile, IDEs)
- helped to create a set of common schemas and rules for the multiple SAST, DAST and 'everything in between' tools

[23] https://www.owasp.org/index.php/GSD
[24] https://www.owasp.org/index.php/OWASP_Codes_of_Conduct
[25] http://www.curphey.com/blog/2012/10/19/investing-in-software-security-talent/
[26] https://www.owasp.org/index.php/Category:Cheatsheets

- a website that is easily consumed and its content forked (with the content available as git repositories)
- a collaborative/thread discussion environment (think StackOverflow or Reddit vs the current mailman solution)
- a proper OWASP books collection and distribution on major bookstores/eStores (as per the original vision and design)
- a place at the table on the most important web application security related discussions/threads
- multiple summits where everything comes together and everybody is working 100% of the areas they are passioned about, collaborating with other like minded individuals and creating magic
- regular 'OWASP Tours' where multi-city/country events allow ideas/projects to be presented, debated and improved
- an active role in the evolution of the new generation of fast-deployment-SDLs (in public or private clouds) with security baked into the 'deploy' workflow
- a number of standards that allow the pragmatic evaluation of security services (by commercial vendors) so that the best ones are rewarded for their excellence
- a standard for the first generation of Software/Application Security Labels[27] that would allow consumers to make informed decisions
- helped and accelerated the change of focus/investment on 'Network Security' into 'Application Security'. Note: this would expand the current AppSec market by 10x (and OWASP by 10x)
- helped to bridge the gap between the application security industry and the software-development industry, where they realize that the tools (and services) currently provided in the AppSec world can add a LOT of value (after a couple tweaks). Note: this would expand the current AppSec market (and OWASP) by another 10x

The best part is that this is all doable because OWASP already has enough funds, community, brand and people to kickstart this.

The question is if the focus/energy is there....

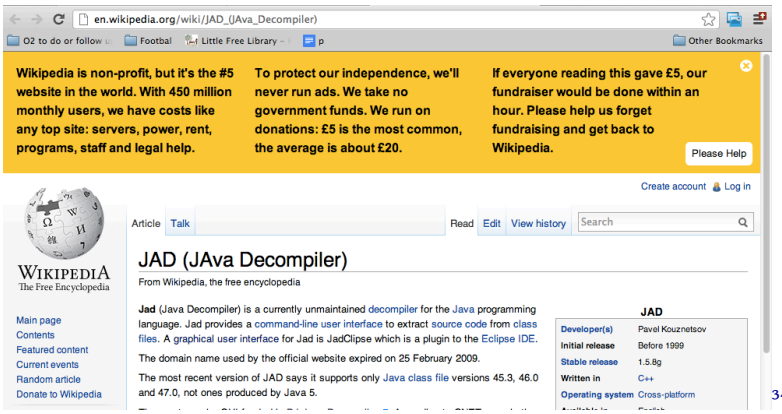
UPDATE: Related posts written after this one (see also the posts tagged with the OWASP label[28])

- Jan 2013: OWASP Principles based on NHS?[29]
- Jan 2013: On how to get paid to work on OWASP projects [30]
- Dec 2012: OWASP Revenue Splits and the "Non-profits have a charter to be innovators"[31]
- Nov 2011: Improved Wikipedia funding page, why OWASP needs something similar, and who buys OWASP Corporate Memberships[32]
- Nov 2011: The difference between being 'Appointed' and being 'Accepted' as an OWASP Leader (of its Fork) [33]

[27] https://www.owasp.org/images/1/17/2010-11_OWASP_Software_Labels.pptx
[28] http://blog.diniscruz.com/search/label/OWASP
[29] http://blog.diniscruz.com/2013/01/owasp-principles-based-on-nhs.html
[30] http://blog.diniscruz.com/2013/01/on-how-to-get-paid-to-work-on-owasp.html
[31] http://blog.diniscruz.com/2012/12/owasp-revenue-splits-and-non-profits.html
[32] http://blog.diniscruz.com/2012/11/improved-wikipedia-funding-page-why.html
[33] http://blog.diniscruz.com/2012/11/the-difference-between-being-appointed.html

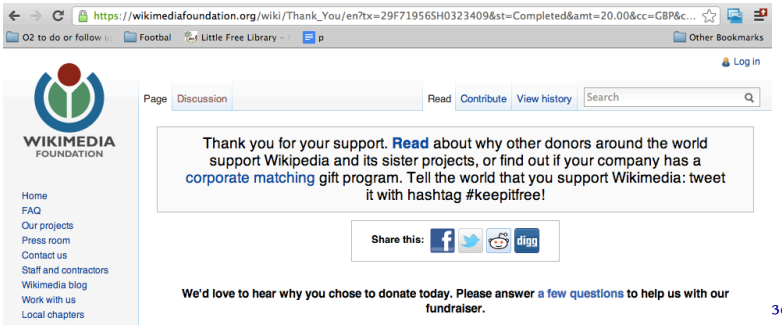
1.3 Improved Wikipedia funding page, why OWASP needs something similar, and who buys OWASP Corporate Memberships

Just went to Wikipedia and saw this:



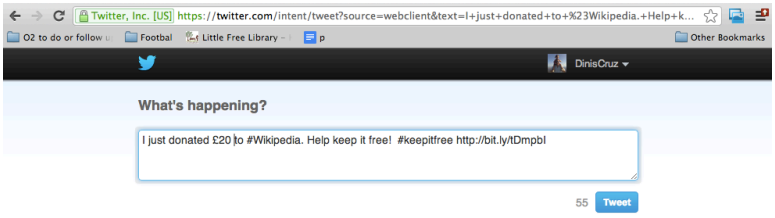
[34]

which just sounded fair (and much better that looking at Jimmy's eyes[35] :)), so I clicked on the **Please Help **Button and used Paypal to help with £20:



[36]

and since it was so easy to retweet, I also did that too :)



[37]

I think it is very important for Wikipedia to have a funding model[38] that keeps it ad free[39] and comes directly

[34] http://4.bp.blogspot.com/-0SfJKHi8gP4/UKYd4rx9CrI/AAAAAAAACD8/aqp3dgzNJ2U/s1600/Screen+Shot+2012-11-16+at+11.03.57.png
[35] http://readwrite.com/2010/11/19/wikipedia_has_raised_in_a_week_what_took_a_month_i
[36] http://2.bp.blogspot.com/-bmqbyV2b5zI/UKYhgnUCbhI/AAAAAAAACFE/ez5CYznEbDs/s1600/Screen+Shot+2012-11-16+at+11.05.52.png
[37] http://3.bp.blogspot.com/-uEVFXTsRlU4/UKYhhyvMcEI/AAAAAAAACFM/gIXv0jQQqmI/s1600/Screen+Shot+2012-11-16+at+11.06.14.png
[38] http://www.economist.com/node/21536580
[39] http://readwrite.com/2011/01/01/wikipedia_raises_16_million_to_remain_ad-free

from it's users (which means that the '*Wikipedia Users*' are the '*Wikipedia Customers*' instead of being the '*Wikipedia Product*' (which btw, is what users are for Google, Facebook, Twitter, etc..)).

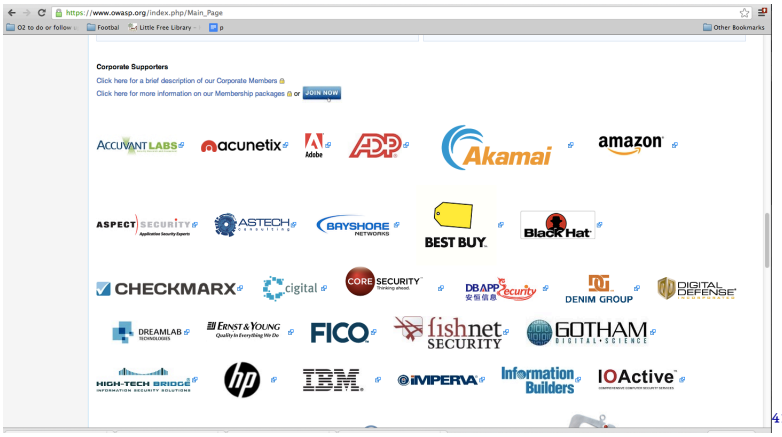
In fact that is why it was such an easy decision for me to 'help' (which is a better word than 'donate') since I value Wikipedia's services (provided by its operational machine) and I want to be Wikipedia's *Customer* not its *Product*

Now OWASP really needs to figure out a similar model, since the current membership model works OKish but creates massive conflicts of interrest.

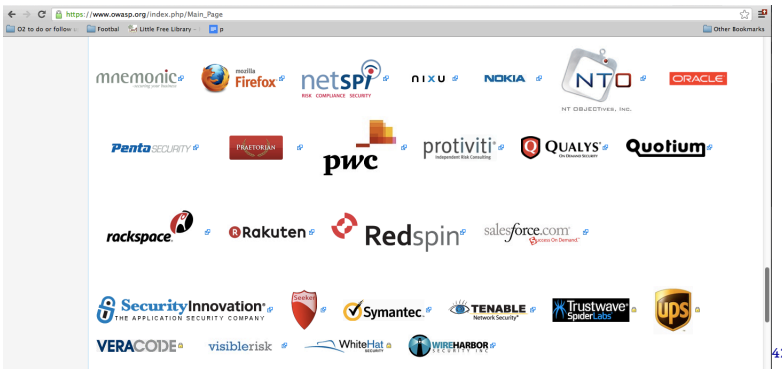
Ideally OWASP should be funded by its users, not by the companies that provides services to its users.

Of course that there are some exceptions (like Mozilla) but if you look at the shopping list of logos that is the membership page[40] that is a massive security product/vendor collection.

And btw, I think the time as come to remove the OWASP Membership logos from the HomePage, its getting ridiculous:

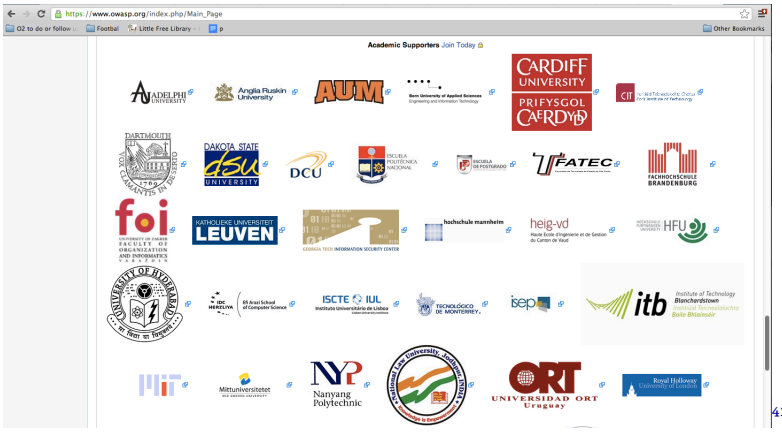


[41]



[42]

[40] https://www.owasp.org/index.php/Membership
[41] http://2.bp.blogspot.com/-2gM__l5RQaA/UKYjGKKgYRI/AAAAAAAACFU/5bM2LYPohyI/s1600/Screen+Shot+2012-11-16+at+11.26.38.png
[42] http://2.bp.blogspot.com/-NSAITD6-qXw/UKYjjTEl_AI/AAAAAAAACFc/eap-Quafns4/s1600/Screen+Shot+2012-11-16+at+11.28.22.png



[43]

Are we really THAT independent and vendor neutral?

Here is an interesting question (since OWASP generates revenue and is profitable):** WHO and WHAT are OWASP's product? I.e. what is OWASP really selling? **

As an OWASP **Leader**, am I the product? or the customer?
As an OWASP **User**, am I the product? or the customer?
As an OWASP **Corporate Member**, am I the product? or the customer?
As an OWASP **AppSec Conference or Chapter speaker**, am I the product? or the customer?
As an OWASP **AppSec Conference or Chapter attendee**, am I the product? or the customer?

This actually takes me to another really interesting question which is '**What is the drive behind an OWASP Corporate Memberships' **(the 5k USD one[44])?

My theory is that in most cases (90%+) **these memberships are directly connected to an OWASP leader** (I don't think this analysis has been done, but from all the OWASP leaders I know, this fells right). Important questions to answer are:

- *"what is the time-delta between 'somebody' becoming an OWASP leader, and the company he/she is working for, becoming an OWASP Corporate member?"*
- *"how many __OWASP Corporate members exists that have NO OWASP leader(s) in its payroll?'*
- *"how many lapsed (or not renewed) OWASP Corporate Memberships happened from companies whose past (in payroll) OWASP Leader(s) are not 'active at OWASP' any more?"*
- *"how many __OWASP Corporate members exists from companies that provide NO security services or products"*
- **"how many __OWASP Corporate members exists from 'development organisations' (i.e. companies or groups focused on writing secure code)" (for example it doesn't look like Etsy is a member[45])**

What is important about this idea, is that **IF OWASP memberships are a direct or 'natural' consequence/evolution of an OWASP Leader existence**, that would mean that OWASP's lack of focus on its leaders, is not only '*the wrong thing to do*' but a very bad business decision.

[43] http://2.bp.blogspot.com/-swb7da0Vrv0/UKYjlVBiZLI/AAAAAAAACFk/Tr-b5jOrhaE/s1600/Screen+Shot+2012-11-16+at+11.28.32.png
[44] https://www.owasp.org/index.php/Corporate_Member
[45] http://diniscruz.blogspot.co.uk/2012/10/open-question-to-etsy-security-team-how.html

One of the things I tried most when I was a board member was to get OWASP to take more care about its leaders, and it was always an up-hill battle because there is this view that '*hey the leaders contribute because they want*' (I remember having to argue hard for the concepts of *'OWASP Leaders are given free OWASP Memberships'* _*and*_ *'OWASP Leaders can go for free to any OWASP conference'*).

It is critical for OWASP's future to look after its leaders much better than it currently does, and if you look at my list on I wish that OWASP in 2014 ....[46] you will see that most are *'OWASP leaders focused'*.

Focusing on OWASP Leaders is a win-win situation[47] and what makes sense from a commercial point of view!

The more OWASP invests and looks after its leaders, the:

- better projects OWASP will have
- better presenters OWASP will have
- more Corporate memberships will exist
- more value OWASP will be providing to its key target audiences: developers/companies who want to write/buy/use secure code

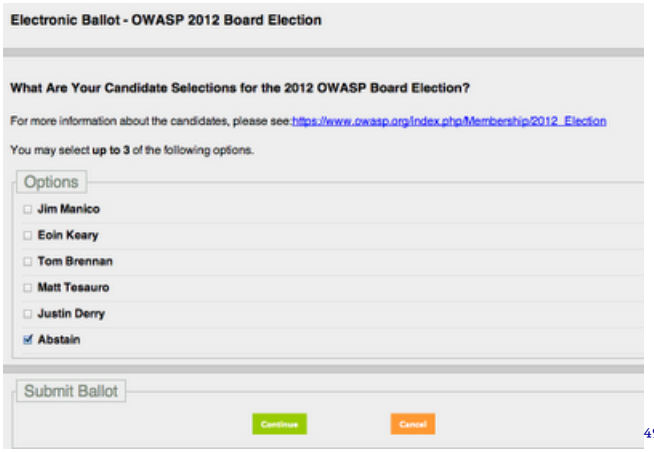
[46] http://diniscruz.blogspot.co.uk/2012/11/i-wish-that-owasp-in-2014.html
[47] http://en.wiktionary.org/wiki/win-win

1.4 OWASP Board Election: Why I voted 'Abstain' and why you should go on the record with your vote

(as sent to the owasp-leaders list)

I actually wanted to write a long email about his, but since I'm running out of time, here is the short version:

I just voted **Abstain** on the Board Election because I think that OWASP needs a new structure[48] and the sooner we replace the current Board, Committees, etc.. with something that works, the better.



[49]

When I stepped-down from the Board 18 months ago, I did ask the other Board Members to also step-down, since my idea was that if there was no Board, we would be faced with the 'nice problem' to come up with a new model. Jeff was the only one that did it (I'm not taking the credit for it since he had his reasons), but the others stayed there and have since been re-elected or are part of the current election.

I had a big list of items that I wanted to raise (with more details on what is not working, areas that need to be addressed and ideas for the future), but I guess the two ones recurring themes are:

- **Are we (OWASP) really doing our best with what we have?** (just think of the brain power that exists at OWASP)
- **Where is the dialog, debate, argument, passion about OWASP and AppSec?** (for example, on this election, the only thing that we had were some podcast interviews (or the transcripts created via the GSD project), which I read, and …. I'm actually not going to comment since I want this to be a positive email)

Another reason to vote **Abstain **is *to go on the record that I don't agree with the current model* and that (maybe) if enough OWASP leaders also vote **Abstain **, the required changes will happen faster :)

Now, **if you are going to vote, I also think that you should go on the record **about which candidates you voted for ** **(by email or wiki or your blog) .

This 'public vote of support' will create a two-way relationship between you (the voter) and the elected board member. It will be more transparent/open and will allow for accountability (which is another thing missing)

[48] http://diniscruz.blogspot.com/2012/10/an-idea-of-new-model-for-owasp.html
[49] http://1.bp.blogspot.com/-rjbXvcSYOSw/UHzGErNHkXI/AAAAAAAAATk/9hQIthLLuRY/s1600/Screen+Shot+2012-10-16+at+02.41.17.png

Note that I'm not saying that the current Board Members (and candidates) don't work hard for OWASP and help a lot. They do , just like a lot of other owasp-leaders. It's just that the current model is broken and if we really want OWASP to go to the next level and make a 'dent in the WebAppSec Universe' we need a new model.

Unless of course you think that all is great with OWASP, that we are doing the best that is possible with our human, financial and technological resources, and that no major change is need. I don't happen to share that view :)

Finally, over the past months I've been thinking and blogging about OWASP, and since I know that some of you have 'owasp-leaders email overload', I didn't post all of them here.

Here is a collection of some of my thinking and ideas:

- An Idea of a new model for OWASP[50]
- Some ideas for OWASP GSD Project[51]
- OWASP GSD Project (GSD = Get Stuff Done)[52]
- ROI on OWASP investment on Projects (ie paying leaders)[53]
- Why OWASP can't pay OWASP Leaders[54]
- Project Management at OWASP[55]
- Why large OWASP projects start to stale (and who should pay for the work)[56]
- Secure coding (and Application Security) must be invisible to developers[57]
- Great description of why OWASP Summits are special[58]
- Some proposed Visions for next OWASP Summit[59]
- Summits must be part of OWASP's DNA[60]
- I want to vote for a Summit Team+Vision , NOT for a venue[61]

I also tagged a number of posts with OWASP MIA, which where the cases where I was thinking "*humm.... shouldn't OWASP be involved in here?*"

- 'Using the HTML5 Fullscreen API for Phishing Attacks', OWASP MIA and 'We need SAST technology for browsing the web safely'[62]
- Great animation that shows how BootStrapToday works[63]

[50] http://diniscruz.blogspot.com/2012/10/an-idea-of-new-model-for-owasp.html
[51] http://diniscruz.blogspot.com/2012/05/some-ideas-for-owasp-gsd-project.html
[52] http://diniscruz.blogspot.com/2012/05/owasp-gsd-project-gsd-get-stuff-done.html
[53] http://diniscruz.blogspot.co.uk/2012/04/roi-on-owasp-investment-on-projects-ie.html
[54] http://diniscruz.blogspot.co.uk/2012/04/why-owasp-cant-pay-owasp-leaders.html
[55] http://diniscruz.blogspot.co.uk/2012/04/project-management-at-owasp.html
[56] http://diniscruz.blogspot.co.uk/2012/04/why-large-owasp-projects-start-to-stale.html
[57] http://diniscruz.blogspot.co.uk/2012/04/secure-coding-and-application-security.html
[58] http://diniscruz.blogspot.co.uk/2012/04/great-description-of-why-owasp-summits.html
[59] http://diniscruz.blogspot.co.uk/2012/04/some-proposed-visions-for-next-owasp.html
[60] http://diniscruz.blogspot.co.uk/2012/04/summits-must-be-part-of-owasps-dna.html
[61] http://diniscruz.blogspot.co.uk/2012/04/i-want-to-vote-for-summit-teamvision.html
[62] http://diniscruz.blogspot.co.uk/2012/10/using-html5-fullscreen-api-for-phishing.html
[63] http://diniscruz.blogspot.co.uk/2012/10/great-animation-that-shows-how.html

- Big Security challenges with creating APIs for US Gov agencies[64]
- To read: ENISA on 'National Cyber Security Strategies'[65]
- Hack Yourself First: Jeremiah at TEDxMaui[66]
- Trustworthy Internet Movement and SSL Pulse[67]
- Blogger in HTTP only? What happened to HTTPS?[68]

Enjoy AppSec USA (which is the first OWASP AppSec USA that I'm going to miss since they started), and please feel free to disagree with this email (and create some debate)).

[64] http://diniscruz.blogspot.co.uk/2012/06/big-security-challenges-with-creating.html
[65] http://diniscruz.blogspot.co.uk/2012/05/to-read-enisa-on-national-cyber.html
[66] http://diniscruz.blogspot.co.uk/2012/04/hack-yourself-first-jeremiah-at.html
[67] http://diniscruz.blogspot.co.uk/2012/04/trustworthy-internet-movement-and-ssl.html
[68] http://diniscruz.blogspot.co.uk/2012/04/blogger-in-http-only-what-happened-to.html

1.5 OWASP Executive Director Role (Not yet)

Following the announcement sent today to the owasp-leaders list[69] *(see below), I replied with my view that OWASP doesn't need this role today:*

I think it is great that a decision to add another resource to OWASP super OpsTeam (the employees) was made, but as I said many times before[70] **I don't think that OWASP needs a CEO/ Executive-Director today**.

For the record, I DO think that one day OWASP will need such position, but not today. At the moment, my view is that we should be adding resources to help our Projects or in managing the owasp.org[71] website content.

What we need are another Kate, Sarah, Kelly or Samantha, they still work FAR too much for OWASP and my worry is that they will implode one day. **Not sure that they need a boss to tell them what to do, if anything **I would delegate to them the powers currently 'assigned' to the Executive Director.

That said, assuming that this hire will go ahead, can we please have the whole process done in a transparent and open way? And by that I mean that ALL details about this job should be done via the OWASP wiki (including the 'salary package'). We should also ask all candidates to apply publicly and to be available to answer questions from the OWASP leaders and members.

Dinis Cruz

On 9 April 2013 00:04, Michael Coates <michael.coates@owasp.org[72]> wrote:

> Leaders,
>
> I'm excited to announce the creation of an executive director position at owasp. The motion was passed at today's board meeting.
>
> Here's the public post that went out today.
>
> http://owasp.blogspot.com/2013/04/owasp-creates-executive-director.html[73]
>
> ### OWASP Creates Executive Director Position
>
> OWASP is driven by volunteers and the contributions of thousands all over the world. Behind the scenes there is also a group of dedicated paid staff that focus on critical operations to ensure the OWASP engine keeps running strong. This team has grown organically over the years as OWASP has recognized the need for dedicated full time individuals to focus on specific task items. In each of these areas we've seen great successes from our staff.
>
> As OWASP continues to grow we must also ensure our structure and supporting operations team grows too. The next step in that growth is the creation of the OWASP Executive Director[74] role. The individual in this role will lead the focus and resourcing of our operations team to ensure we execute on our strategic goals each year. This individual will ultimately be responsible for

[69] http://lists.owasp.org/pipermail/owasp-leaders/2013-April/009188.html
[70] https://twitter.com/DinisCruz/statuses/126805325058818048
[71] http://owasp.org/
[72] mailto:michael.coates@owasp.org
[73] http://owasp.blogspot.com/2013/04/owasp-creates-executive-director.html
[74] https://docs.google.com/document/d/1z4Pl7C-jbgtuV2nR-MaW2Rs-6u3RnC4RKNGCmUcX-zo/edit?usp=sharing

leading the operations team to success and will report directly to the OWASP board. This role will maximize the value our operations team provides to our community, projects and the world.

This is an exciting step forward for OWASP and a demonstration of the continued growth of our community.

–
Michael Coates | OWASP | @_mwc

OWASP-Leaders mailing list
OWASP-Leaders@lists.owasp.org[75]
https://lists.owasp.org/mailman/listinfo/owasp-leaders[76]

[75] mailto:OWASP-Leaders@lists.owasp.org
[76] https://lists.owasp.org/mailman/listinfo/owasp-leaders

1.6 OWASP Principles based on NHS?

For a while now, my view is that OWASP's Mission, Focus and Vision should just be: ***"WEB APPLICATION SECURITY"***

That's it. OWASP's community and scope is so wide (a great thing) that trying to be even more specific will end up in a massive thread and unproductive discussion (where just about everybody will be a bit right about something)

In you look at the current text in the owasp[77] home page (which I helped to write) it says:

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

I don't really agree with this mission, since for example I think that OWASP should be "Making Security Invisible (by Becoming the Developer's Best Friends)"[78]. I.e. **Invisible** not **Visible** :)

Also, where is '_writing secure cod_e' on that mission :)

That said there is (some) value in documenting and talking about values and principles, so while writing the Private threads are SO inefficient, Application Security Knowledge is available at the point of Need, and Password Hashes over SSL[79] post, I had a look at the NHS core principles[80] and constitution[81], and I wonder if we can re-write them :)

Here are the seven key principles that guide the NHS, *'OWASP Style':*

- *The NHS _OWASP* provides a comprehensive service, available to all irrespective of gender, race, disability, age, sexual orientation, religion or belief_
- *Access to NHS _OWASP* services *(and knowledge)* is based on clinical *Web Application Security* need, not an individual's ability to pay_
- *The NHS __OWASP aspires to the highest standards of excellence and professionalism*
- **The NHS __OWASP_** services must reflect the needs and preferences of developers, security professionals and application consumers patients, their families and their carers_
- *_The NHS __OWASP _works across organisational boundaries and in partnership with other organisations in the interest of _application security* patients, local *development* communities and the wider population_
- *_The NHS __OWASP _is committed to providing best value for taxpayers' money _its funds* and the most effective, fair and sustainable use of finite resources_
- *_The NHS __OWASP _is accountable to the public, communities and patients _professionals* it serves_

This would of course mean that OWASP's OpsTeam (the current employees) take a much stronger role, and that the OWASP 'machine' is given the resources/authority to become the _strong services oriented _team that it wants to be.

[77] https://www.owasp.org/
[78] http://blog.diniscruz.com/2012/04/making-security-invisible-by-becoming.html
[79] http://blog.diniscruz.com/2013/01/private-threads-are-so-inefficient.html
[80] http://www.nhs.uk/NHSEngland/thenhs/about/Pages/nhscoreprinciples.aspx
[81] http://www.nhs.uk/choiceintheNHS/Rightsandpledges/NHSConstitution/Pages/Overview.aspx

A key challenge will be to do this without paying OWASP leaders (NHS does pay its doctors) which in my view shouldn't be done. See Why OWASP can't pay OWASP Leaders[82] and On how to get paid to work on OWASP projects[83]

Maybe I should add these principles to the list I wrote at I wish that OWASP in 2014 ...[84]

[82] http://blog.diniscruz.com/2012/04/why-owasp-cant-pay-owasp-leaders.html
[83] http://blog.diniscruz.com/2013/01/on-how-to-get-paid-to-work-on-owasp.html
[84] http://blog.diniscruz.com/2012/11/i-wish-that-owasp-in-2014.html

1.7 OWASP Revenue Splits and the "Non-profits have a charter to be innovators"

Seth Godin recent post on Non-profits have a charter to be innovators[85] is really spot-on, and very accurately describes the problem that (I believe) exits today at OWASP[86]

When Seth mentions that non-profits usually say: _'...We're doing important work. Our funders count on us to be reasonable and cautious and proven, because the work we're doing is too important to risk failure...', _ he could be speaking on behalf of a number of OWASP Leaders, since I have heard many variations of that phrase at OWASP before (in fact you will see such variation later on this post)

Contrary to what a lot of OWASP core leaders (the ones that care and spend time on *'OWASP the entity'*) believe, **OWASP doesn't have a lack of funds problem!**
**

****OWASP has a 'how to spend money' problem **

and a

'Not spending enough OWASP funds' problem!

**

**If you look at the current situation, you will find:

- OWASP Chapters with 150k+ funds available to them[87]
- OWASP Projects with 45+ allocated to them[88] (I was going to point to the actual budget spreadsheet, but couldn't find it)
- OWASP Committess with 115.5k allocated to them[89]
- OWASP GSD Project with 1,500 USD still available to OWASP Projects[90] (btw, this project has completely been ignored by the OWASP Leadership and community)

But, although there is enough money available, the amount spent from those budgets is very small (again I wanted to point to the real numbers, but couldn't find them)

**So does OWASP really needs fund raising? **

**

**

**Does it really need an improved Conference/Chapter revenue model as proposed by **New Profit Sharing Model Proposal[91] (which is where 'OWASP energy' is being spent)

[85] http://sethgodin.typepad.com/seths_blog/2012/11/non-profits-more-innovative.html
[86] https://www.owasp.org/
[87] https://docs.google.com/a/ddplus.net/spreadsheet/pub?hl=en_US&hl=en_US&key=0Atu4kyR3ljftdEdQWTczbUxoMUFnWmlTODZ2ZFZvaXc&output=html
[88] https://www.owasp.org/index.php/Projects_Reboot_2012
[89] https://docs.google.com/a/owasp.org/spreadsheet/ccc?key=0Atu4kyR3ljftdFBsRFVxSmpVVE5hN1g1bmYySjdMLXc#gid=0
[90] https://www.owasp.org/index.php/OWASP_GSD_Project
[91] http://lists.owasp.org/pipermail/owasp-leaders/2012-November/008227.html

Does it really need more rules and 'Project Stage Benefits' with special carrots for projects being given budgets? (see current Samantha's ideas on it here[92])

OWASP's problem is not that it doesn't have enough funds for its projects, chapters, committees, etc...

The problem is that the funds available are NOT being spend!

This means that the current focus should on **finding ways for the available funds to be spent**

**

**

Maybe one day OWASP will have the **great problem of having to regulate and control the spending of the available funds**.

But that is not the problem that exists today!

And as programmer, my view is that the way to takle a big problem, is to solve the ones that we have today, and then deal with other issues later.

To see if I could point OWASP on the right direction, on the New Profit Sharing Model Proposal[93] thread I asked[94]:

> _"...Is there a place where I can see/read the current objectives and rational behind the profit sharing? Basically: _
>
> - _why it is done? _
> - _what are the objectives that we are trying to achieve? _
> - _based on the past 12 months (and what happened with the use of those funds), have those objectives been meet? _
> - _what is working and what is not working? (with the current profit sharing model) - what is the % of the funds allocated that have been spent in the last 12 months? _
> - *where have those $$$ been used for? Also, can you point me to an analysis (or list) of all the expenses made by the chapters that received a $$$ share? (and their balances) ..."*

And Michael's response [95]is one I have heard many times before, and is exactly the kind of problem Seth Godin talks his Non-profits have a charter to be innovators[96] post:

_

_

"...The new policy is straightforward and also strikes a better balance between declaring foundation funding needs to keep the overall OWASP machine moving and also chapter desires to raise funds and foster chapter/regional growth. ..."

[92] https://docs.google.com/a/owasp.org/document/d/15lPNSxokO5ogGxWo-xvLNYh0C3c8-nWjgWnRfTfm0OU/edit
[93] http://lists.owasp.org/pipermail/owasp-leaders/2012-November/008227.html
[94] http://lists.owasp.org/pipermail/owasp-leaders/2012-November/008228.html
[95] http://lists.owasp.org/pipermail/owasp-leaders/2012-November/008244.html
[96] http://sethgodin.typepad.com/seths_blog/2012/11/non-profits-more-innovative.html

What is interesting about that thread and its responses, is that the key issue (which I was trying to get to, with my questions) is *"The current funding model for chapters and projects is not working! simply because the money is not being spent!"* (and btw, OWASP has enough funds coming in via its Memberships to keep the 'lights on')

**

**

So instead of '*refining*' the current OWASP revenue splitting model, my view is that it should be dramatically changed to a model similar to the GSD project[97].

For example, **here is how it could work**, where only the following rules would be in place:

1. OWASP chapters and projects get 100% of the funds they generate, and have 6 months to spend it
2. After 6 months that money goes to a global Projects and Chapters pot/bucket/account, which ALL chapters and Projects can access (and spend from)
3. No OWASP leader can be paid using these funds
4. There is an '*approval by default*' on spending requests (with maybe a *request for more details*' mode (see GSD project[98] for an example))

And that's it!

This would put the focus and the energy into spending the money, which is what OWASP should be doing.

Because, just like Seth says:

–

–

"...Go fail. And then fail again. Non-profit failure is too rare, which means that non-profit innovation is too rare as well. Innovators understand that their job is to fail, repeatedly, until they don't...."

–

–

And in OWASP's world, **this means**, **that if every Six months we don't have a list failures**, ie places where OWASP money was REALLYYYY badly spent, **it means that we are not trying hard enough** (or course that we will also have a list of good uses of OWASP money, but those tend to be ignored by the peanut gallery[99])

See, I know how to spend OWASP money, in fact I am by FAR the one that has spend more OWASP funds ($400K+ on Summits $250K+ on OWASP Seasons of Code, and others). And I can speak by personal experience, that it is very hard to spend OWASP money. I takes a LOT of energy, time, commitment and an ability to accept failure.

At the moment spending money is VERY hard at OWASP, because:

...the culture doesn't promote that spending

...the culture doesn't reward spending

[97] https://www.owasp.org/index.php/OWASP_GSD_Project
[98] https://www.owasp.org/index.php/OWASP_GSD_Project
[99] http://en.wikipedia.org/wiki/Peanut_gallery

….doesn't reward failure

….doesn't reward action

AND THAT's what need to be fixed!

But, the first hurdle, is accepting the real problem, and as you can see by the New Profit Sharing Model Proposal[100] thread, we are not there yet. Only after accepting the fact that **OWASP has a 'spending the money problem'**, will a real solution be found (I'm proposing one here, but I'm sure other solutions can be found that are better).

What really matters is if in 6 months time, a very high % of OWASP available funds has been spent.

And I hope it does, since we need to spend those funds if we are going to achieve some of the ideas I posted on my I wish that OWASP in 2014… [101] :)

Unfortunately, things/actions/ideas/projects/events _"that could happen but didn't" _is something that is very hard to quantify and to mesure. And if creative ways are not found to mesure them, then the status-quo is what is rewarded.

For example, **why hasn't Seth spoke at an OWASP conference? or Summit?**

Clearly Seth will add a lot of value to OWASP, but unless we (OWASP) explicitly go after Seth, he is not going to turn up. But what will happen in Six months time, where Seth still hasn't been at one of OWASP's events! Will that be seen as a failure, as a missed opportunity? or will that not even be on the radar?

At the last two Summits, there was an idea to bring guys like Seth to it, so that he could share his views and ideas, but at the time there was not enough energy and focus at OWASP to make that happen (we were still trying to make the 'Summit work' and spent (for example) a lot of time discussing the need to have a 'fixed schedule', instead of getting guys like Seth to be part of it).

Maybe for the next OWASP summit (see Some proposed Visions for next OWASP Summit[102]) that will happen :)

[100] http://lists.owasp.org/pipermail/owasp-leaders/2012-November/008227.html
[101] http://diniscruz.blogspot.com/2012/11/i-wish-that-owasp-in-2014.html
[102] http://diniscruz.blogspot.com/2012/04/some-proposed-visions-for-next-owasp.html

1.8 OWASP: Proposed change for SoC: Use budget to pay for project related expenses

Just posted this to the owasp-leaders list, and would also like to hear your opinion on it:

Hello OWASP leaders,

Since its creation at the OWASP Summit, the OWASP Global Projects Committee[103] has been meeting every week (see agenda of past meetings here[104]) to try to improve the organization and structure of OWASP Projects.

Our first major deliverable was the Assessment Criteria v2.0[105] which follows the footsteps of the previous version (now called Assessment Criteria V1) and aims to increase the visibility, usability and quality of the amazing projects you have created.

Our next challenge was to organize the 2009 OWASP grants scheme which (as with the Assessment Criteria) was thoroughly debated, discussed and modified, until we reached the format that is currently here: [http://www.owasp.org/index.php/OWASP_Season_of_Code*2009](http://www.owasp.org/index.php/OWASP_-Season_of_Code*2009) .

There are three main changes from the previous OWASP Season of Code:

Change #1) we are proposing that applications are targeted at the following 4 areas (each assigned to one or two committees)

- . **OWASP Education Pack** - (Education Committee[106])
- 2. **Enterprise usability of OWASP projects** - (Projects Committee[107])
- 3. **Additional Sources of Funding** - (Membership[108] & Chapters Committee[109])
- 4. **Marketing & PR** - (Industry[110] & Conferences Committee[111])

**Change #2) **we are encouraging proposals to be made by groups of OWASP contributors instead of Individuals (or specific projects). For example I really love the idea to create a number of "super OWASP teams" made up of a mix of 'with-proven-track-record' OWASP leaders/contributors and new 'full-of-energy-motivation-

and-sills' contributors

**Change #3) **to use the Season of Code 2009 budget to pay for 'Project related expenses' instead of 'Contributors/Leaders work"

This last change is quite radical, but one that I really believe is key for OWASP's future.

[103] http://www.owasp.org/index.php/Global_Projects_Committee
[104] http://www.owasp.org/index.php/Category:GPC_Meetings
[105] http://www.owasp.org/index.php/Assessment_Criteria_v2.0
[106] http://www.owasp.org/index.php/Global_Education_Committee
[107] http://www.owasp.org/index.php/Category:Global_Projects_Committee
[108] http://www.owasp.org/index.php/Global_Membership_Committee
[109] http://www.owasp.org/index.php/Global_Chapter_Committee
[110] http://www.owasp.org/index.php/Global_Industry_Committee
[111] http://www.owasp.org/index.php/Global_Conferences_Committee

And because this change is so important, the decision to do it is not final (hence why it is not on the SoC 2009 page), and I/We want to hear your opinion on this. So please chip-in with your comments, ideas and suggestions.

I'm quoting below two texts from internal GPC (Global Projects Committee) emails which provide additional background information on the rational behind this decision and the operational issues we need to address (these quotes also highlight the enormous value to OWASP that these Committees are creating, since in the past, these type of discussion and threads would have never existed (since apart from the OWASP Board there really was nobody else involved in these types of issues)). I would like to give special credit to Jason Li, for his hard work on this process and for taking the time to write a number of detailed emails (like the one below which I complely agree with)"

Looking forward to your comments,

Dinis Cruz (email continues below)

Jason Li on why the move to change # 3)
"...The direction ... to go with SoC funds is that they shouldn't be use to pay for technical work by our community members.

The hope is to get away from using money as the incentive for our community members to become more active and involved. Rather ... the funds ... used for things that the OWASP community could not otherwise produce - for example, physical books for promotion, graphic design costs for documentation, design work for templates, etc.

The SoC money would be allocated to the budgets for accepted projects and the budgets would be presumed for "operating costs" so to speak as opposed to "development costs".

It's a huge change in direction to be sure...."

_
"...I just wanted to clarify a little bit of the history of SoC. This is paraphrasing Dinis' oral history so he can correct me where I've gone wrong._

The SoC idea was intended as a way to get OWASP more recognition and also to attract new members to the OWASP community. Monetary grants were never intended to "pay for" or cover the cost of the actual work being done. Those grants were meant serve as a "reward" or sorts for participants (as you know, the grant amounts in the past certainly have not equated to the hours put in).

The hope was that OWASP would grow to the point that participating in SoC, and the positive recognition associated with leading an OWASP SoC project would be reward enough. Obviously this might be a little idealistic, and there have been discussions about how to properly "reward" SoC participants. Among the current proposals includes a guaranteed speaking slot at one of the major OWASP conferences (either US or European conferences) and prominent display in the to-be-redesigned OWASP Project website.

But SoC was never meant to pay OWASP community members for development work and a majority of the OWASP Board feels that the longer we continue to do so, the more we encourage that perception. The Board, and Dinis in particular, is extremely adamant that OWASP should not be on a path where OWASP project leaders expect to get paid for their contributions. It runs contrary to the open and volunteer philosophy of OWASP.

The 20k is still legitimate, but it needs to be clarified along with the rest of the page regarding this new direction for SoC funds. The 20k remark is trying to indicate the limits on a proposal. As a completely off

the wall example, say the OWASP NeverNeverLand and Wonderland chapters got together and said, "We're located very far from the US, where OWASP servers are hosted, and it's prohibitively slow for us to get access to OWASP materials. It would take us $12k to arrange an adequate mirroring solution to improve access to the OWASP website in our part of the world. We know that's a lot of money but together between our combined regions, there are hundreds of millions of developers that could use OWASP materials. Because of this, we feel like it's a good use of OWASP funds." Obviously this is a silly example, but that is type of proposal that we want to allow by indicating large proposals will get more leeway in terms of budget…

Paulo Coimbra on the operational issues created by Change #3 (most of them still need to be sorted out)

"…Committee,

Below, as for SoC 09, I am somewhat randomly pointing out a couple of questions that, from my point of view, are without clarification still.

1. Precisely what kind of expenses and/or investments will be and will not be paid? It seems to me we still need at the least a clear definition of the non paid rubrics.
2. What instrument will we use to clarify/define what type of expenses will be paid for each project? Will we ask for an initial estimate of expenses for the whole project? Assuming that we do – and that each applicant attaches the budget estimation to the project– can the jury decide that some expenses will be paid and others won't? If so, what will the criteria for this decision be?
3. Let's assume we ask for an initial estimate of expenses. Let's assume OWASP Testing Guide made an application and it was approved. Let's also assume the approved budget is something similar to the following:

- *Technical writing review - $ 2,500*
- *Book design/content layout – $ 1,500*
- *Publicity/Marketing/Public Relations – $ 2,000*
- *Total = $ 6,000*

_
3.1. Have we approved a sponsorship of $ 6,000 or have we approved the value of three distinct rubrics?_

3.2. What will happen if the project's leader ends up saying "I haven't spent the money approved for book design but I spent more than forecasted to be spent with marketing and so I would like to have a fund re-allocation"? Who will analyse and decide upon these situations?

3.3. Who will control the overall fund allocation? How?

3.4. Who will be paid? The project's leader or his supplier? When will the payment be done? When the project finishes or when the expenses have been done? Will the payment be made exclusively against invoices/receipts? What will be the admin circuit?

3.5. If we say "Joint proposals (up to 20k) are highly encouraged" and SoC 09 budget is =<>

1.9 Proposal: Remove all commercial/non-OWASP logos from OWASP.org

Following the recent threads about the commercialization of OWASP, I think the time as come for a simple move, that will be a little bit painful, but will clear the water and send a nice big message of what OWASP stands for.

Remove all commercial/non-owasp-projects logos from OWASP.org

This move has a log of advantages:

- it is generic so it doesn't single out anybody
- it can be done since there are no 'real' contractual obligations for OWASP to put company's XYZ logo on the OWASP site
- note that OWASP can change the contents of any content/text hosted on owasp.org[112] , as long as the changes are released in an compatible license :)
- in fact anybody can start the http://owasp-without-logos.org[113] site with all content from owasp.org[114], expect the 3rd party logos
- it will push the cases where sponsor-logos are expected to exist, to be placed in separate/dedicated 3rd party websites (like what happens with AppSec conferences)
  - and if there ARE execptions, they should be treated as one-of exceptions (and be fully documented)
- it will stop the current ***'F1/NASCAR logo parade'*** that is the OWASP main page, and some of its projects
- it will stop the nasty and non-productive ***"hey that company shouldn't have their logo in that project"*** threads
- it will send a strong message that OWASP is about sharing information and all information/tools/projects that are 'donated' to owasp are supposed to be shared in a no-strings/logos attached mode
- it will clarify that **the OWASP logo, name, tools and content CAN be used in commercial situations, as long as it is done outside of OWASP.org**
- it shows a sign of maturity for OWASP, where OWASP doesn't need (anymore) to sell a bit of its soul in exchange for good content and tools
- it shows that OWASP's value to the corporate sponsors, is NOT a logo on owasp.org[115], but the amazing value provided by the multiple OWASP activities, events and projects.
- it shows that OWASP can learn from others, and in this case, follow (as Jim recommended) the Apache foundation example (see http://www.apache.org/foundation/marks/responsibility.html[116])

There are a couple disadvantages:

- Some OWASP leaders and supporting companies will be annoyed and fell that *'OWASP changed the value-added they would get by contributing to OWASP'*

[112] http://owasp.org/
[113] http://owasp-without-logos.org/
[114] http://owasp.org/
[115] http://owasp.org/
[116] http://www.apache.org/foundation/marks/responsibility.html

- Some OWASP corporate sponsors might even be so angry that they don't renew their anual membership
- Some OWASP leaders might be so annoyed that they stop contributing at all to OWASP
- This is one of those issues that has the potential to generate a gazilion of emails, with lots of opinions and no decisions in the end. Btw, the faster 'a' decision is made the better (Yes or No).

I believe that OWASP today (April 2013) is in the perfect situation to make this move. There is enough money to sustain any financial loss (which I don't think will happen) and the OWASP projects are still in a state where a drop of a couple OWASP leaders wouldn't have a dramatic effect (which again i don't think will happen)

So what do you say, fellow OWASP friends, should we make this jump?

My vote is YES, lets get rid of the commercial logos in OWASP and start a new generation of OWASP content and tools

Dinis Cruz

1.10 Sarah Baso as OWASP Executive director, how it broke the model, structure and culture of OWASP employees

(note: I don't have a lot of time to write the detailed analysis that I wanted to do, but as time is passing by, I wanted to go on the record with my thoughts of that happened. So think of this post as a brain dump of my views on this important topic for OWASP)

In April 8th the OWASP board announced that OWASP Creates Executive Director Position[117].

My view at the time (and still is) was that OWASP Executive Director Role (Not yet)[118], specially because:

_What we need are another Kate, Sarah, Kelly or Samantha, they still work FAR too much for OWASP and my worry is that they will implode one day. Not sure that they need a boss to tell them what to do, if anything **I would delegate to them the powers currently 'assigned' to the Executive Director**._What happened next surprised most OWASP leaders since a couple days later the OWASP board announced that Sarah Baso[119] would become the new OWASP's New Executive Director[120]

Which of course means that there was never an effort/attempt to fill that position (externally or internally), and that the decision of that appointment was done much before the 8th of April OWASP Creates Executive Director Position[121] post.

**BIG DISCLAIMER: ** before you read the next part, it is good to take into account that:

- I was the one that found Sarah Baso for OWASP:
  - I meet her on the 10th of August 2010 when I was doing my crazy OWASP/O2 US Tour Aug 9-17 (6 cities in 8 days)[122]
    - here is the photo I took of Sarah after she picked me up from the airport and stopped at the local FedEx Kinkos: http://a.yfrog.com/img838/3711/bf6j.jpg[123] (here is the tweet I wrote at the time[124])
  - I hired Sarah for the OWASP Summit 2011 as one of the external contractors[125]
  - I was very unhappy with the time that it took to make Sarah an official OWASP employee
  - I went on the record with Let's not lose Sarah Baso too (22.5k USD needed)[126] with my show of support and urgency in hiring her
- During the OWASP Summit we worked a LOT together, with a really amazing collaboration and work environment (yes, there were a couple speed bumps, but Sarah was one of my most trusted helpers and really delivered when it mattered)
- I have sleep a couple times in her house (when in Minneapolis) and when in London she also spend a couple days in my house

[117] http://owasp.blogspot.co.uk/2013/04/owasp-creates-executive-director.html
[118] http://blog.diniscruz.com/2013/04/owasp-executive-director-role-not-yet.html
[119] https://www.owasp.org/index.php/User:Sarah_Baso
[120] http://owasp.blogspot.co.uk/2013/04/owasps-new-executive-director.html
[121] http://owasp.blogspot.co.uk/2013/04/owasp-creates-executive-director.html
[122] http://blog.diniscruz.com/2010/08/owaspo2-us-tour-aug-9-17-6-cities-in-8.html
[123] http://a.yfrog.com/img838/3711/bf6j.jpg
[124] https://twitter.com/DinisCruz/status/20819271151
[125] https://www.owasp.org/index.php/Summit_2011/External_Contractors
[126] https://lists.owasp.org/pipermail/owasp-leaders/2011-August/005999.html

- She is an a O2 Platform user: Batch PDF creation from OpenXml file (by O2 user)[127]
- She is a friend and deserves that I spend the time to write these words (remember that the real friend is the one that speaks what is on their mind (and cares enough to spend the time))
- I have not spoken with Sarah since this appointment was made
- I am not speaking on behalf of the other OWASP employees (in fact their silence in this matter speaks volumes)

So as you can see I know Sarah very well and have been part of the efforts to bring her to OWASP.

But the appointment of Sarah as the OWASP Executive Director doesn't feel right to me, and from my view is another reason why the current OWASP board needs to be disolved and re-created from scratch (see An Idea of a new model for OWASP[128]).

Ironically, right in the middle of this situation, lies a really good decision by the OWASP Board (which for an group that is famous for not making decisions, it's a great move and evolution). I'm talking about **the delegation of power and budgets to the OWASP employees**, which at least is a step in the right direction, by putting the power and responsibility for key OWASP operational issues in the hands of the OWASP employees.

The problem is that (from my point of view), this '*appointment*' has a number of issues:

Issue #1: Break of the OWASP Employees model, culture and social-contract

**

**

Lets be clear here, with this move, and with the powers given to Sarah, she can hire and fire other OWASP employees[129], namely: Kate, Samantha, Alison, Kelly and Matt

This is a massive mistake because it transformed the OWASP Employees (the OpsTeam like I like to call them) from a coesive and strong team, into a fragmented, hierarchical, bureaucrat and 'political' structure.

It is very important that the OWASP employees feel empowered to fight for OWASP and its multiple activities (projects, chapters, conferences, initiatives, tours, etc...). But without all being 'equals' this is very hard to do.

Issue #2: Lack of transparency on how/when the decision was made

This is a topic that I can't speak without getting into 'conspiracy theories' so I will just say that for an Open organisation like OWASP, this is probably the most *'non-open/behind-the-scenes activity that I have even seen'*

The rest of the analysis I leave to you :)

Issue #3: The way the appointment was done is a case-study on how not to do it

**

**

Not only there was the false impression that there would be a 'call for candidates', the way that the OWASP board first pushed it as an appointment, and then (after questions where raised) re-phased it as an 'Promotion from within', shows a massive lack of common sense, and more importantly lack of understanding of the OWASP leadership community.

[127] http://blog.diniscruz.com/2012/09/batch-pdf-creation-from-openxml-file-by.html
[128] http://blog.diniscruz.com/2012/10/an-idea-of-new-model-for-owasp.html
[129] https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project#Employees_of_the_OWASP_Foundation

I'm not on the board any more, so I don't know the details of what happened, by my understanding is that this was not done in a united/coordinated way (by all members of the OWASP board). Which is another bad move, due to the sensitivity of the situation and the massive change of the OWASP operational structure.

**
**

Issue #4: Sarah is not THAT much better than the other OWASP Employees

This is a though one to say on the record, but unfortunately Sarah is in a position where we need to look objectively at her appointment and ask '*compared with the other OWASP employees, does she deserve the promotion?*'

_
_

I.e. is Sarah that much better and qualified than the other current employees: Kate, Samantha, Alison, Kelly and Matt

Remember that we can't use the measure '*Sarah is working really hard for OWASP and she has done great stuff for OWASP*'

Because, ALL current OWASP employees (Kate, Samantha, Alison, Kelly and Matt) fit that bill.

In fact OWASP is very privileged to have such amazing team, which is actually quite qualified for the job they do.

And remember that by promoting Sarah and making her the 'boss' of the other OWASP Employees is basically saying that:_ 'Sarah is much better then the others and she deserves to be in power'_

Issue #5: Sarah has no CEO or Executive Director experience

Again, if we are going to look at this objectively, Sarah doesn't have the qualifications for this job. Now It is great to give people opportunities, but for me the position of CEO/Executive-Director of OWASP should be given (one day) to somebody:

- with a proven track record in that role,
- that is clearly 'above' the current OWASP employees,
- with past experience in running large teams of organisations with open culture like OWASP (for example a past senior executive of Mozilla, Wikipedia, Apache, etc...)

Issue #6: It is not fair for Sarah that she has been robbed of the opportunity to earn this role

**
**

Ultimately the biggest loser here (at least in the short term) is Sarah. She deservers better than the 'cold' reception that she got from the OWASP leadership community, and me writing posts like this.

Note that I'm not saying that Sarah could not 'one day' become the OWASP executive director, but not like this, and not like it was done.

For example, if there was supposed to be an 'promotion from within' then that should had been a democratic process from within the OWASP employees, namely there should had been a vote where only the OWASP employees would vote and chose amongst themselves who would have the extra powers

Also the lack of public support by the other OWASP employees and 'heavy weight' OWASP leaders speaks volumes, and show how divisive this move was.

This role really needs to be given to somebody that has a HUGE amount of political capital to spend (and get things done). Without that grass-roots support, any major (or minor) change is going to be a struggle, specially given the distributed nature of OWASP community (and opinions :))

Issue #7: Sarah doesn't need the extra power, is the OpsTeam who need it

I also fail to understand why in the current size of the OWASP employees (the OpsTeam) there is a need to have an 'Executive Director' with absolute powers over the others?

What decision is Sarah going to do with that power?

Fire one of the employees? I hope not, since none of them deserve that and it would be a crazy move (even worse than the current appointment)

Also, there is already a good separation of duties of the current employees, so they should be empowered to make decisions, not being given an extra management layer and 'chain of command'

If I talk with Kate, Samantha, Alison, Kelly or Matt, on an topic that they are currently responsible for, I EXPECT them to have the authority and power to deal with the issue at hand. Not to have to go to the board or Sarah and 'ask for permission or decision'

**

**

Issue #8: It is not fair on the other OWASP employees that they didn't had a change to apply

**

**

Again I don't have much inside track on what happened and who-knew-what-when.

And since there is no documentation about the decision, it is fair to assume that the other employees never had a chance to apply.

This is where process and respect matters. It quite possible that on a parallel universe, Sarah would had become the Executive Director in a way that was highly celebrated and endorsed. In this parallel universe, after _**an open**, **transparent**, **democratic and pragmatic evaluation/process**, _Sarah would had emerged as the perfect choice. But that would had required a completely different process and sequence of events.

The issue here is not that Sarah was chosen, the issue is how it was done. Note that although I hired a number of people I knew personally to work on the OWASP summit, all those efforts were done in the open and there was plenty of opportunity for others to apply and take those 'paid roles' (and there was budget for more talent (but we couldn't find it))

Issue #10: Sarah already had a full time job at OWASP: Conferences

So if she is going to take on more responsibilities and roles, who is going to continue the amazing work Sarah was doing at the Conferences?

The other OWASP employees are already maxed out!

If Sarah keeps doing it, why the appointment?

If Sarah drops parts of it, OWASP will be losing energy and focus on one of the areas that is currently working really well!

Issue #11: I'm disappointed with Sarah by her allowing this to happen

Of course that most of you will not care about by the fact that I'm *disappointed*, and maybe even Sarah wont.

But I was very disappointed by Sarah allowing this happen (specially because she didn't took the opportunity to use her new powers to make it better (see first points of '*How to fix it*' section below)).

This fells like a 'power grab' and Sarah was not able to resist the offer.

Well ... I expected more from Sarah, and she missed an opportunity to show the human and professional qualities that she has.

I hope to change my mind in the future, but I have to say that at the moment I loss some of the respect I had for Sarah :(

Of course that this doesn't matter since I have no more power at OWASP.

I'm also disappointed by the lack of public critical thinking at the OWASP's leaders list, and the few number of OWASP leaders that actually take the time (and still care enough about OWASP) to write about their views/opinions (note: I'm not even going to post this blog into the OWASP leaders list (it would be great if somebody else cared enough about OWASP that they posted it there, together with their views on this post)).

I don't claim that I'm 100% correct with my views and that I have all solutions, but the only way to fix things is to have open and franc discussions/threads about what is going on. And once the 'issues' are identified, it is important to also proposed solutions.

.... which leads me to:

How to fix this

We can't go back in time, so what we need to do now is to look at ways to fix this

Assuming that there is an agreement that something should be done, here are my proposed actions:

1. **change the model so that all OWASP employees are 'equals'**
2. **put a rule in place where the OWASP employees can only be fired by a majority of the OWASP leaders** (by vote)
3. **Cross post or link this blog entry from the OWASP's official blog **(http://owasp.blogspot.co.uk/[130]) together with other related threads / responses (after all, OWASP is about being open, and this current blog post contains an analysis of OWASP by somebody who has done a lot for this organisation (me :))
4. **publicly apologise to Sarah** for putting here on such though position
5. **publicly apologise to Kate, Samantha, Alison, Kelly and Matt** for the unnecessary stress created
6. **publish details for how the decision was made** (and when), so that we have a good documentation of what happened and future generations of OWASP leaders can learn from past mistakes

[130] http://owasp.blogspot.co.uk/

Of course that given the current structure and political mess that is OWASP at the moment, it is probably more likely that we will have an unthinkable _'5 days-in-a-row without rain and cold ***_here in London'***, than this happening :)

Good luck Sarah, and how can I help?

Since probably Sarah is one of the few ones that is still be reading this post, I would like to first say to you:

I'm sorry …

… for writing this email, and hopefully one day you will appreciate it and see that I'm writing this because I'm your friend and still care about you and OWASP

Good luck …

… with your efforts to making OWASP an amazing organisation

Please prove me wrong…

**

**

… by showing how your appointment as Executive Director was a turning point for OWASP and that what happens next will make this post look like the most 'stupid thing that I ever did'

Let me know how I can help…

… I expect that you will not be happy with this post, but remember that I love OWASP and that I'm writing this because I still care (in fact, a worrying sign for me is how long I took to write this, since there were multiple times last month where I started 'not caring' enough to stick my neck out, and do what I believe to be the best for OWASP (in this case, write this post))

Good luck OpsTam, and how can I help?

**

**

Kate, Samantha, Alison, Kelly and Matt (OpsTeam), since you are also reading this, I would like to also say to you:

**

**

I'm sorry …

… for posting something that might make your live harder.

Now you know and I know that you didn't ask me to write this, and have barely taked to me since the 'appointment', hopefully Sarah (and the OWASP Board) will also believe that, and not give you any trouble for this public criticism of their actions.

Sarah, I hope that you view this post as an opportunity to connect and listen to your 'employees' and create something positive

Good luck …

… since your job at making OWASP work just got more complicated and frustrating.

Let me know how I can help…

**

**

You are the heart and soul of OWASP and nobody cares about OWASP as you do :)

Please keep doing your amazing work for this crazy community, and as active member of that community, I'm here to help you in as much as I can

1.11 Why OWASP can't pay OWASP Leaders

Since I was the one that created and executed (initially alone and then with Paulo) the only Seasons of Code that OWASP did (AoC 2006[131] , SoC 2007[132] , SoC 2008[133]) I know first hand what can be done, what works, what doesn't work and its side effects. In fact it was that experience that made me have such strong views on this topic.

There is a subtle but very key distinction that we need to have in this thread. And that is the issue of 'OWASP paying OWASP leaders'

Hiring interns or other professionals to work on specific projects/tasks is fine (specially if they are doing what our OWASP leaders and contributors don't want to do). The main problem happens when OWASP leaders can be part of the pool that can be paid by OWASP (again nothing wrong with them being paid by a 3rd party to work on an OWASP Project (like what already happens today)).

So why it is very wrong to pay OWASP leaders to work on OWASP projects?

Let say that there is 2000 USD available to pay an OWASP leaders to work on his project

- **Changing of the social contract - **The moment money is introduced, invariably the target individual is going to make a math calculation (what is his current daily rate?, how much he earns at the moment?, how much his current boss bills for his time? , etc….).The end result is that we moved from a 'contributor' model to a 'service provider' model
- **_'I will do that for free, but won't do it if I am paid' _syndrome** - If one starts to look at OWASP contributions with a financial angle, then what one would gladly do for free is now viewed from a completely different angle. I would strongly recommend the 'Predictably Irrational' book on this topic, which has tons of great example on how money doesn't help (here is preview of what the author talks about: http://en.wikipedia.org/wiki/Predictably_Irrational#Being_Paid_vs._A_Friendly_Favor[134])

The RSA Animate - Drive: The surprising truth about what motivates us[135] is also a brilliant video/animation on motivation:

- **A rate for an Worldwide audience? - **given the truly global presence of OWASP, $2000 might not be a lot for a successful security professional (or conference speaker), but it is good money in countries like Portugal/Italy, and if you go to India/China it is a lot. So how do we do this? Surely it doesn't make any commercial sense (for OWASP) to pay a guy from London or the US, right? Can't we get a LOT more hours and effort from somebody that lives in a cheaper country! I'm sure there are places in the world (or on elance.com[136]) that we can rent a team of workers for $2000 for a month !
- **Prevents multi-national teams from occurring** - What happens when you want to get a couple resources involved from different countries? Are you going to pay them the same? And if not, is that really sustainable? There is a huge amount of HR theory that shows that collaborators are much happier

[131] https://www.owasp.org/index.php/OWASP_Autumn_Of_Code_2006
[132] https://www.owasp.org/index.php/OWASP_Spring_Of_Code_2007
[133] https://www.owasp.org/index.php/OWASP_Summer_of_Code_2008
[134] http://en.wikipedia.org/wiki/Predictably_Irrational#Being_Paid_vs._A_Friendly_Favor
[135] http://www.youtube.com/watch?v=u6XAPnuFjJc
[136] http://elance.com/

(and productive) when they don't know how much money their colleges earn (but how can you do that in an OWASP environment like OWASP where all financial deals must be disclosed)
- **A lot more money will be needed** - This is another massive problem. If we REALLY want to get the best talent, and REALLY want to take a professional approach, then we will have to buy the best talent, which is expensive AND will need to be paid a good rate.

And why should we pay them so much? … They will deliver, right? Aren't they the best? Why shouldn't we put 40k or 100k of OWASP's money in their hands?

Well, apart from the fact that those 100k would not *'create that super-duper deliverable'* (we are talking about big projects with complex problems that need LOTS of work), the problems I'm raising here would be dramatically multiplied

- **Nobody is independent at OWASP - **Here is the catch, it is impossible to find somebody (or a group) inside that OWASP that has any kind of independence to be able to make a real solid decision (everybody has an agenda, a pet project/chapter/conference, a particular vision for what OWASP should be doing, etc…) So who is going to make the call?
- **Little secret - on the last OWASP Seasons of Code, all (decent) proposals got funded **- so how did we avoided this problem in the last OWASP Seasons of Code? I.e. how did we actually selected the owasp leaders who deserved the funding? In what turned out to be an amazing feat of maths and mappings, we actually funded every decent proposal that was summited (remember that OWASP was MUCH smaller than it is now, and there was still space for a number of new OWASP contributors to join the party)
- ***'He/she are the ones being paid, THEY should do that'* syndrome** - This is another problem that happens when there is somebody that clearly is being paid when others are not. Yes we will still have this problem when they are paid outside of OWASP, but to be on the same 'level' as somebody else and they are being paid, really creates a bad vibe
- **Lots of negative energy is created - **For me the point of the last Seasons of Code, was not to pay people!

It was to motivate them, to empower them and to give them space inside OWASP.

This is why It was so important to me that no good proposal was left out, since the objective was to motivate people to do their best (not to get a group of OWASP contributors to start fighting each other)

- **It breaks an OWASP Contributor heart to receive a NO - **We also had a couple cases were great OWASP leaders/contributors, turned to the board (where I was at the time) and said. *"..Hey I have this idea, can you give me 20k / 40k so that I can spend the time to do it? … you know I can do it!, I have a good track record !.."*. And it was pretty obvious that when we didn't support that idea, that OWASP leader was really not happy
  - How to say NO to a big contributor - If OWASP leaders could be paid by OWASP, it would create situations where it is very hard to say NO to a big OWASP contributor, even if maybe he is not as qualified to do the job as the other candidates (there are always emotions involved).
  - _'**I could had done better with that money**' _**syndrome** - And then after the work is done and delivered, the one who got paid, is now a sitting duck for sniper fire that will pick his/hers work apart

  - **What to do when the leaders don't deliver? - **We also had this on the last OWASP Season of Code, where a couple really Large (with capital L) OWASP contributors, took a good chunk of cash and didn't really do a good job! So what do you do? Are we really going to buy that fight and shame that person in public for doing a bad job? Also, how to you handle other OWASP leaders/contributors that also worked on that task but didn't get paid.
  - **We can't even count the leaders that we have today, can we review their work? **At the moment we can't even keep track of our current projects and still have a lot of project review work to be done. Are we (OWASP) really in any shape to review commercial/paid work?
- **What about the other big contributors** - Also take into account, that there are a number of OWASP leaders who have spent years of their life working for OWASP projects
  - **For example: My Wife would kill me (if other owasp leaders got paid) **I spent 18 months without any pay to work on the OWASP O2 Platform. I still have debts today from the lack of income I suffered during that period. My wife was really unhappy with that (understatement of the century) and my kids gave me a very hard time. But they supported it, because they accepted my passion and focus on 'doing the right' thing. I'm not asking for any money from OWASP, BUT if others are getting paid, then that would completely change the dynamics of my relationship with OWASP (at least it would for my wife)
  - **What about Jeff and Dave?** These two, even had to use some of their own money to buy some OWASP assets and release them to the OWASP community (surely they should be repaid that?)
  - **What about Denis, Andrew, Daniel, Matteo, John …. **(the list would go on and on and on…)
  - **Slippery slope**:
  - **What about the conference organizers** - shouldn't they also get slice of the profit they generate?
  - **What about the successful chapters?** - specially the ones with lots of attendees and generated funds?
  - **What about those hard-working board and committee members?** - should they also be paid for they countless hours?
  - **This will bread corruption and favouritism **- which is human nature given the right environment
- **Killing the golden goose - **If you look carefully, we already have an amazing capability to 'convince' highly paid individuals to work for free and dedicate their energy into something they believe. For example if you add up all the 'money' (in time) that is 'donated' to OWASP every day or month by its leaders, contributors, participants, you would be amazed (for example it would probably cost 1,000,000$ (1M$) to pay for the talent that we were able to assembly at the last Summit (and even then, I don't think that if we were paying the attendee's a fee for their time, we would had been able to assembly that crowd)
  - **Not Paying OWASP Leaders is a self-defence mechanism - **Give the massive web of trust that OWASP has (just add up all its leaders), it is much easier to trust them with OWASP funds when they can't pay themselves or a friend (it also dramatically simplifies the rules of engagement)
- **Let's get 3rd parties to fund those OWASP leaders **- Jeff and John proposed a great model with the OWASP Project Partnership Model[137] which is how we can get OWASP leaders/contributors to be paid for working on OWASP projects. I don't know who said _'..the real sign of a product's value is when somebody is willing to pay for it…' _but it is very true. In fact, it should be a sign of maturity and market-acceptance, the fact that somebody (company, government, etc) is ready to invest on that project.

[137] https://docs.google.com/document/d/1ea4jWVDziLcZMTJUC5qW5psWYROpB-oPlqyl4Ei2xHA/edit?hl=en_US

- **Prevents OWASP from finding better solutions (to Money) - **Finally this is (for me) the key reason why paying OWASP leaders is a very BAD idea.

We (OWASP) need to figure out what are the social/commercial models that work for OWASP (and make us productive).

Clearly contributing to OWASP makes business sense. If it didn't we wouldn't have the sustainability and energy we have.

There are countless stories of OWASP leaders getting better jobs, being promoted, increasing their income, learning key skills, etc… There are also a number of companies that regularly support OWASP. They don't do it because they want to be nice, they do it because it makes commercial sense to them.

**So what we REALLY need to do, is to rationalize what makes OWASP work, and see if we can improve the current model, so that we can have more and more people being paid to work for OWASP Activities. **

I could continue, but hopefully some of these points will clarify why OWASP can't pay OWASP.

Wrapping up, this is actually a great opportunity to move OWASP to the next level.

1.12 Why the need to enable the use of OWASP chapter funds

I just send the text below to the OWASP Leaders list, which was part of this thread[138]

_

_*My answer was to Tim's comment*[139] *and I started a new thread with it*[140]

Tim's solution (see below) is great and we should apply it now (using data from the last year). The only thing I would change is to remove the C (soft cap) and P (hard cap). This would have a net positive result for all chapters (and not move the money to the 'OWASP mothership' which is a very sensitive topic).

For the ones really interested in this thread/topic, you should read the amazing Seth Godin's post Non-profits have a charter to be innovators[141] which really explains why OWASP (as an organisation) as the DUTY and moral responsibility to spend its available funds, to experiment, to get things done, etc....)

The other very important question is **WHY! **(as explained by the also amazing 'Why how what' presentation by Simon Sinek[142])

Why does OWASP need money?

Why do chapters need money?

Why should owasp leaders use their political/business/personal capital in becoming a 'vendor' for OWASP?

In my view, OWASP needs money to **Get Stuff Done!**

**

**

And although there is always an idea that OWASP funds will be massively wasted, the reality (just look back at History) is that **It is very hard to spend OWASP Money**

**

**

The best examples are the dormant funds in the Chapters, the Project Reboot funds that have barely been used and (my failed attempt) at the GSD project (Get Stuff Done)[143] which has **3k USD that any of you could spend TODAY**

As I mentioned in my OWASP Revenue Splits and the "Non-profits have a charter to be innovators"[144] post, OWASP has a** 'How to spend the money' **problem and in the 160k USD available to OWASP Chapters and Projects[145] (written in April 2012 hence the smaller amount) I wrote:

[138] http://lists.owasp.org/pipermail/owasp-leaders/2013-June/009446.html
[139] http://lists.owasp.org/pipermail/owasp-leaders/2013-June/009459.html
[140] http://lists.owasp.org/pipermail/owasp-leaders/2013-June/009487.html
[141] http://sethgodin.typepad.com/seths_blog/2012/11/non-profits-more-innovative.html
[142] http://www.ted.com/talks/simon_sinek_how_great_leaders_inspire_action.html
[143] https://www.owasp.org/index.php/OWASP_GSD_Project
[144] http://blog.diniscruz.com/2012/12/owasp-revenue-splits-and-non-profits.html
[145] http://blog.diniscruz.com/2012/04/160k-usd-available-to-owasp-chapters.html

In fact, the 160k USD currently available, shows that the model is not working as well as it should, i.e. OWASP leaders are not spending (i.e. investing) the money make available to them!

_
_
I think there are two reasons for it:

- *spending money in an organization like OWASP is not easy*
- *there is an idea that 'money should be kept' in the bank since it is not wise to spend it all (i.e. be fiscally conservative)*

The problem here is that the amount of missed opportunities caused by the non-spending on these funds ie enormous, but because that is very hard to measure (how do you quantify missed opportunities?), it is hard to visualize the solutions and ideas we have not executed on.

_
_
I think that one way to help the chapters to spend the $ allocated to them is for them to 'invest' in OWASP Projects under a program like the one I present at OWASP Project Reboot 2012 - Here is a better model [146]

What is great about such_ 'owasp chapters global fund' _is that:

- It moves the discussion from '*how much money do I have*' to '*what should I do with the funds available*'
- It really supports the chapters that don't have a lot of funds today
- It can also also benefit chapters with substancial funds today, since there is no reason why they can't also access those resources
- it promotes accountability and ownership of funds allocated
- it puts an 'artificial' timeline on the use of funds allocated (i.e. there is a 'pressure' to deliver)
- it helps to find the OWASP leaders who know how to spend OWASP funds and make magic happen (like Fabio with the Latam and EU tours)
- It empowers action, and promotes the idea that '*we trust our chapter leaders to do the right thing'*
- it documents the places where OWASP funds are used (making those ideas/actions easy to replicated)
- it also documents the failed experiments (which are healthy, but don't need to be repeated :)).
- it stops the 'ownership of funds' and 'lets keep it in a safe place' that we currently have
- It can dramatically simplify how the funds are accessed since there will be a central point of contact and pot (with better/faster processes that world worldwide)
- it turns up the volume/pressure on the '_% of OWASP funds used', _since everytime **_something that could happen**, **doesn't happen**, _OWASP misses an opportunity (and we need some 'urgency' and focus on 'not lossing those opportunities).

[146] http://diniscruz.blogspot.co.uk/2012/04/owasp-project-reboot-2012-here-is.html

See the rules I wrote down at the GSD project[147] for how this could work in practice.

Like I mentioned before, I don't really care about where the money is, and what percentages there are in place (in fact history is showing us how divisive those splits can be). The point is that **OWASP Funds MUST be available to Who wants to use them!**

**

**

And as I listed in I wish that OWASP in 2014 ....[148], it would be great that one day we will have at OWASP:

- ....
- _a model where OWASP leaders are empowered to make financial decisions/commitments and spend the available OWASP funds in the way they believe is best, with no (very little) questions asked and very fast approval cycles (see the GSD project for details)

  _
- ....

Dinis Cruz

On 6 June 2013 17:35, Tim <tim.morgan@owasp.org[149]> wrote:

> Yes, this is what came to my mind as well. Incorporating Dinis suggestion and some of my own ideas, what about this:
>
> Individual membership dues: 75% to chapter, 25% to foundation
> Corporate membership dues: 25% to chapter, 75% to foundation
> Conference/event profits: 25% to chapter, 75% to foundation
>
> Let C be the chapter funds "soft" cap
> Let P be the shared chapter pool "hard" cap
>
> Once per year, do the following:
> For any chapter with funds greater than C, move %50 of any excess funds C into a shared chapter pool
>
> If the the chapter pool is greater than P, move all excess funds to the global foundation
>
> Any chapters can "overdraw" their chapter account and pull from the chapter pool. Perhaps some kind of limit should be put on how much any given chapter pulls from the shared pool in a year.
>
> Reasoning:
>
> I think individual membership dues are important to keep with the chapter. It encourages contribution and participation at the local level. Corporate membership is probably not quite the same in that

[147] https://www.owasp.org/index.php/OWASP_GSD_Project
[148] http://blog.diniscruz.com/2012/11/i-wish-that-owasp-in-2014.html
[149] mailto:tim.morgan@owasp.org

way. Also, I'm guessing individual membership dues are not the biggest contributor to chapter funds right now (whereas conferences and corporate contributions probably are), so it isn't going to cause a big lockup of funds by putting more of the individual dues toward a chapter.

In this system, the shared chapter pool is not so much different than what we are doing this year in 2013 where a $500 overdraw was offered to poor chapters. I think this overdraw ability is *very* useful to new chapters.

Of course all suggested numbers above are negotiable, it's just a framework for more fairly unlocking excess funds.
tim

1.13 Why NDAs have no place at OWASP

I was looking for a place to link why it is such a bad idea for OWASP to consider or accept the idea of signing NDA's with 3rd parties, and since I couldn't find it on the OWASP Wiki, I'm reposting here what I wrote in June 2011:

```
_I don't buy the argument that there is a ton of opportunities that OWASP is
missing because we don't have this 'save harbour' locations to talk.

The other key concept that you guys are missing is that the 'no
NDA everything is public' is actually the best way for *OWASP to control
OWASP* and to prevent the existence of 'pockets of knowledge' or 'groups
that know more than others' inside OWASP (just try to image how this would
work in practice and you will see how impractical this would be).

If we want to preserve our community and open spirit we need to have
an uncompromising Open environment.

I would also argue that a big problem in our industry (and software
development/apps in general) is the excessive use of NDA and lack of
information sharing. So if any thing, OWASP should be pushing the other
direction and be actively promoting dialog and 'conversations'

For example look at how we were able at the last OWASP Summit to get
directly competing companies to sit on the same table and talk 'openly'.
THAT is what we need to. Create the time and place, and the dialog with
OWASP will come.

_

_
_

You can read the rest of the threat at: [No i will not sign your NDA but...](https://lists\
.owasp.org/pipermail/owasp-leaders/2011-June/005700.html)









A good example of the mess created by providing 'secret data' to an OWASP leaders (with th\
e promisse the it wont be disclosed) if what has happened with the OWASP Top 10 data. See \
this post: [Stats used to support OWASP Top 10 entries (next version must publish them)](h\
```

```
40 ttp://blog.diniscruz.com/2013/01/stats-used-to-support-owasp-top-10.html) for more details\
41 .
```

1.14 Me and Jim Manico

I really like Jim. He is passionate, loves OWASP and has great energy.

Although he is from the Hawaii, he has Italian Sicilian blood, which means that his first reaction tends to be a bit off piste. But he listens well, he has an amazing breadth/depth of technological skills and is (like me) trying to change/fix the world.

These days, since I'm not in any position of power at OWASP (I left the Board two years ago), I am in a very privileged position where I can speak freely about my ideas (see You will not have your best ideas when you are in a position of Power[150]). And as you can see by the 46 posts (so far) on this blog about OWASP[151] I have been doing that a lot :)

Since I know that I can hard to deal with and can sometimes cause offence with my comments, views or actions (see Why do others think that I'm "hard to deal with" and that "I don't listen"[152]), I asked him recently: _"Jim, are we ok? or have my latest OWASP related emails pissed you off." _

And true to form, here is Jim's answer (re-posted with permission) which just shows how an amazing person he is:

Dinis,

Sure you annoy me sometimes, but more importantly you always stay on topic around web security, OWASP governance and OWASP's future. And you are solid about respecting OWASP's basic ethical guidelines.

The fact that you annoy me irrelevant. This is not about me. The fact that you are "on point" around OWASP issues is what matters. It's about what is good for OWASP.

I really don't agree with you that much either. On occasion I do agree, but I often do not.

But this is ok, we need to keep rattling each others cages. I can take it. We are pushing for the same thing - a healthy OWASP.

So, Dinis. Bring it, man. Give me your best. It's my **job** and **responsibility** as an OWASP board member to engage with you respectfully when you express ideas about making OWASP better.

[150] http://blog.diniscruz.com/2012/10/you-will-not-have-your-best-ideas-when.html
[151] http://blog.diniscruz.com/search/label/OWASP
[152] http://blog.diniscruz.com/2012/10/why-do-others-think-that-im-hard-to.html

1.15 On John Wilander....

John asked me this today via linkedIn to write a recommendation for him:

_Dear Dinis, _

_As I wrote on the leaders list I'm no longer co-leader of OWASP Sweden as of this week's chapter meeting in Stockholm. Hopefully you can help to briefly summarize/recommend my OWASP work 2007 till now.

Thanks in advance!

-John Wilander_

Which of course I was happy to do.

Here is what I wrote:

John is one of the few guys in the world that I would hire on the spot (if I could). Not only he is an expert in his field (checkout his PHD on 'using static analysis for security') he is a great Person (with capital P)

His contributions at OWASP rank above the highest ever, specially the way he organised the OWASP AppSec EU conference in Stockholm, and how we was able to assembly an amazing set of participants for his 'Browser track' at the the OWASP Summit in Lisbon.

John also is a great singer and I have really amazing memories of us playing together in multiple OWASP conferences and summit.

Finally, but as important, John is a team player, has a great soul and is somebody I would trust implicitly. This means that he is an amazing asset for any team.

As you can see by this review, I have John in very high regard, and hope that one day I will be privileged to work with him on another project/initiative :) Thanks John for all your great work and contributions (so far) to OWASP and the WebAppSec community :)

2 OWASP Projects

This section has the following chapters:

Table of Contents[12]

[1] /manuscript/2.OWASP_Projects/160k_USD_Available_to_OWASP_Chapters_and_Projects.md

[2] /manuscript/2.OWASP_Projects/If_you_ever_doubt_that_OWASP_needs_more_Project_Managers_Resources.md

[3] /manuscript/2.OWASP_Projects/On_how_to_get_paid_to_work_on_OWASP_projects.md

[4] /manuscript/2.OWASP_Projects/OWASP_GSD_Project_(Get_Stuff_Done).md

[5] /manuscript/2.OWASP_Projects/OWASP_Project_Reboot_2012_-_Here_is_a_better_model.md

[6] /manuscript/2.OWASP_Projects/OWASP_project_reboot_spent_funds_(not_a_lot_spent_so_far).md

[7] /manuscript/2.OWASP_Projects/Project_Management_at_OWASP.md

[8] /manuscript/2.OWASP_Projects/ROI_on_OWASP_investment_on_Projects_(ie_paying_leaders).md

[9] /manuscript/2.OWASP_Projects/Some_ideas_for_OWASP_GSD_Project.md

[10] /manuscript/2.OWASP_Projects/The_difference_between_being_'Appointed'_and_being_'Accepted'_as_an_OWASP_Leader_(of_its_Fork).md

[11] /manuscript/2.OWASP_Projects/Why_large_OWASP_projects_start_to_stale_(and_who_should_pay_for_the_work).md

[12] ../../Table_of_Contents.md

2.1 160k USD available to OWASP Chapters and Projects

This spreadsheet: https://docs.google.com/spreadsheet/pub?hl=en_US&hl=en_US&key=0Atu4kyR3ljftdEdQWTczbUxoMUFnV contains the list of funds available to OWASP Chapters and Projects (actually mainly chapters)

The concept of allocating funds to Chapters was something that I help to implement a while back and the key concept of it was to allocate a certain % of OWASP membership funds to chapters (or projects) from either a local company 5k corporate membership or a locally executed profitable conference.

The objective was to empower the leaders to spent the funds available to OWASP since 'in principle' they owned it..

I'm not sure how much funds have been spent over the last couple years, but I don't think that it is a lot, specially if we don't count the amounts used by the last Summit

In fact, the 160k USD currently available, shows that the model is not working as well as it should, i.e. OWASP leaders are not spending (i.e. investing) the money make available to them!

I think there are two reasons for it:

1. spending money in an organization like OWASP is not easy
2. there is an idea that 'money should be kept' in the bank since it is not wise to spend it all (i.e. be fiscally conservative)

The problem here is that the amount of missed opportunities caused by the non-spending on these funds ie enormous, but because that is very hard to measure (how do you quantify missed opportunities?), it is hard to visualize the solutions and ideas we have not executed on.

I think that one way to help the chapters to spend the $ allocated to them is for them to 'invest' in OWASP Projects under a program like the one I present at OWASP Project Reboot 2012 - Here is a better model[14]

[13] https://docs.google.com/spreadsheet/pub?hl=en_US&hl=en_US&key=0Atu4kyR3ljftdEdQWTczbUxoMUFnWmlTODZ2ZFZvaXc&output=html

[14] http://diniscruz.blogspot.co.uk/2012/04/owasp-project-reboot-2012-here-is.html

2.2 If you ever doubt that OWASP needs more Project Managers/Resources

Like Samantha Groves[15] :

[16]

Then you should read these amazing monthly reports (written by Samantha)

- OWASP Project Manager Activity Reports/April 05 2013[17]
- OWASP Project Manager Activity Reports/March 11 2013[18]
- OWASP Project Manager Activity Reports/February 11 2013[19]
- OWASP Project Manager Activity Reports/January 14 2013[20]
- OWASP Project Manager Activity Reports/December 10 2012[21]
- OWASP Project Manager Activity Reports/November 12 2012[22]
- OWASP Project Manager Activity Reports/September 10 2012[23]
- OWASP Project Manager Activity Reports/August 13 2012[24]

And also take a look at the new OWASP Projects page: https://www.owasp.org/index.php/Category:OWASP_Project[25]

My only worry is that there is SO MUCH to do!!! and Samantha is only one :(

Last time I spoke with Samantha she was still under the impression that she would only need help in late 2014, I hope that she will soon realize that there are a lot of areas where she could do with more resources (starting with resources to do actual 'project management', since at the moment she doesn't have the time to do that for the projects that really need it)

[15] https://www.owasp.org/index.php/User:Samantha_Groves
[16] http://lh3.ggpht.com/-x6pby3-8gLA/UWmLkD9Vy4I/AAAAAAAABRA/7OL-GEOpZ1Q/s1600-h/image%25255B2%25255D.png
[17] https://www.owasp.org/index.php/OWASP_Project_Manager_Activity_Reports/April_05_2013
[18] https://www.owasp.org/index.php/OWASP_Project_Manager_Activity_Reports/March_11_2013
[19] https://www.owasp.org/index.php/OWASP_Project_Manager_Activity_Reports/February_11_2013
[20] https://www.owasp.org/index.php/OWASP_Project_Manager_Activity_Reports/January_14_2013
[21] https://www.owasp.org/index.php/OWASP_Project_Manager_Activity_Reports/December_10_2012
[22] https://www.owasp.org/index.php/OWASP_Project_Manager_Activity_Reports/November_12_2012
[23] https://www.owasp.org/index.php/OWASP_Project_Manager_Activity_Reports/September_10_2012
[24] https://www.owasp.org/index.php/OWASP_Project_Manager_Activity_Reports/August_13_2012
[25] https://www.owasp.org/index.php/Category:OWASP_Project

2.3 On how to get paid to work on OWASP projects

Here is an old blog post (from May 2012) that I never got around to publish (got lost on the drafts folders), that provides more info on why OWASP cannot pay its leaders, and how to get paid to work on OWASP projects

Since this was a personal email, I replaced the OWASP leader name and project with XYZ and Project ABC

Hi XYZ

(before you read my answer below, read this email to the leaders I sent last year: https://lists.owasp.org/pipermail/owasp-leaders/2011-January/004493.html[26] about the opportunity to hire Sandra to work on OWASP Projects)

I know you are not doing it for the money (none of us are), and I agree that if you were able to have dedicated time to work on the Project XYZ it would make massive progress (same thing for a lot of other projects)

The problem is that YOUR fees cannot be paid by OWASP (for all the reasons I mention in the 'Why OWASP can't pay OWASP Leaders' blog post[27]). Even worse, if OWASP would pay your fees, it would probably be a disservice to you since you probably would not be able to charge close to your commercial value (i.e. what a company would pay you). Again that would not be scalable, since it would mean that the the only way you could get paid to work on OWASP is to take a big pay cut.

Now two things:

**1) The way you are currently planning to spend the funds **(which you applied for) is exactly the way I think OWASP can support your (and other leaders) efforts. In fact my idea with OWASP GSD Project (GSD = Get Stuff Done)[28] is to take that to another level and say *"Hey... we trust XYZ so he can just get on and get it done (no need to 'submit proposals', just list where he wants to spend it)"*

2) You are asking your currently employer to 'sponsor' you with paid time. Now THAT is the way to get you paid. Recognizing when an OWASP Leaders is being sponsored by a company to spend 'Company time' on a project is one of the areas that we have failed miserably at OWASP. I tried to move things on the right direction when at the Summit I was able to inject that information into the Attendee list (see "Summit Time paid by' column in https://www.owasp.org/index.php/Summit*2011_Attendee)*. And this type of 'payment' is the most effective one, since you can negotiate your contract with the company that is hiring you (in Private) and it would not break the contributors model. Note for example that that type of deal is the one I have with SI at the moment. I am able to spend my paid time on OWASP and O2 (with no cost to OWASP). And this also happens with a LOT of other OWASP leaders

So XYZ , I still want you (and) other OWASP leaders to be paid for working on OWASP projects. In fact I want you to be paid your full (or close) commercial rates. The key is that we need to figure out a model where 3rd party companies (or governments) pay that bill.

I think we are getting closer now, but with everything, if there isn't a model created, it will not scale and we will not be able to take it to the next level. This is what I tried to create last year with Sandra's proposal

[26] https://lists.owasp.org/pipermail/owasp-leaders/2011-January/004493.html
[27] http://diniscruz.blogspot.co.uk/2012/04/why-owasp-cant-pay-owasp-leaders.html
[28] http://diniscruz.blogspot.co.uk/2012/05/owasp-gsd-project-gsd-get-stuff-done.html

(https://lists.owasp.org/pipermail/owasp-leaders/2011-January/004493.html[29]) and unfortunately there wasn't momentum (and vision) on our community to push it (I was also leaving the OWASP Board so I was not comfortable in pushing that concept without full support and commitment from the board and leaders).

Basically the model at https://lists.owasp.org/pipermail/owasp-leaders/2011-January/004493.html[30] is the one that I think will work for you (note how in that case the fees where arranged between SI and Sandra, which is how it should be)

Dinis Cruz

On 15 May 2012 09:55, XYZ wrote:

> Hi Dinis,
>
> I've agreed to disagree with you on this one; I'm not in it for the money. I just want it to get it done, but I can't do that (in a reasonable time) whilst working 12-14 hour days. My job allows me to pay my rent, health insurance, car payments, and allow my family to eat. However, it's not to be, so my time will necessarily limited to weekends, nights after my daughter goes to sleep, and train rides when my paying job doesn't have too much on.
>
> If OWASP could fund me so that I could take leave without pay (i.e. a career break) for say six months, the headstart would be fantastic. You experienced that headstart when you did O2, and I understand your family's sacrifice to make that work. Realistically, I don't have the luxury of savings, so even though I know what is a minimal amount of money I need to live, one to two weeks is not going to get that far on the Project ABC.
>
> I've put a budget submission in for the new Project ABC, primarily to organize a face to face at appsec research to do a planning session and most importantly, a hack-a-thon. I have asked my work to sponsor the Project XYZ effort so that I can travel to Athens, but if they don't agree to allowing me time off and 20% time (i.e. the sponsorship element), then I can't be there. The reality is that if they say "no" then there's every chance I can't work on the project until I leave Company ABC. I hope it's not a "no". This is one of the reasons I've never done Project ABC work in my employer's time or on their equipment.
>
> thanks,
>
> XYZ
>
> On Sat, May 12, 2012 at 1:50 PM, Dinis Cruz <dinis.cruz@owasp.org[31]> wrote:

[29] https://lists.owasp.org/pipermail/owasp-leaders/2011-January/004493.html
[30] https://lists.owasp.org/pipermail/owasp-leaders/2011-January/004493.html
[31] mailto:dinis.cruz@owasp.org

Hi *XYZ*, I know that we have disagreed in the past on how to best support efforts like the one you are doing, hopefully we can find some common ground on the GSD project[32] .

I've just started a new OWASP project (called GSD) that represents how I think OWASP projects can be supported by OWASP:

- OWASP GSD Project (GSD = Get Stuff Done)[33]
- Some ideas for OWASP GSD Project[34]

Note on the 'where to spend the funds' examples, that both your projects are perfect fits :)

What do you think?

Dinis Cruz

[32] https://www.owasp.org/index.php/OWASP_GSD_Project

[33] http://diniscruz.blogspot.co.uk/2012/05/owasp-gsd-project-gsd-get-stuff-done.html

[34] http://diniscruz.blogspot.co.uk/2012/05/some-ideas-for-owasp-gsd-project.html

2.4 OWASP GSD Project (GSD = Get Stuff Done)

Yesterday I started the OWASP GSD Project[35], based on:

- the ideas first presented on OWASP Project Reboot 2012 - Here is a better model[36],
- the fact that there is a good amount of funds available at OWASP (160k USD available to OWASP Chapters and Projects[37]) and
- the need that OWASP has to inject energy into its projects, .

The Project's main page is at: https://www.owasp.org/index.php/OWASP_GSD_Project[38] and below (end of this post) you will find a copy and paste of today's version of this project page (which is the first pass at defining what the GSD is)

What I like about this model is that is **as empowering as I think one can make it**.

Basically this model:

- Empowers OWASP leaders to spend funds on OWASP projects
- Puts a very 'light' moderation/control system in place, where proposals are approved by default (in 1 day for < $500 and 7 days for < $5000)
- Creates a chain of trust beween the multiple parties
- Can be this simple due to the key '*OWASP leaders cannot be paid*' rule
- It is based on trust and reputation
- It is designed to be simple to use and could be easy abused
- It is a grass-roots, bottom up approach (i.e. done from the OWASP Community to the OWASP Community)

Now you might think that such system would be abused. My experience in implementing very similar solutions (at OWASP and other places) has shown me that in an open environment, it is very hard to abuse the system in a way that doesn't (eventually) backfire.

The only places I've seem 'abuses' is when the information is not clearly presented, attributed and linked

In a way, a system like this shows how hard it is to get stuff done at an organisation like OWASP. Even when just about ALL barriers of entry are removed, and it is really simple to 'do it', it takes a lot of effort to create something.

And the reason is simple. There is always a good crowd that has 'ideas' on what should happen. But the hard part is to actually 'do it' (or create a good brief so that it can be delegated/contracted-out).

Another key concept about this model is that it is not done by the OWASP Board or Committee. I think it is very important that initiatives like this happen from the 'bottom-up' and not from the 'top-down'. That said, I

[35] https://www.owasp.org/index.php/OWASP_GSD_Project
[36] http://diniscruz.blogspot.co.uk/2012/04/owasp-project-reboot-2012-here-is.html
[37] http://diniscruz.blogspot.co.uk/2012/04/160k-usd-available-to-owasp-chapters.html
[38] https://www.owasp.org/index.php/OWASP_GSD_Project

have asked both OWASP Board and GPC (Global Projects Committee) to provide some seed funds, since that is the equivalent of directly investing on OWASP projects.

And you, dear reader (maybe from a company that likes what OWASP is doing or a leader of an OWASP Chapter), if you have funds that you would to see put to a good use , please allocated some of it to this project :)

What do you think? Any comments, ideas, criticisms, suggestions, etc...?

OWASP GSD (Get Stuff Done) project is focused on enabling and empowering other OWASP Projects with funds, resources, energy and ideas.

The first initiative is the 'Funds Available for OWASP Projects' (see details and rules-of-engagement below)

- *Project Leader: Dinis Cruz*
- *Proposals Review Team: Dennis Groves, Daniel Cuthbert, Dinis Cruz ... (more to be announced)*

Initiative: Funds Available for OWASP Projects

***What**: OWASP Project Sponsorship model where OWASP Leaders can spend up-to the current allocated budget on OWASP Projects*

***Rules-of-Engagement**:*

- *Funds are to be used on OWASP Projects*
- *Funds to be personally allocated by an OWASP Leader (who takes responsibility for its use and execution)*
- *OWASP leaders are free to spend the funds on OWASP Projects in anyway they feel relevant, with only the following KEY restrictions:*
  - *They can't pay another OWASP leaders or a company that an OWASP leader is directly connected to*
  - *For amounts less than $500 they add its description to the respective OWASP WIKI page 24h before they commit to make the expense*
  - *For amounts less than $5000 they add its description to the respective OWASP WIKI 7 days before they commit to make the expense*
  - *If there are no comments or objections by the 'Proposals Review Team', the funds are automatically approved*
  - *If a member of the 'Proposals Review Team' objects or asks for more information, the funds are NOT approved (until further clarifications)*
- *Each expense item is mapped to an individual OWASP leader and multiple OWASP Leaders can work together.*
- *Payments will be made by Alison on Invoice submission (by paypal or direct bank transfer)*

In 6 months time, a review of the outcomes will be done and see these rules need to be changed

Current Funds Available

- *Total: 0 USD*
- *Sponsors: none yet (these could be OWASP Chapters, OWASP Members or 3rd party companies/organizations)*

Proposed Use of Funds Available

- *None*

FAQ

For Participants:

- ***What is an OWASP Leader?** : Everybody in the owasp-leaders list*
- ***Can these funds be used on other OWASP innitiatives (Chapters, Conferences, Summits, etc..)** : Nope this is only for OWASP Projects*
- ***What happens if the 'Proposals Review Team' objects or asks questions** : The OWASP Leader behind the proposal needs to come back with a better idea or answer :)*
- ***Is there some kind of 'Gamification[39] theory' behind this idea?** : Yes :)*

_
_*For Members of the 'Proposals Review Team':*

- ***What should I do if I like a proposal?** : Nothing (unless you have time to help that proposal). Note that proposals with no 'doubts' are approved by default*
- ***What should I do if I have doubts about a proposal?** : Write a comment and raise your doubts/questions. Note that proposals with (at least one) 'doubt' comment and NOT approved by default*

_
__
_

[39] http://en.wikipedia.org/wiki/Gamification

2.5 OWASP Project Reboot 2012 - Here is a better model

In the last ROI on OWASP investment on Projects (ie paying leaders)[40] post I mentioned that we need a better model to empower OWASP leaders with available funds (which seem to be at the moment about 100,000 USD)

My proposal / idea is to create a OWASP Project Sponsorship model based on these following simple rules:

- OWASP makes available a budget for OWASP Projects (for example 100k)
- OWASP leaders are free to use that money in anyway they want, with only the following restrictions:
  - They **can't pay another OWASP leader**s or a company that an OWASP leader is directly connected to
  - For amounts** less than $500** they add its description to the respective OWASP WIKI page **24h** before they commit to make the expense
  - For amounts** less than $5000 **they add its description to the respective OWASP WIKI **7 days** before they commit to make the expense
  - Each **expense item is mapped to an individual OWASP leader** and multiple OWASP Leaders can work together.
  - **Payments **will be made by Alison **on Invoice submission** (by paypal or direct bank transfer)
- After the budget is spent (or in 6 months time), OWASP will review the outcomes and see if these rules need to be changed

And that's it!

This will allow the OWASP leaders (of any type) to just get on with it and find the best ways to take OWASP projects to the next level.

After you read this idea, take a look at the current Project Reboot Proposal[41] at the OWASP Wiki.

From my point of view, there are a number of problems with that proposal:

- **It allows the payment of OWASP leaders** (see Why OWASP can't pay OWASP Leaders[42] for a list of reasons why this is a bad idea)
- **It doesn't learn from the past and all the hard work that went into the OWASP Season Of Code (SoC) concept** - This proposal is basically OWASP SoC 2012, so at least least reuse what has been done before: https://www.owasp.org/index.php/Category:OWASP_Season_of_Code[43]
- **It puts the barrier of entry as an OWASP Membership (which is a 50USD registration)** - I would put this barrier of entry at OWASP Leader level, since those are individuals that have earned OWASP's trust and have delivered (note that the issue of *'does an OWASP leader deserve to be OWASP leader'* is a separate thread)
- **There are a lot of pieces missing** - If we are going down this path (which again is OWASP SoC 2012), then we will need to be as transparent and efficient as the last OWASP SoC. To get a better picture of what will need to be done, spend some time with the amazing pages that Paulo Coimbra (and the GPC) created on https://www.owasp.org/index.php/Category:OWASP_Season_of_Code[44] (for example

[40] http://diniscruz.blogspot.co.uk/2012/04/roi-on-owasp-investment-on-projects-ie.html
[41] https://www.owasp.org/index.php/Projects_Reboot_2012
[42] http://diniscruz.blogspot.co.uk/2012/04/roi-on-owasp-investment-on-projects-ie.html
[43] https://www.owasp.org/index.php/Category:OWASP_Season_of_Code
[44] https://www.owasp.org/index.php/Category:OWASP_Season_of_Code

a lesson learned from past SoC is that all proposals must be submitted via the OWASP wiki)

- **There is no Project Manager - **Investing in OWASP projects in this way is a full time job. The first step should be to hire a project manager to work on this (one of the beauties of the model I propose above is that is much lighter to implement (since there is a high degree of self control)

Finally, don't get me wrong! Investing on OWASP's projects is one of most important things that OWASP needs to do, and if the Project Reboot Proposal[45] is approved, we will be better than we were before.

The reasons for this post, is that I just think there is a better and simpler way of doing it :)

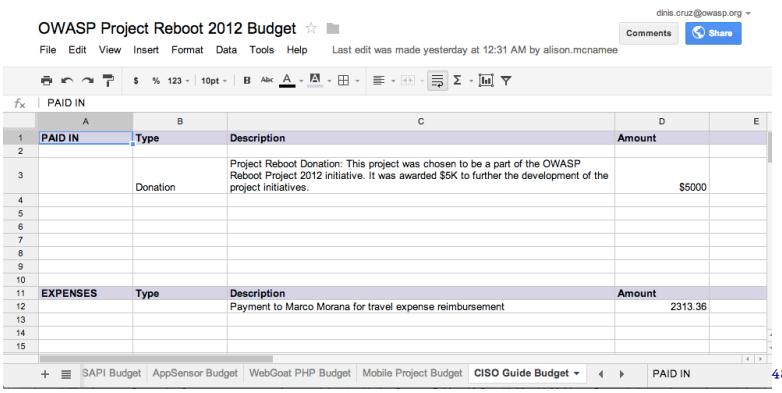
[45] https://www.owasp.org/index.php/Projects_Reboot_2012

2.6 OWASP project reboot spent funds (not a lot spent so far)

From Alison here are the latest numbers from the OWASP Project Reboot 2012[46] initiative:

- Project reboot funds/expenses[47] in a Google Spreadsheet

Humm, from the numbers in there, it looks like only the ***CISO Guide*** spent some funds



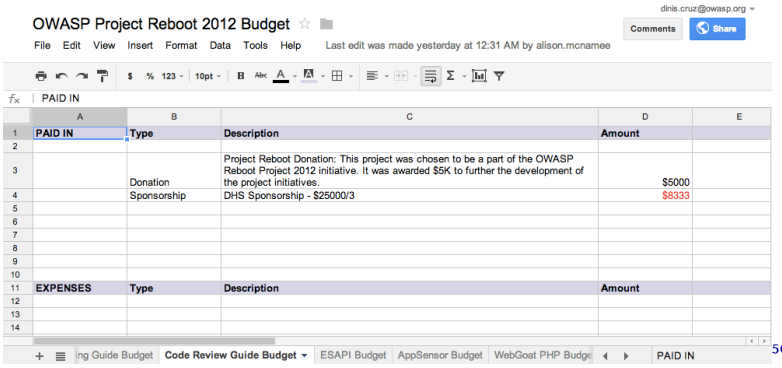
[48]

If true, and as we reach the 6 months of the allocation of those funds, the interesting question to ask is : WHY?

Why havent these funds been spent?

I think part of the answer can be found at OWASP Revenue Splits and the "Non-profits have a charter to be innovators"[49]

One interesting development (and potential issue) is the case with the DHS funded projects (like the **_Code Review Guide** _shown below), which have an expectation to deliver something:



[50]

[46] https://www.owasp.org/index.php/Projects_Reboot_2012
[47] https://docs.google.com/a/owasp.org/spreadsheet/lv?key=0AllOCxlYdf1AdHJWMlMyemwzbWNkbV9Uczd4bjVhb1E
[48] http://2.bp.blogspot.com/-F0tEqa4dPYM/UMrhf2WUjtI/AAAAAAAAHI4/P_xBVQ8G4Wc/s1600/Screen+Shot+2012-12-14+at+08.20.46.png
[49] http://blog.diniscruz.com/2012/12/owasp-revenue-splits-and-non-profits.html
[50] http://3.bp.blogspot.com/-NLg3pLbWvNA/UMrjDnHUHDI/AAAAAAAAHJA/IbYPU55ckdY/s1600/Screen+Shot+2012-12-14+at+08.26.54.png

2.7 Project Management at OWASP

What OWASP needs ASAP is Project Management (the type Paulo was doing).

In fact, we don't need 1, we need 4 or 5 project managers….

But I will settle for one in the short term,

There is a HUGE amount of work that needs to be done by the OWASP Operational machine, and THAT is where we (OWASP) needs to be putting our resources (i.e. creating the 'OWASP Platform') .

**At the moment we (OWASP) can't even accept and guide projects that want to become OWASP projects!!! **And let's not forget the 'huge' (i.e. none) support we give our current projects leaders (Hey !..I'm one of those OWASP Leaders that feels quite abandoned at a conner of the OWASP Project's landscape…)

In fact, the other two tragedies (and losses for owasp) are when regular OWASP contributors and members of our community:

- choose NOT to host their projects at OWASP, because they see no value in doing that!
- choose NOT to join an OWASP projects and contribute, because they don't know how, there is nobody on the other side, or the project is a mess and not easy to see where to start!

And being harsh on us (since we need to), why should they move their project to OWASP or Contribute? It's too much hard work, there are two many politics, emails don't get answered, etc…

We (i.e. OWASP) treat our project leader as dirt, we don't know who they are, we don't give them any support, we might even (if some OWASP conference organizers have their way) ask them to pay an entrance fee at our conferences (so that they (the project leaders) become a profit center).

This needs to change!!!

Our leader (projects, chapters, conferences, etc…)** are our most valuable asset, and we (OWASP) need to hire the resources** (i.e. project manager)** required to deal with them in the most professional, cordial, quick and focused way** (which is what Paulo was doing (and Kate, Sarah, Allison , Kelly do every day))

2.8 ROI on OWASP investment on Projects (ie paying leaders)

I was thinking about the crazy idea of paying OWASP leaders[51] (still supported by a number of OWASP leaders) and I started wondering what was the ROI (Return of Investment) for OWASP and its community when OWASP did pay OWASP leaders (existing and new ones) to work.

For reference here are the projects sponsored in the past:

OWASP Autumn Of Code 2006[52] - 34,000$ USD invested on :

- WebScarab NG[53] ,
- Live CD[54] ,
- CAL9000[55] ,
- SiteGenerator and ORG[56] ,
- Pantera[57] ,
- Web Goat[58] ,
- Testing Guide[59] ,
- OWASP .NET Tools[60] ,.
- OWASP Website and Branding[61]

OWASP Spring Of Code 2007[62] - 117,500$ USD invested on:

- The OWASP Web Security Certification Framework[63] ,
- SqlMap[64] ,
- OWASP Site Generator[65] ,
- Attacks Reference Guide[66] ,
- The Scholastic Application Security Assessment Project[67],
- Inspekt: Input filtering and validation library for PHP[68] ,
- Code review Project[69] ,

[51] http://why%20owasp%20can%27t%20pay%20owasp%20leaders/
[52] https://www.owasp.org/index.php/OWASP_Autumn_Of_Code_2006
[53] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Projects:_WebScarab_NG
[54] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Projects:_Live_CD
[55] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Projects:_CAL9000
[56] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Projects:_SiteGenerator_and_ORG
[57] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Projects:_Pantera
[58] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Projects:_Web_Goat
[59] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Projects:_Testing_Guide
[60] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Projects:_Owasp_.Net_Tools
[61] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Projects:_Website_and_Branding
[62] https://www.owasp.org/index.php/OWASP_Spring_Of_Code_2007
[63] https://www.owasp.org/index.php/SpoC_007_-_The_OWASP_Web_Security_Certification_Framework
[64] https://www.owasp.org/index.php/SpoC_007_-_SqlMap
[65] https://www.owasp.org/index.php/SpoC_007_-_OWASP_Site_Generator
[66] https://www.owasp.org/index.php/SpoC_007_-_Attacks_Reference_Guide
[67] https://www.owasp.org/index.php/SpoC_007_-_The_Scholastic_Application_Security_Assessment_Project
[68] https://www.owasp.org/index.php/SpoC_007_-_Inspekt
[69] https://www.owasp.org/index.php/SpoC_007_-_Code_review_Project

- OWASP Certification Project[70] ,
- OWASP Education Project[71] ,
- OWASP The Anti-Samy Project[72] ,
- Security throughout the SDLC[73] ,
- OWASP WebGoat Solutions Guide[74] ,
- OWASP WeBekci Project[75] ,
- Python Tainted Mode[76] ,
- WebScarab NG Security Test Automation[77] ,
- Refresh Attacks list[78] ,
- Best Practices & Countermeasures[79] ,
- OWASP brand[80] ,
- Web Application Security put into practice[81] ,
- OWASP JBroFuzz Project[82] ,
- Owasp Orizon Project[83] ,
- Enigform: Firefox Addon for OpenPGP signing of HTTP requests[84] ,
- OWASP LiveCD Education Project[85] ,
- OWASP Java Project[86] ,
- OWASP LiveCD Project[87] ,
- Interim @ Aspect Offices[88] ,
- Help with SpoC project management[89] ,
- OWASP Corporate Application Security Rating Guide[90]

OWASP Summer of Code 2008[91] $104,000 USD invested on

- 100% Completion

[70] https://www.owasp.org/index.php/SpoC_007_-_OWASP_Certification_Project
[71] https://www.owasp.org/index.php/SpoC_007_-_OWASP_Education_Project
[72] https://www.owasp.org/index.php/SpoC_007_-_OWASP_The_Anti-Samy_Project
[73] https://www.owasp.org/index.php/SpoC_007_-_Security_throughout_the_SDLC
[74] https://www.owasp.org/index.php/SpoC_007_-_OWASP_WebGoat_Solutions_Guide
[75] https://www.owasp.org/index.php/SpoC_007_-_OWASP_WeBekci_Project
[76] https://www.owasp.org/index.php/SpoC_007_-_Python_Tainted_Mode
[77] https://www.owasp.org/index.php/SpoC_007_-_WebScarab_NG_Security_Test_Automation
[78] https://www.owasp.org/index.php/SpoC_007_-_Refresh_Attacks_list
[79] https://www.owasp.org/index.php/SpoC_007_-_Best_Practices_%26_Countermeasures
[80] https://www.owasp.org/index.php/SpoC_007_-_OWASP_Brand
[81] https://www.owasp.org/index.php/SpoC_007_-_Web_Application_Security_put_into_practice
[82] https://www.owasp.org/index.php/SpoC_007_-_OWASP_JBroFuzz_Project
[83] https://www.owasp.org/index.php/SpoC_007_-_Owasp_Orizon_Project
[84] https://www.owasp.org/index.php/SpoC_007_-_Enigform:_Firefox_Addon_for_OpenPGP_signing_of_HTTP_requests
[85] https://www.owasp.org/index.php/SpoC_007_-_OWASP_LiveCD_Education_Project
[86] https://www.owasp.org/index.php/SpoC_007_-_OWASP_Java_Project
[87] https://www.owasp.org/index.php/SpoC_007_-_OWASP_LiveCD_Project
[88] https://www.owasp.org/index.php?title=SpoC_007_-_Interim_@_Aspect_Offices&action=edit&redlink=1
[89] https://www.owasp.org/index.php/SpoC_007_-_Help_with_SpoC_project_management
[90] https://www.owasp.org/index.php/SpoC_007_-_OWASP_Corporate_Application_Security_Rating_Guide
[91] https://www.owasp.org/index.php/OWASP_Summer_of_Code_2008

- OWASP Testing Guide v3[92]
- OWASP Ruby on Rails Security Guide v2[93]
- OWASP Live CD 2008 Project[94]
- OWASP Code review guide, V1.1[95]
- OWASP AntiSamy .NET[96]
- OWASP .NET Project Leader[97]
- OWASP Source Code Review OWASP Projects[98]
- OWASP AppSensor - Detect and Respond to Attacks from Within the Application[99]
- OWASP Backend Security Project[100]
- OWASP Securing WebGoat using ModSecurity[101]
- OWASP Teachable Static Analysis Workbench[102] Dmitry Kozlov[103]
- OWASP Access Control Rules Tester[104]
- OWASP Skavenger[105] Matthias Rohr[106]
- OWASP Online code signing and integrity verification service for open source community (OpenSign Server)[107]
- OWASP Code Crawler[108]
- OWASP OpenPGP Extensions for HTTP - Enigform and mod_openpgp[109]
- OWASP Application Security Verification Standard[110]
- OWASP Classic ASP Security Project[111]
- OWASP UI Component Verification Project (a.k.a. OWASP JSP Testing Tool)[112]
- OWASP SQL Injector Benchmarking Project (SQLiBENCH)[113]
- OWASP Spanish Project[114]
- OWASP Internationalization Guidelines Project[115]
- GTK+ GUI for w3af project[116]

[92] https://www.owasp.org/index.php/Category:OWASP_Testing_Project
[93] https://www.owasp.org/index.php/Category:OWASP_Ruby_on_Rails_Security_Guide_V2
[94] https://www.owasp.org/index.php/Category:OWASP_Live_CD_2008_Project
[95] https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
[96] https://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project_.NET
[97] https://www.owasp.org/index.php/Category:OWASP_.NET_Project#OWASP_.NET_Project_Leader
[98] https://www.owasp.org/index.php/Category:OWASP_Source_Code_Review_OWASP_Projects_Project
[99] https://www.owasp.org/index.php/Category:OWASP_AppSensor_Project
[100] https://www.owasp.org/index.php/Category:OWASP_Backend_Security_Project
[101] https://www.owasp.org/index.php/Category:OWASP_Securing_WebGoat_using_ModSecurity_Project
[102] https://www.owasp.org/index.php/Category:OWASP_Teachable_Static_Analysis_Workbench_Project
[103] mailto:ddk(at)cs.msu.su
[104] https://www.owasp.org/index.php/Category:OWASP_Access_Control_Rules_Tester_Project
[105] https://www.owasp.org/index.php/Category:OWASP_Skavenger_Project
[106] mailto:mro(at)securenet.de
[107] https://www.owasp.org/index.php/Category:OWASP_OpenSign_Server_Project
[108] https://www.owasp.org/index.php/Category:OWASP_Code_Crawler
[109] https://www.owasp.org/index.php/Category:OWASP_OpenPGP_Extensions_for_HTTP_-_Enigform_and_mod_openpgp
[110] https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
[111] https://www.owasp.org/index.php/Classic_ASP_Security_Project
[112] https://www.owasp.org/index.php/Category:OWASP_JSP_Testing_Tool_Project
[113] https://www.owasp.org/index.php/Category:OWASP_Sqlibench_Project
[114] https://www.owasp.org/index.php/OWASP_Spanish
[115] https://www.owasp.org/index.php/OWASP_Internationalization
[116] https://www.owasp.org/index.php/Category:GTK_plus_GUI_for_w3af_Project

- OWASP Book Cover & Sleeve Design[117]
- OWASP Individual & Corporate Member Packs, Conference Attendee Packs Brief[118]
- Above 50% Completion
  - OWASP Orizon Project[119]
  - OWASP Application Security Desk Reference (ASDR)[120]
  - OWASP Application Security Tool Benchmarking Environment and Site Generator refresh[121]
  - OWASP Education Project[122]
  - OWASP Python Static Analysis[123]
- Below 50% Completion
  - OWASP WeBekci Project[124] Bunyamin Demir[125]
  - OWASP Positive Security Project[126]

As you can see there were a LOT of projects that OWASP sponsored

From a pure ROI point of view, we need to ask: "**How many of these projects are successful (or even active) today?**" and "**How much impact did these this investment actually had?**"
**
**

If we look purely from a project deliverables point of view, although there were a number of solid deliveries I think one will struggle to come up with a positive balance (specially since some of the best things done to these projects happened after this sponsorship).

But if we look at this from the point of view of:

- Bringing new energy to OWASP (namely OWASP leaders)
- Improve the research on WebAppSecurity
- Improving the connections and relationships between these OWASP Leaders
- Empowering these OWASP Leaders to be involved in other areas (and projects) at OWASP (note how a lot of the most active OWASP leaders today were involved)
- Creation of new Chapters (directly connected to a sponsored OWASP leader) , with some of these chapters also eventually organizing OWASP Conferences

I would say that the balance is massively positive!

So the question is: ***"if we want to achieve similar results today, should we pay OWASP leaders again or do something different?"***

[117] https://www.owasp.org/index.php/Category:OWASP_Book_Cover_%26_Sleeve_Design
[118] https://www.owasp.org/index.php/Category:OWASP_Individual_and_Corporate_Member_Packs_plus_Conference_Attendee_Packs_Brief
[119] https://www.owasp.org/index.php/Category:OWASP_Orizon_Project
[120] https://www.owasp.org/index.php/Category:OWASP_ASDR_Project
[121] https://www.owasp.org/index.php/Category:OWASP_Application_Security_Tool_Benchmarking_Environment_and_Site_Generator_Refresh_Project
[122] https://www.owasp.org/index.php/Category:OWASP_Education_Project
[123] https://www.owasp.org/index.php/Category:OWASP_Python_Static_Analysis_Project
[124] https://www.owasp.org/index.php/Category:OWASP_WeBekci_Project
[125] mailto:bunyamin@owasp.org
[126] https://www.owasp.org/index.php/Category:OWASP_Positive_Security_Project

**

**

My view is that we need a new model, one that is based on the concept that 'OWASP cannot pay for OWASP leaders' and focused on empowering those leaders.

For more on this topic see:

- Why OWASP can't pay OWASP Leaders[127]
- Project Management at OWASP[128]
- Why large OWASP projects start to stale (and who should pay for the work)[129]
- OWASP: Proposed change for SoC: Use budget to pay for project related expenses[130] (from 2009)

[127] http://diniscruz.blogspot.co.uk/2012/04/why-owasp-cant-pay-owasp-leaders.html
[128] http://diniscruz.blogspot.co.uk/search/label/OWASP
[129] http://diniscruz.blogspot.co.uk/search/label/OWASP
[130] http://diniscruz.blogspot.co.uk/2009/06/owasp-proposed-change-for-soc-use.html

2.9 Some ideas for OWASP GSD Project

When I started talking about the OWASP GSD Project (GSD = Get Stuff Done)[131] , with fellow OWAPS leaders, one of the questions I received was_ 'Ok so where will the money be used?'_

The concept of GSD is to empower the OWASP Leaders to spend on OWASP projects, so in way the _'what would it be be used for' _will be defined by them (the OWASP Leaders).

If you are an OWASP Leader, you are the one that will be empowered to spend GSD funds, so look in the mirror and ask yourself the question _'Where would I spend funds on OWASP Projects' _:) .

Here are a couple ideas on where to use available GSD funds:

- buy 20 copies of the (for example) Open SAMM book and distribute it at a local OWASP chapter meeting
- support the OWASP Developer Guide and ASVS projects (for example with copywriting, formatting, design, research, proof-reading, pagination, etc...)
- improve the formatting and presentation of the 'Cheat-Sheet' series,
- hire a transcription service for key presentations done at OWASP chapters/events (or OWASP PodCasts)
- create a DVD with all presentations from a specific OWASP event (or other video materials like the AppSec tutorial series)
- sponsor a booth at an event to present OWASP Projects
- sponsor travel expenses for a project leader to meet with other project leaders or collaborators (to work on a particular project)
- organize a mini-summit around an OWASP project
- create a mini-website focused on a particular project (like ESAPI.org)
- try out a specific commercial service that will make a particular project more effective (version control, bug tracking system, mailing lists, etc...)
- hire designers to work on OWASP projects
- translate OWASP content (to and from English)
- sponsor students to work on OWASP projects (maybe even run a mini-OWASP Season of Code)
- hire mediawiki editors for the OWASP website (the OWASP projects part of it :))
- hire project manager(s) for OWASP projects
- etc...

What I've found is that unless we remove just about all barriers of entry for the use of Funds on an OWASP project, what tends to happen is 'Nothing'.

Hopefully the GSD project will help in Getting Stuff Done :)

[131] http://diniscruz.blogspot.co.uk/2012/05/owasp-gsd-project-gsd-get-stuff-done.html

2.10 The difference between being 'Appointed' and being 'Accepted' as an OWASP Leader (of its Fork)

OWASP is a community that really embraces new ideas, new contributors and projects.

For somebody motivated (and with time/energy) there are very few 'real' barriers on entry. Even the cases where it 'feels' like there are barriers of entry or 'bureaucracy', those are mainly artificial and easy bypassed (with the right level of energy and commitment)

The problem is ***Empowerment***

What I found (by observing lots of OWASP projects starting, blossoming and dying) is that what makes the difference is how ***Empowered*** is an individual on a particular project/tasks.

The easiest scenario is when a new project is born, since by default the person motivated to launch it, will feel ***empowered*** to do work on that project.

But when we get into contributing/collaborating with other projects, or in dealing with community matters (like what the OWASP Committees try to address), it gets more complicated, since there is an invisible barrier that most don't want to cross.

Although the default answer at OWASP to people with ideas is *"why don't you go and do it yourself"*, what actually tends to happen is: **Nothing **(or very little)

And yes, OWASP does have a problem with the *'...yes I can help...'* brigade, which are the ones that are first to offer to help, but seldom do any actual work (in most cases these 'non-helpers' are neutral, since they don't have an significant impact (positive or negative)).

For me, the the real problem is one where the candidate (current or future OWASP leader) '*feels*' that he/she needs to be '***Appointed***'

I think it is human nature that creates the '*need*' to feel that one is allowed to touch/change a particular project. And since there isn't a direct effort to tackle that '*need*', we go back to the default outcome which is: **Nothing **(or very little).

And what a great tragedy it is, when you have somebody who wants to work, wants to learn, wants to contribute, wants to change, but somehow the initial spark fails to happen, and that energy/focus is lost.

There were four cases where I really saw this in action.

1. the OWASP Seasons of Code[132]
2. the OWASP Summits[133]
3. the OWASP Committees[134] (created in the first Summit)
4. creating a web page in the OWASP wiki

In all these cases, all that it took for a huge amount of energy (and work) to happen on particular project (or area) was for somebody to have his/her idea 'accepted' in the public sphere

[132] https://www.owasp.org/index.php/OWASP_Summer_of_Code_2008
[133] https://www.owasp.org/index.php/Summit_2011
[134] https://www.owasp.org/index.php/Global_Committee_Pages

- the Season of Code participants (which would had made more money flipping burgers) felt empowered to participate and contribute to a particular project or idea
- the OWASP summits, that where designed around the idea of 'working sessions', which made the participants fell empowered on these 'working sessions' topics
- the committees which (initially) empowered existing OWASP leaders to tackle a huge amount of OWASP related issues (Projects, Conferences, Chapters, Membership) and outreach efforts (Industry, Education, Connections)
- the magic sparkle and empowerment that happens when an owasp leaders/contributor sees a webpage in owasp.org with his name

The problem with these activities is that they are very 'top down' and rely on an 'higher authority' to do the '***Appointments***'.

Which means that when that when the '***Appointments'*** stop, (in 95%+ of cases) the ***Empowerment*** and energy stops.

In fact, what happens after a while, is that we have a perverse model where the people appointed have run out of energy,ideas or time, but still have the role, which now prevents new blood from taking over. The current state of the Committees are a great case study of this. Most are just about dead (and the ones that are not, are being driven by external events: Conferences, an election a new project manager, etc...), but since there a '*felling*' that '*somebody in charge*' there isn't the urgency (and awareness) that really important areas for OWASP (and AppSec) are currently (for all practical purposes) stopped and leaderless

The problem is that OWASP at the moment doesn't do a *'Spring Clean'* of leaderships and '***Appointments***', which means that although it is **easy to get in**, it is very **hard to get out **(and it takes a lot to step down from a Leadership position). Humm ... maybe at the next OWASP Band we should play the *Hotel OWASP* to the tune of *Hotel California* :)

In my view, the solution is to:

- re-invent the OWASP committees as OWASP Initiatives[135] (which are focused on empowering specific tasks)
- remove all project leaders that have been on a project, initiative, committee but have done nothing (measurable) in the last 6 months (a good test is just to ask: '*Dear project leader XYX, what have you done for the project/initiative/committee ABC over the last 6 months.'*).

The removal of the OWASP leaderships is very important, since the dark side of **_Appointing** _leaders, is that while they are there, it is quite toxic (and political) for somebody else to 'step-up' and start doing something about that project (i.e. most don't want to buy that fight, or have the time to deal with the political implications/BS).

And this takes me to the real idea behind this post:

The difference between being '*Appointed*' and being '*Accepted*' as an OWASP Leader (of its Fork)

What we want is a situation where members of the OWASP community fell empowered to Fork (i.e take ownership) a particular project or idea.

[135] https://www.owasp.org/index.php/OWASP_Initiatives_Global_Strategic_Focus

Then, the real '***Appointment***' happens by the community that recognises his/hers ideas, and accepts the vision followed/executed (with eventually that person becoming the 'project leader').

This is much more healthier and risk-free than the current '*Appointment*' model since, if that person fails to deliver, the loss is minimal

Also important is the fact that this 'Forking' allows for multiple simultaneous attempts/efforts by different participants. Which maximizes the changes of success.

Compare that with the current '***Appointment***' model, which by design choses one path/person vs another one (unless all candidates are accepted), and removes energy/***Empowerment*** from the 'losing' parties.

For more thinking on the *'Fork projects or content'* idea see the Design for Fork and the liquididy of OpenSource/Git[136] post.

Linus has shown us that Forking is the way to create a community around code. **Now we need to use the same principles of Forking to create vibrant communities OWASP projects and activities**

[136] http://diniscruz.blogspot.co.uk/2012/09/design-for-fork-and-liquididy-of.html

2.11 Why large OWASP projects start to stale (and who should pay for the work)

A critical evolution-stage that is happening with a significant number of OWASP (and other FOSS) projects is the moment when the project grows so large that any key change requires a substantial amount of work.

Another problem is the fact that most successful projects are the result of only a small number of key contributors (also called the projects-leader) who after a significant personal time-commitment, move on into other projects/initiatives/ideas.

Most of our guides have that problem, so does WebGoat, WebScarab, ESAPI, O2, etc…

In fact, for a while there was a lot of effort put into 'normalizing' the references between the multiple guides, which is A MASSIVE piece of work (btw, this probably can only be done if you got 5 to 10 key players in the same location for 1 week (with a good amount of preparation work)).

It is just a reality that when OpenSource projects grow, they need commercial support that pays for contributors to work on it.

And here is the catch, OWASP can't be the one that pays for it (it can pay for the operational support, project management, mini-summits, infrastructure, etc.. but not the salaries of the contributors).

It should be the companies (or groups) that benefit from that project that should come up with the money and hire the key contributors.

In fact, that already happens a lot today at OWASP. There are a huge amount of OWASP contributions that is already funded by commercial companies that get value from those projects.

In a way we just need to formalize and operationalize this model.

3 OWASP Summits

This section has the following chapters:

- Great description of why OWASP Summits are special[1]
- I want to vote for a Summit Team and Vision , NOT for a venue[2]
- OWASP Flight Booking using Amex and Project's Mini-Summit at OWASP AppSec USA 2013[3]
- Some proposed Visions for next OWASP Summit[4]
- Summits must be part of_OWASP's DNA[5]
- When is the next OWASP Summit?[6]

Table of Contents[7]

[1] /manuscript/3.OWASP_Summits/Great_description_of_why_OWASP_Summits_are_special.md
[2] /manuscript/3.OWASP_Summits/I_want_to_vote_for_a_Summit_Team_and_Vision_,_NOT_for_a_venue.md
[3] /manuscript/3.OWASP_Summits/OWASP_Flight_Booking_using_Amex_and_Project's_Mini-Summit_at_OWASP_AppSec_USA_2013.md
[4] /manuscript/3.OWASP_Summits/Some_proposed_Visions_for_next_OWASP_Summit.md
[5] /manuscript/3.OWASP_Summits/Summits_must_be_part_of_OWASP's_DNA.md
[6] /manuscript/3.OWASP_Summits/When_is_the_next_OWASP_Summit.md
[7] ../../Table_of_Contents.md

3.1 Great description of why OWASP Summits are special

Abe (on the owasp-leaders list) just posted the text below in response to my Summits must be part of OWASP's DNA[8] reply and it provides one of the best descriptions of what makes Owasp Summit's special and worthwhile doing (please read it).

If you've never been to one of our Summits, this is why they are so important and necessary (Imagine what we could achieve with regular Summits) On 6 Apr 2012, at 18:14, Abraham Kang <abraham.kang@owasp.org[9]> wrote:

> Although, I agree with Jim in spirit.
>
> I have to admit that I was able to get things accomplished at the 2011 Summit that would have taken longer had I not attended the Summit.
>
> I was kind of Stuck on the DOM based XSS cheat sheet because there were just so many existing ways and new ways of exploiting DOM based XSS. I was lost in trying to understand the exploiting instead of focusing on the Mitigating.
>
> The Summit gave me an opportunity to work with some of top guys (Jim Manico, Stefano Di Paola, Robert Hansen, Gareth Hazes, Chris Schmidt, Mario Heiderich, Eduardo Nava, Achim Hoffman, John Stevens, Arian Evans, Mike Samuel, Jeremy Long, Dinis Cruz, and others please forgive me if I forgot to mention you) in Web security to get their ideas and refine mine.
>
> I also was able to bring up issues that were affecting adoption by large enterprises of OWASP materials with Jeff Williams and others.
>
> Finally, I was also able to meet the people interested in OWASP Web Development Guide (which I have been trying to reboot but having started a new job have failed to make much progress on) to discuss issues related to the guide and try to address them.
>
> All of this would have been impossible to do without the summit.
>
> I was also hoping to suggest that this year we try to bring other security members of the community that haven't traditionally participated (iSec Partners, Gotham Digital Science, etc.) in OWASP to the summit as I have great respect for those guys and think they could contribute greatly to the success of OWASP.
>
> The conference is viewed as being private but I thought it was open to anyone interested in contributing to OWASP. I think people would be willing to pay to attend a conference where they could speak to other leaders in informal meetings on topics of interest and provide the additional benefit of OWASP deliverables.

[8] http://diniscruz.blogspot.co.uk/2012/04/summits-must-be-part-of-owasps-dna.html
[9] mailto:abraham.kang@owasp.org

We are a very disperse group, it helps to get people together to work things out, discuss and see the other people as human beings. I have to admit that the conference was also a lot of fun. I got to laugh with people I would have never had the chance to before this. Jokes don't seem to go over as well when they are made over email. I got to hear stories of (Larry's or Chris's – the last names have been omitted to protect the Guilty) midget experiences/encounters. I got to know of other people skeleton's in their closets.

This allowed all of us to bond in a way that couldn't happen without a conference like this.

Another benefit of these types of interactions is that everyone that attended last summit was involved with an OWASP project (which may be a good requirement). I met Andras (my German brother) of WS-Attacks.org[10] and although I haven't done a good job of it yet, I was hoping to reboot the OWASP Web Development Guide (I will send another email on that thread to explain my struggles) and see if I could use the content from WS-Attacks.org[11] in the new guide (seeing as I did the translation revision for Andras) for the Web Services chapter. If I didn't attend the Summit I wouldn't have met him and made this connection.

Yes there were a couple of things that could have been handled better related to the usurping of funds from individual Chapter's accounts and we probably could have spent less money on the incidentals but there is great value in the Summit.

OWASP Rocks!

Warmest Regards,

Abe

Sorry for being so long winded.

[10] http://ws-attacks.org/
[11] http://ws-attacks.org/

3.2 I want to vote for a Summit Team+Vision , NOT for a venue

I wrote the text below in 11/Mar/12 and sent it originally to the OWASP Summit 2013 mailing list (you can see some comments to it there[12]) and with the recent Cancelation of the OWASP Summit 2013[13] announcement, I wanted to write a number of blog posts about OWASP Summits (so here is the first one)

Subject: I want to vote for a Summit Team+Vision , NOT for a venue

Following the Summit call on Friday I finally realized what was worrying me with the current Summit 2013 planning process: **we are being asked to vote/select a venue, before we have chosen: **

- **a) who is going to lead the summit team**,
- **b) what is its vision and **
- **c) what team/energy can they generate**.

When I asked at the end of the call *"so who is going to be the leadership team of the Summit since that should be different depending on which venue is selected?" _I got the answer "*..this time is going to be different.. this whole group (on the Summit mailing list) is that leadership team, and it doesn't matter where the venue is, once it is chosen, we are all in charge..."_

Now I am the first to want open solutions, **but you don't organize a Summit by Committee** (in fact you don't even do it for conferences, chapters or projects).

There needs to be a core leadership team (1 to 4) that is all in sync with their vision for the Summit. Of course that we want as many OWASP leaders to be involved, BUT, there needs to be a core team with the vision and authority to make decisions, mainly because some of the decisions cannot be realistically made by a bigger group (not to say that the bigger group shouldn't be involved, but there are moments when decisions need to be made, and not everybody will have the same opinion/vision on the best course of action).

Just to be clear this is what I would like to be asked to vote on.

A 'Summit Proposal' with:

- **Summit Leadership Team **(1 to 4) who are responsible for defining and executing a proposed vision for the Summit (see below)
- **Local Summit Team **(5++) who COMMIT to going to the Summit
- **Remote Summit Team **(5++) who cannot go to the Summit but will help remotely (before, during, after) and even might try to organize a local (to them) event (Seba's idea of other simultanious mini summits)
- **Advisory Team and Working Sessions Champions** (5++) responsible for providing advice to the Summit Team and to help with the development, promotion and (ideally) execution of the Summit's Working Session

[12] https://groups.google.com/a/owasp.org/group/owasp-summit-2013/browse_thread/thread/fff1b9a4cf1eeaad
[13] https://groups.google.com/a/owasp.org/group/owasp-summit-2013/browse_thread/thread/938e40b807dd5cd9?hl=en#

- **External (to OWASP) participants** (as many as possible) - who agree with the proposed vision and commit to going, promoting or helping
- At the last Summit we (finally) had good success at brining a good number of external (to OWASP) participants (Mozila, Microsoft, Google, etc...). A large number of them already had good ideas on '_what the next Summit should be about', _and we need to leverage these ideas and get them involved as soon as possible
- **Paid Summit Team** - professional contractors that will help to run the event (at the last Summit we had 6 external contractors + travel agency[14])
- **A vision for the Summit**:
  - What are the topics/themes?
  - What is it all about?
  - What type of venue they would like to get?
  - Where should be Summit be
- **A solution for improving the 'Summit Deliverables'**
  - This is what will survive the Summit, and we need to do a much better job at creating and promoting a number of solid+useful deliverables
  - This needs its own strategy, and should be a key reason of why we go with a specific Summit team (for example, should there be post-Summit group that stays on the venue to wrap up the deliverables?)
- **Budget and Dates**
  - How much money they would like to have from OWASP?
  - When would they like to do the summit?
  - Other sources of income

In this model, an owasp leader could be part of multiple teams (since the objective is the get the best out of available resources). For example, given their past involvement+contributions of (just to name a few) Lorna, Jason, Justin, John W, Jeff W, Colin W, Jim M, etc... , it would be crazy to not have them involved in these teams (even if only as 'advisers').

I'm very happy that after two Summits there is so much energy behind having another Summit, but we need to do this right.

Now, at the moment we have two realistic proposals for the Summit (Royal Holloway and Boat) which come from two different points of view (and visions) for what the Summit should be. The other proposals are either not realistic or too far away (we can't have a Summit that takes 20h+ to get to from Europe, US or Asia)

For the record, **I am not going to vote on the two venue proposals** since both have what I consider to be 'show stoppers'. We have talked about the positives of each venue, so there is no need to repeat them.

'Show stoppers for Royal Holloway'

- **There is no team behind this proposal **(see above)
- **There is no active participation from the London/UK chapters **(after Dennis dropped his support)

'Show stoppers for Boat Option'

[14] https://www.owasp.org/index.php/Summit_2011/External_Contractors

- **There is no team behind this proposal **(see above)
- **The venue is a 3000+ guest's hotel on water** - this will make it very difficult to re-create the Summit Experience in a boat with that size, and will mean that we will not 'own the venue'. Since even in the unlikely case that that have 300ish participants, we will still be about 10% of the venue capacity. This for example might limit our:
- **ability to bring in our own Food and Drinks - **This is very important since we know that we will need a good amount of beer (and wine) to be made available to the attendees
- **Hard Limit on start and stop of the Summit **(i.e. mandatory boarding day) - at the last two Summits we had people arriving and departing all the time (some due to other commitments and some due to missed/delayed flights)
- **No ability to have 'drop in' participants** - this is something we had a bit on the last summit (some Portuguese Government officials where there some a couple hours), and something that we should try to have a lot more in the next summit (think of special key note speakers, industry/government participants or special guests).
- **No ability to go an 'buy something that is needed ASAP' - **I lost count how many 'shopping trips' happened during the last Summits. It doesn't matter how much you plan (and we tried hard), but there is always something that is needed ASAP (from office supplies, to A3 paper, to network equipment, to medical supplies, to food, to drinks, etc …)

'Not Show stoppers but areas of concern: for Boat Option'

- '**Holiday perception**' - in addition to the fact that the argument _'…its a good holiday venue which will allow the participant partners to also attend'… _is not correct (no partners will want to attend the venue (neither will the attendees want them to go)), in the case of the boat, its 'holiday' perception actually backfires. I.e. there is good tradition to go to hotels/venues for Summits and work hard, there is less tradition to do that on boats.
- Another issue with that many people on the boat is the 'holiday atmosphere' that will exist (with 90% of the other passengers on holiday).
- Both will make it hard to justify the trip to employers
- **No experience at OWASP in doing an event on a boat** - regardless of how much research we can do before hand, as far as I know there has been no previous events organized by owasp at a boat. This menas that the number of unknowns is even bigger.

Moving forward, I think we have two options:

Option A) go with the Boat option

- Mark has done extended research on this option and as long as he takes the leadership role on the next Summit (i.e. he is one of the 'Summit Leadership Team') then we should trust him to make it a success
- Mark has extended experience and track record at delivering owasp conferences, so since he feel so strongly about the boat option, he should ge given the change

Option B) wait for a 'Summit Team+Vision' proposal (as defined above)

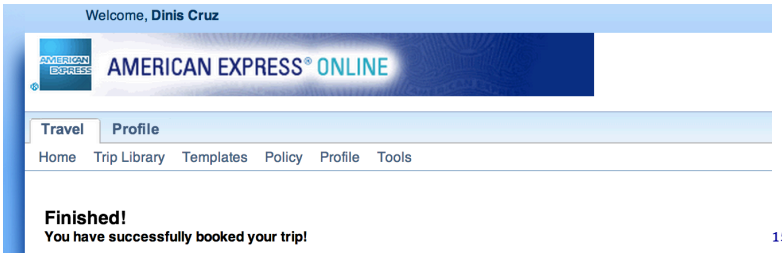
- Put a pause in the current 'Summit Venue' allocation process
- Make a public request for 'Summit Team+Vision' proposals
- Wait for those proposal to appear (wait if needed 1,2,3 or 6 months for it)
- Vote on the best one

Sorry for not raising these issues before, but only on the last couple days I was able to rationalize my worries about the current Summit 2013 process, which come down to this simple concept:

> **I want to vote on a Summit Team+Vision, not on a Venue**

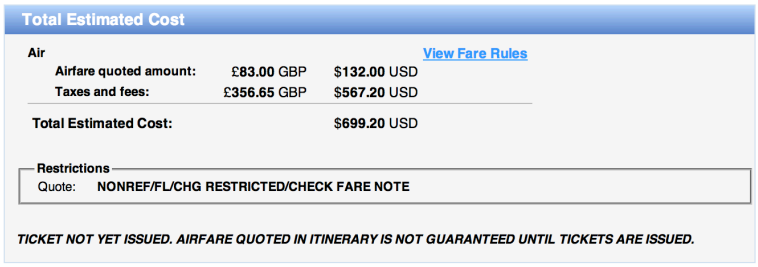
3.3 OWASP Flight Booking using Amex and Project's Mini-Summit at OWASP AppSec USA 2013

I just booked my flight using the new OWASP 'Amex travel' partnership and it was a great experience



[15]

The price is quite decent (for an transatlantic flight), and since OWASP is covering this flight I'm now very motivated to really deliver and help out during the conference :)



[16]

And what makes me really happy is how this happened!

Basically Samantha Groves[17] deserves 100% of the credit for me attending this conference (I didn't go to last year's OWASP AppSec USA), namely for finding a space for the O2 Platform at the Project's Mini-Summit that is going to happen during the conference[18] (I'm calling it a mini-summit since the format is quite different from the previous Summits) and sorting out the budget to cover my flight expenses.

This means that Samantha is (finally) being much more proactive in her role as 'OWASP Project Manager[19]' and is starting to push the OWASP Project leaders to be involved and to participate (which is what I've been asking her to do for a while, and she is finally doing it :))

**So Thanks Samantha, and please keep up the pressure for getting OWASP project leaders together, **and to expose the OWASP community to the great stuff that is happening at these OWASP Projects:

- OWASP AppSensor ,
- OWASP Code Review Guide ,
- OWASP Development Guide ,
- OWASP Training and OWASP Academies (from OWASP Education Project)
- OWASP Enterprise Security API ,

[15] http://1.bp.blogspot.com/-zLt8DDYclds/UkArsIoEvhI/AAAAAAAADgw/--fSE2hvQZM/s1600/Screen+Shot+2013-09-23+at+12.51.54.png
[16] http://2.bp.blogspot.com/-uiqpVDZAUb4/UkAr9wsO-OI/AAAAAAAADg4/62IL0G606Pw/s1600/Screen+Shot+2013-09-23+at+12.53.52.png
[17] https://www.owasp.org/index.php/User:Samantha_Groves
[18] http://appsecusa.org/2013/activities/owasp-project-summit/
[19] https://www.owasp.org/index.php/Category:OWASP_Project#tab=PM_Information

- OWASP O2 Project ,
- OWASP Open SAMM ,
- OWASP Security Principles Project ,
- OWASP Testing Guide ,
- OWASP Zed Attack Proxy (ZAP)

3.4 Some proposed Visions for next OWASP Summit

Since Summits must be part of OWASP's DNA[20] , and in case some of you are thinking of putting energy in creating the next OWASP Summit, I really think that the 'Summit Proposal' concept I detailed here[21] is a good model.

So starting from the point that first we need a strong theme/vision, here are a couple ideas:

- **OWASP Summit on OWASP Projects** - This would actually be at least one or more 'mini-Summit(s)' followed by a bigger one. The mini-summit(s) would be focused on very specific OWASP project's activities (project review, project's normalization/mapping, project XYZ, work, project's consolidation, GIT migration, etc…) with the bigger Summit the one where the results (of those mini-summits) would be presented, and the main stakeholders (i.e. the OWASP Projects users) would come together to learn, share and collaborate
- **OWASP Summit on Web Frameworks - **This would be the location where the key players of Web Frameworks (like Spring, Struts, Apache Shiro, RoR, ASP.NET[22], J2EE Stack,Grails etc…) would come together with OWASP's community, AND developers AND their 'clients'. The key objective would be to figure out how to help to make those frameworks/platforms 'secure by default' or at least to allow developers to easily code them in a secure way. In fact we could even be a bit radical and do a **OWASP Summit on Apache Shiro **(http://shiro.apache.org/[23]) since those guys are clearly doing something right and have the momentum in working with key frameworks
- **OWASP Summit on Static Analysis** - This is one that I'm specially very interested in, and would be focused on figuring a way to really make Static Analysis work in a web security world. There is so much potential with SAST technology which currently is not fulfilled because the multiple parties (from tools developers, to security consultants, to users, to clients, to regulatory bodies, etc…) are not collaborating and working together to figure out a number of Open Standards which we call all use to communicate (for example why can't we feed static analysis data to a web proxy/scanner like ZAP?)
- **OWASP Summit on Web Privacy** - Privacy is becoming more and more a big issue in the Web World, and with: a) Browsers adding features like the Do not track header[24] (http://donottrack.us/[25]), b) new laws being passed, c) recent big privacies breaches, d) governments regulatory bodies wanting to do something about it , and … {many more recent developments} … Privacy is definitely a topic which will draw a good crowd (and although one day it might be big enough to have it's own dedicated 'Brower Summit', I think in the short them, the Browser track (following the work done at the last Summit) should be part of this Summit).

Of course that there are many other hot topics or OWASP Projects we could create a Summit around (ESAPI, OpenSamm, Guide Trilogy, Cloud, DAST, Secure Coding, Code Review, PenTesting, etc…), what is needed to make it happen is a core team with passion and energy for it.

[20] http://diniscruz.blogspot.co.uk/2012/04/summits-must-be-part-of-owasps-dna.html
[21] http://diniscruz.blogspot.co.uk/2012/04/i-want-to-vote-for-summit-teamvision.html
[22] http://asp.net/
[23] http://shiro.apache.org/
[24] http://en.wikipedia.org/wiki/Do_not_track_header
[25] http://donottrack.us/

On the financial side of things, one thing that OWASP could do is to say:_ “Here is 50k seed money, the rest you need to find from other sources (including internally like OWASP Chapers)”_. And maybe even that 50k is not needed (if there is enough energy and supporters willing to buy ‘20k Summit tickets’)

3.5 Summits must be part of OWASP's DNA

[26]The last OWASP Summit 2011[27] represents the best of what OWASP can do, and nothing we did that year come even close in generating so much work, energy, serendipity and connections (not projects, chapters or conferences)

What you had there was a week of massive collaboration, relationship creation, work , brainstorming and planning (just look at this amazing picture Ofer [28], Carlos[29], Vlatko[30] (can you fell the energy!!! :)).

That Summit was not a private/closed party, just take a look at the participants again (read it slowly paying attention to the name of the attendee , it's company and reason for attending: [https://www.owasp.org/index.php/Summit*2011*_-*Attendee](https://www.owasp.org/index.php/Summit*2011*_Attendee) (even better, read their bio here[31]).

Also take a look at the planned tracks to see the wide range of topics[32] that were on the agenda. For what actually ended up as a session, see the Fixed Schedule[33] and the Dynamic Schedule[34]

[26]https://www.owasp.org/images/6/67/Final_summit_logo_half.jpg
[27]https://www.owasp.org/index.php/Summit_2011
[28]https://picasaweb.google.com/owaspphotos/OWASPSummit#
[29]https://picasaweb.google.com/carlos.j.serrao/OWASPSummit2011?authkey=Gv1sRgCN3g-7qmu_i93QE#
[30]https://picasaweb.google.com/103488670506331805557/OWASPSummit2011Portugal?authkey=Gv1sRgCLSQr-TtgqrGEA&feat=directlink#
[31]https://www.owasp.org/images/9/97/Attendee_Bios_for_Outcomes_-_Participants.pdf
[32]https://www.owasp.org/index.php/Category:Summit_2011_Tracks
[33]https://www.owasp.org/index.php/Summit_2011_Schedule
[34]https://www.owasp.org/index.php/Summit_2011_Schedule_Dynamic

 [35]

Just about everybody that went to the Summit really worked hard, and we showed that OWASP is the only organisation in the world that is able to put in the same place (working together) individuals that are from different companies, races, religions and politics.

THAT is spectacularly unique.

One of my favourite comments about the Summit was: *'Hey! This is just like the UN, but actually working!'*

 [36]

For example the crowd that John was able to assemble in the browser track had never meet before! (and some of them had even wrote a book together before). Also, they are not you typical OWASP crowd (ie we were reaching out)

[35] http://4.bp.blogspot.com/-QiNjCuHgxaY/TVQem9GrmjI/AAAAAAAAARA/9LwO7GN3Seg/s800/IMG_5671_DM.jpg
[36] http://4.bp.blogspot.com/-uy2U28REC-4/TVFTTu-BiII/AAAAAAAAAJg/qOMh0ZbqpXs/s800/IMG_5430.JPG

Yes (on next summits) we need to be more focused on the deliverables, handle better the post-summit activities and bring (even more) developers/architects/business-reps/'non typical Owasp Contributor'. That said, if you haven't already please go and read now the Summit Outcomes[37] and Final Report[38] (if you looking for an area of OWASP to be involved, there are lots of opportunities still left in those outcomes)

BUT!!!! let's not confuse the problems with the failed Summit 2013[39] attempt with the need for Owasp to have more Summits.

I was publicly very critical of the Summit 2013 (namely when I stated that 'I want to vote for a Summit Team+Vision, NOT for a venue'[40]), but that doesn't mean that we should abandon the Summit activities.

Summits should be key to OWASP's DNA since that is where we should regularly meet to work hard, collaborate, present recent developments and create action plans.

Inside that last post[41] I presented a really interesting concept of what a 'Summit Proposal' should look like.

That is how (in my view) successful Summits are set-up and executed (that is what I tried to do the last two Summits), so please let's make another summit happen :)

[37] https://www.owasp.org/index.php/Summit_2011_Outcomes
[38] http://sl.owasp.org/summit2011_finalreport
[39] https://groups.google.com/a/owasp.org/group/owasp-summit-2013/browse_thread/thread/938e40b807dd5cd9#
[40] http://diniscruz.blogspot.co.uk/2012/04/i-want-to-vote-for-summit-teamvision.html
[41] http://diniscruz.blogspot.co.uk/2012/04/i-want-to-vote-for-summit-teamvision.html

3.6 When is the next OWASP Summit!!!!!

Looking at the OWASP Summit pictures[42] reminded me of the amazing experience that the OWASP Summit 2011[43] was. There was so much positive energy in the air and we got much done (see the final report[44] and the session's outcomes[45]).

We need another one!!!!

Surely we can have one in 2013!

But if we are going to do it, we have to do it right :)

- Some proposed Visions for next OWASP Summit[46]
- Great description of why OWASP Summits are special[47]
- Summits must be part of OWASP's DNA[48]
- I want to vote for a Summit Team+Vision , NOT for a venue[49]
- OWASP Revenue Splits and the "Non-profits have a charter to be innovators"[50]
- Sometimes the best response is just say 'YES'[51]

[42] https://picasaweb.google.com/103054218257696470914/OWASPSummit?gsessionid=5EHA7D4GzGOw0L8iAqcVrw#
[43] https://www.owasp.org/index.php/Summit_2011
[44] http://sl.owasp.org/summit2011_finalreport
[45] https://www.owasp.org/index.php/Summit_2011_Outcomes
[46] http://diniscruz.blogspot.com/2012/04/some-proposed-visions-for-next-owasp.html
[47] http://diniscruz.blogspot.com/2012/04/great-description-of-why-owasp-summits.html
[48] http://diniscruz.blogspot.com/2012/04/summits-must-be-part-of-owasps-dna.html
[49] http://diniscruz.blogspot.com/2012/04/i-want-to-vote-for-summit-teamvision.html
[50] http://diniscruz.blogspot.com/2012/12/owasp-revenue-splits-and-non-profits.html
[51] http://diniscruz.blogspot.com/2012/10/sometimes-best-response-is-just-say-yes.html

4 OWASP Education

This section has the following chapters:

- Let's make this happen 'Investing in Developing Software Security Talent'[1]
- PDF with (draft) Exam of OWASP Top10 questions[2]

Table of Contents[3]

[1] /manuscript/4.OWASP_Education/Let's_make_this_happen_'Investing_in_Developing_Software_Security_Talent'.md
[2] /manuscript/4.OWASP_Education/PDF_with_(draft)_Exam_of_OWASP_Top10_questions.md
[3] ../../Table_of_Contents.md

4.1 Let's make this happen: "Investing in Developing Software Security Talent"

Mark posted yesterday an 'draft' idea which I think is GREAT!

**Please read it at Investing in Developing Software Security Talent[4] **

Although I think that Mark is on a great path, one that is consistent with his views of bringing developers to security (not security to developers), I have a couple comments on is proposed model :)

Here are my key proposed changes:

- **Separate the 'creating security talent' from Seconauts **(ie 'separate code from data', or using a git analogy 'fork the main repository')
- **Expand the concept to include current Developers and Security Professionals**
- **Create a financial model that is easy to implement, transparent and morally effective**

This is how I would slice it:

Master version (the 'code'): "Developing Software Security Talent" Programme:" - **Improving the Software Security Talent of a new Generation of Software developers and 'code fixers'._
**_
__*The focus of this program is to help **Developers or Security Professionals who want to write secure code or fix security vulnerabilities**. The model proposed is one based on Internships and Mentorships.*

- *The key objective is to create the next generation of developers who will:*
  - _know how to write secure code, _
  - _work with the multiple SDL parties in the multiple secure coding/architecture activities and _
  - *fix security vulnerabilities*
- *The program will measure its success by the number of 'conversions' made over a period of time:*
  - *# of students that are now focus on secure coding*
  - *# of real-world developers who have added 'secure coding' to their skill set*
  - *# of developers (and job applications) that have 'secure coding' on its job spec*
  - *# of Application Security professionals who have acquired 'secure coding' skills and can talk with developers (in the developer's language) and are able (when requested) to sit down and fix code*
- *A desired site-effect is the creation of an open community and 'high-quality body of work', that supports the millions of developers who need to write secure code worldwide, and ask 'secure coding questions' everyday.*
- *How these 'conversions' are made, is not an important detail:*
  - *The 'Seconauts model' (descibed below) is just one way to achieve this goal*

Fork #1 (the 'data) "Seconauts participation in *"Developing Software Security Talent" Programme:***

Seconauts will:

[4] http://www.curphey.com/blog/2012/10/19/investing-in-software-security-talent/

- *Find the sponsors and mentors*
- *Handle the logistics (from payments, to selections, to contacts, to introductions, to public reporting, etc..)*
- *Define the selection criteria, select the candidates and allocated them to the mentors*
- *Define the Seconauts projects that will be worked on (by the candidates) and ensure that there is enough high-quality reviewers at hand to help with task allocation and questions raised (by the candidates)*
- *Help and brief the Mentors (with clear definitions of what are the expectations and responsibilities of each party)*
- *...see mark's post[5] for a specific details (like the number of mentors, what each one should do, etc...)*

Fork #2: XYZ Company ....

Fork #3: XYZ University ....

Fork #4: UK Government ....

Fork #5: OWASP ....

etc...

Remember that the objective is to develop Security Talent, so it doesn't really matter how it is done, as long as it happens.

It is also important to take into account that some companies or organisations have a _'Not invented here' _syndrome, and it is important to present them with ideas that they can consume, re-brand and execute

Rough/Draf notes

Since Mark's original post was in a 'Draf' mode', here are a bunch of semi-related notes and ideas that I had when reading and thinking about this.

Starting with some comments on the proposed model, I'm going to use SI (Security Innovation)[6] as an example of a company that could participate on the mentoring and hiring activities (note that I have not spoken with the SI guys about this, it is just easier to have a specific example in mind):

- I think that the amount paid to the 'candidate' should 'be defined' by the 'contracting party', in this case SI. Since SI would want to get the best talent, it can chose to pay more (this will also depend on the geographical location of the candidate)
  - Although I'm a big believer of openness, in this case, the 'financial arrangement' should be a private matter between SI and the candiate
- I like the ideas to give the candidate some money, but this should ONLY be used to cover expenses (computer equipment, travel, hosting services, software, etc). In a similar way that I wrote on Why OWASP can't pay OWASP Leaders[7] the moment the sponsorship money is used as 'payment to the candidate' the social contract between the organisation, the mentors and its participants is broken:
  - See previous point on how I'm NOT saying that the candidate should NOT be paid
  - I'm saying that the candidate SHOULD be paid, just not by this program (whose funds should only be used for 'expenses')

[5] http://www.curphey.com/blog/2012/10/19/investing-in-software-security-talent/
[6] https://www.securityinnovation.com/
[7] http://diniscruz.blogspot.com/2012/04/why-owasp-cant-pay-owasp-leaders.html

    * With this in mind, the candidate should be given $4000, where HE/SHE decides where to spend that money (and in time there would be a good number of documented examples of where others spent it)
    * Like I wrote in the problem of paying OWASP leaders[8] and in the OWASP GSD Project (GSD = Get Stuff Done)[9] proposal, the concept is one where **the candidate cannot NOT pay himself, or any company/individual he/she is associated with **(this is a great self-regulated system, and it would dramatically reduce the management, monitoring and 'expense approval' requirements / overhead)
- This can be easily executed on a worldwide basis as long as the pieces are in place
- I don't think that the 'need for the candidate to go everyday' to an office is a critical one.
  - It raises the bar and complexity of the arrangement
  - It goes against the model of the 'distributed' development environment that we have today in the 'GitHub' generation
  - Development is sometimes better done in isolation than in groups
  - Again, not saying that it shouldn't happen, just that it shouldn't be a big criteria
  - For example I have no idea of where some of my good colleagues at SI are (even when I talk to them by voice, email, github, code everyday). They could be somewhere in Europe , in the Boston or Seattle offices or in the middle of the US)
  - So I would change this requirement to be '*the candidate must have a physical connection with the mentors every week, which could range from hours to 5 days*'
- If the cost allocated to each candidate is $4000, then the sponsorship packages should be multiples of that:
  - $4k pays for 1
  - $8k pays for 2
  - $12k pays for 3
  - $20k pays for 5 …. etc…
- This could be set-up on a recurring basis so that the sponsoring companies could view it as a recurring subscriptions.
- I think that there should be NO requirement on either party regarding the next contracts (i.e. namely no obligation for the candidate to work 18 months for the mentoring company).
  - For example I would expect that if a candidate did a successful internship at SI, and he liked SI that he wanted to join the company, and SI liked his/her work so much that it would offer a job:
    * there would be no need for a 'mandatory 18 months contract'
    * the contract offerend by SI should be competitive and fair ,
    * such '18 months requirement to work for SI' would dramatically change the negotiation dynamics (putting a lot of power in the hands of SI) and would most likely leave a bitter taste in everybody involved
- The focus should be on writing secure code and fixing existing code at Open Source projects, BUT we shouldn't have very high hopes that the code created will be of a very high standard since by definition these are inexperience 'secure development' developers (which will take more than 6 months to change)

And here is a brain dump of 'stuff' that needs some more thinking:

[8] http://diniscruz.blogspot.com/2012/04/why-owasp-cant-pay-owasp-leaders.html
[9] http://diniscruz.blogspot.co.uk/2012/05/owasp-gsd-project-gsd-get-stuff-done.html

- it is going to be hard to find a significant number of mentors (which is a catch 22 ,since once the model is proven, they will be easier to find)
- I would say that this is the hard part. At OWASP's Projects (see links below) we had a simpler workflow (which was project leader working with 2 reviewers) and it was REALLY hard to get good reviews created (it does take a lot of time to review something properly). I don't think it should be underestimated how much effort it will take from the mentors and helpers
- There is usually a great difference between the amount of people who will put their hand up and say 'I can do it, I can review that or mentor him/her' to the ones who will actually be able to do it (and sometimes it is not that the reviewer/mentor are not good enough, it is just that it takes a lot of time and effort to do it properly)
- Creating a selection criteria and executing it will be hard, and the best way is to do it 100% in the open (learn from the OWASP seasons of code experience (see links below))
- Expand the target audience (it should also be focused on current professional developers that want to get into application security). We need this NOW for developers that are coding today:
  - In fact most companies that write a lot of software need this TODAY for a number of their current dev teams
  - I don't like the word 'intern' is sounds like it is for a somebody leaving school (or university). This is why I used the word 'candidate' on this post.
  - ex-students should be only one of the target audiences
- The work created by the 'candidates' is most likely NOT going to be production quality (since by default they will be amateurs at it). Only experienced developers (with security awareness/knowledge) are able to create that. So let's not raise the expectations bar too high
- Mark's maths are wrong:
  - $4000 will be barely enough to buy: a decent laptop, airfare expenses, hotels, hosting, software,etc… (over a period of 6 months). It will help if outside the US/UK, but we are talking about 800 USD per month (which is less than you get flipping burgers[10])
  - It also doesn't take into account all the back-office admin costs that it will take to make this happen (which I agree that shouldn't be paid from the $4000 sponsorship money)
- I like this idea as a good way to get talent to work on Seconauts (but i can see some critics saying that this is just a cheap way to kickstart a community)
- This is very similar to what happens on a number of companies, and it is called 'Interns' :)
  - in fact a number of OWASP members have such programs at their companies (which could be leveraged to kickstart this idea)
- **This will not work without operational support/staff, **in fact the first thing to do should be to hire / appoint a project manager to run this (Mark is currently doing that role, but he will soon run out of time/energy)
- There is already lot of mentoring happening at OWASP and I am personally involved in a couple of mentoring cases (not within an explicit framework, but achieving the same goals). So some of those efforts could be recycled to kickstart this idea
  - There are already a good number of targets for mentorship at OWASP, namely some newer OWASP leaders who are still getting their heads around WebAppSec
  - The irony is that OWASP would be the perfect place to do this, since it has the infrastructure, the funds, the community, the brand, etc…

[10] http://www.payscale.com/research/US/Job=Fast_Food_Worker/Hourly_Rate

  - That said, I think the concept is great, and since Mark is focused on it (and nobody is at OWASP), I will ask the Owasp community to support it and commit to at least 10k. I also will raise this idea at SI and see if they would like to participate

Bottom line: Good luck Mark
**

**More Secure Coding talent is something we desperately need, so I hope that this idea really comes into life and I'm happy to help as much as I can.

**Why I have experience in making this comments **

(originally I had this at the beginning of the post, but I figured out, that this will only be relevant to the readers that are reading it all the way to the end):

I'm going to comment on this as somebody who as already implemented a similar program at OWASP namely the OWASPs Seasons of code who had a similar number of moving parts and activities:

- Autumn of Code 06[11],
- Spring of Code 07[12],
- Summer of Code 08[13] (whose results were presented at first OWASP Summit 2008[14])

I was also very involved with Paulo Coimbra and the GPC on the management of OWASP projects, where we did a lot of thinking about this:

- https://www.owasp.org/index.php/Assessment_Criteria_v1.0[15] (more mature model)
- https://www.owasp.org/index.php/Assessment_Criteria_v2.0[16] (note how at the end of this page there is a reference to Project Mentors (there was more on mentoring concept, but I couldn't easily find that page/info))
- https://www.owasp.org/index.php/Tool_Assessment_Criteria[17]
- https://www.owasp.org/index.php/Documents_Assessment_Criteria[18]
- https://www.owasp.org/index.php/Research_and_Activities_Criteria[19]
- https://www.owasp.org/index.php/Assessing_Project_Health[20]
- https://www.owasp.org/index.php/Assessing_Project_Releases[21]

[11] https://www.owasp.org/index.php/OWASP_Autumn_of_Code_2006_-_Selection
[12] https://www.owasp.org/index.php/OWASP_Spring_Of_Code_2007_:_Selection
[13] https://www.owasp.org/index.php/OWASP_Summer_0f_Code_2008_:_Selection
[14] https://www.owasp.org/index.php/OWASP_EU_Summit_2008
[15] https://www.owasp.org/index.php/Assessment_Criteria_v1.0
[16] https://www.owasp.org/index.php/Assessment_Criteria_v2.0
[17] https://www.owasp.org/index.php/Tool_Assessment_Criteria
[18] https://www.owasp.org/index.php/Documents_Assessment_Criteria
[19] https://www.owasp.org/index.php/Research_and_Activities_Criteria
[20] https://www.owasp.org/index.php/Assessing_Project_Health
[21] https://www.owasp.org/index.php/Assessing_Project_Releases

For reference, before Paulo Coimbra left OWASP, we were really close to implementing a similar program at OWASP (the idea was to start with getting reviewers involved into projects (in a 'Season of Quality') and then evolve it into mentorships).

And has Paulo's departure showed, without such back-office support it is impossible to do this.

Btw, to give you an idea of the amazing work Paulo was doing on OWASP projects, take a look at [https://www.owasp.org/index.php/OWASP_Projects_Dashboard*2.0](https://www.owasp.org/index.php/OWASP_-Projects_Dashboard*2.0) (you will be amazed). The good news is that we now have Samantha (Owasp new project manager) who is going to bring things back on track

4.2 PDF with (draft) Exam of OWASP Top10 questions

On the topic of exams and certificates, JBI Training[22] wants to offer their clients some kind of certificates, so I'm helping them to figure out how to do it.

The first step was to have something to ping JBI's developer community with (i.e former students) so I pointed Nigel Laurens[23] to the OWASP Exams project[24] and he created this pdf[25] (embedded bellow) to kickstart things.

Of course that we really need to add some automation here (in terms of getting feedback on questions and processing the results), but even something as crude as this list of questions, will focus the mind of developers and make sure they undertand the OWASP Top 10.

I also noticed that this PDF doesn't include references to the source materials and content license. Which is caused by Nigel's lack of experience in the OWASP and http://creativecommons.org world (so don't go too hard on him :))

Btw, from the OWASP Exams[26] project it looks like the http://www.owaspa.org/moodle/[27] is still up (so take a look, since it is quite a nice solution)

Note that we are taking about certificates and exams here, not certification (since these are early days). That said the path for creating certifications based on OWASP material is already mapped on the OWASP Red book ([28]The OWASP Application Security Code of Conduct for Certifying Bodies)

And I have written about my views of OWASP Certification in this post[29]

[22] http://www.jbinternational.co.uk/
[23] mailto:nigel@jbinternational.co.uk
[24] https://www.owasp.org/index.php/OWASP_Exams_Project
[25] https://dl.dropboxusercontent.com/u/81532342/OWASP%20Files/OWASP%20Top%2010%20Quiz.pdf
[26] https://www.owasp.org/index.php/OWASP_Exams_Project
[27] http://www.owaspa.org/moodle/
[28] https://www.owasp.org/images/5/53/OWASP_Red_Book-Certifying_Bodies.pdf
[29] http://blog.diniscruz.com/2010/11/owasp-and-certifications.html

5 OWASP MIA (Missing in Action)

This section has the following chapters:

Table of Contents[11]

[1] /manuscript/5.OWASP_MIA/'Using_the_HTML5_Fullscreen_API_for_Phishing_Attacks',_OWASP_MIA_and_'We_need_SAST_technology_for_browsing_the_web_safely'.md

[2] /manuscript/5.OWASP_MIA/Big_Security_Challenges_with_Creating_APIs_for_US_Gov_Agencies.md

[3] /manuscript/5.OWASP_MIA/Example_example_of_SQL_Injection_using_Database.SQLQuery_from_GitHub.md

[4] /manuscript/5.OWASP_MIA/Guidelines_of_Owasp.md

[5] /manuscript/5.OWASP_MIA/Hack_Yourself_First_Jeremiah_at_TEDxMaui.md

[6] /manuscript/5.OWASP_MIA/I_think_the_time_as_come_for_OWASP_to_have_its_own_secure_browser.md

[7] /manuscript/5.OWASP_MIA/Nice_list_of_20_online_coding_tools.md

[8] /manuscript/5.OWASP_MIA/No_OWASP_app_on_the_OSX_AppStore_(Nov_2013).md

[9] /manuscript/5.OWASP_MIA/OWASP_and_Privacy_issues,_we_need_to_be_involved.md

[10] /manuscript/5.OWASP_MIA/Software_Labels_-_Jeff's_OWASP_AppSecDC_2010_presentation_(another_dropped_good_idea).md

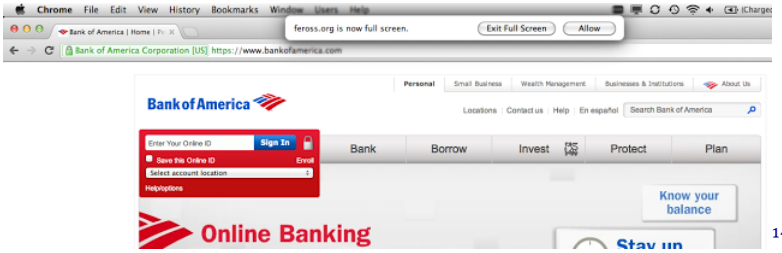
[11] ../../Table_of_Contents.md

5.1 'Using the HTML5 Fullscreen API for Phishing Attacks', OWASP MIA and 'We need SAST technology for browsing the web safely'

Really nice article from Feross Aboukhadijeh[12] on the Phishing potential of HTML5 FullScreen features:

You can read it at Using the HTML5 Fullscreen API for Phishing Attacks[13]

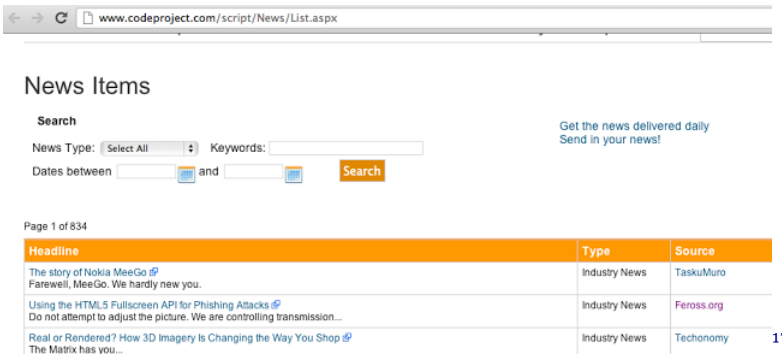
Note that on Chrome in OSx it will show this alert



[14]

... if you're not in Full Screen already. But in a lot of cases that will be easy to dismiss (specially with users used to click that 'Allow' button). See note below on using SAST technology to deal with this.

What is interesting about this story is that is also shows how developers DO care about security. There is a thread about it on Hackers News[15] and on Reddit[16] and I found this article via the CodeProject's Daily New email:



[17]

OWASP MIA

But where's OWASP on this thread?

- both Hackers News[18] and on Reddit[19] have no mention for OWASP (just search the page)
- Feross article[20] also has no mention of OWASP

[12] http://feross.org/about
[13] http://feross.org/html5-fullscreen-api-attack/
[14] http://2.bp.blogspot.com/--RmQBWSarJw/UHfobSTfzPI/AAAAAAAAARg/5UPCRrACiIA/s1600/Screen+shot+2012-10-12+at+10.51.33.png
[15] http://news.ycombinator.com/item?id=4629906
[16] http://www.reddit.com/r/netsec/comments/116mdb/using_the_html5_fullscreen_api_for_phishing/
[17] http://4.bp.blogspot.com/-sE2fCwLRIRM/UHfsQcYfNBI/AAAAAAAAAR4/xNsUgTp4PSI/s1600/Screen+shot+2012-10-12+at+11.04.24.png
[18] http://news.ycombinator.com/item?id=4629906
[19] http://www.reddit.com/r/netsec/comments/116mdb/using_the_html5_fullscreen_api_for_phishing/
[20] http://feross.org/html5-fullscreen-api-attack/

- A quick search for Feross' name and OWASP didn't show anything
- Nothing on OWASP's website (which means that he has not presented at an OWASP conference or chapter)

So is Feross involved at all with OWASP? I can't find it.

As one of the guys who created one of the best ClickJacking examples HOW TO: Spy on the Webcams of Your Website Visitors[21] (and only 22 years old), he is clearly part of the new generation of AppSec Security experts.

But if OWASP is not able to attract him and create environments / ecosystems for Feross (and other new stars), that means that we (OWASP) are starting to be irrelevant for the new Generation :(

And that is a fundamental problem with OWASP. We should be measuring OWASP's success by its community and relevance. But it is much harder to measure 'What could had happened' than 'what is happening'. This (amongst others) is why I proposed a new model for OWASP[22] so that OWASP can reinvent itself and find ways to add value to Feross (and its community).

**

****We need SAST technology for browsing the web safely**

So how to do solve this? Unless we start to have SAST-like Technology on browsers (which allow us to write context-sensitive rules that know the difference between YouTube and Feross' website) I don't think we will find a good solution (it's just patches and hacks)

[21] http://feross.org/webcam-spy/

[22] http://diniscruz.blogspot.com/2012/10/an-idea-of-new-model-for-owasp.html

5.2 Big Security challenges with creating APIs for US Gov agencies

So Barack Obama Directs All Federal Agencies to Have an API[23]

Here is the White house memo[24] (pdf) which mandates the implementation of "Digital Government: Building a 21st Century Platform to Better Serve the American People"[25] (pdf).

The good news it that at least security and privacy seems to be taken into account (with it's own chapter and focus)

I haven't read the document but after a skim, it looks like there is more focus on the non-secure-application-development 'security side' of these APIs.

And this could be an issue, since creating APIs is usually done by exposing internal systems or WebServices, which will now need to have much higher level of security than before (when they were connected to much less hostile environment).

I also like the use/focus on Privacy, since that will be a good way to drive coding and application changes.

This is a great opportunity for OWASP community to be involved since there is going to be a lot of API developers out there that could do with some help

[23] http://blog.apievangelist.com/2012/06/01/barak-obama-directs-all-federal-agencies-to-have-an-api/
[24] http://www.whitehouse.gov/sites/default/files/uploads/2012digital_mem_rel.pdf
[25] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf

5.3 Example example of SQL Injection using Database.SQLQuery from GitHub (and idea for Cat.NET workflow)

After posting Another example why SATS technology needs custom rules (re: Detecting SQL Injection on .NET Entity framework)[26] I did this search on GitHub,[27] and found an example of that dangerous ***Database.SqlQuery*** API in use:

- https://github.com/caioketo/QIERP/blob/master/QIERPDatabase/VerpContext.cs#L55
- **with default sa pwd**: https://github.com/caioketo/QIERP/blob/master/QIERPDatabase/VerpContext.cs#L18
- **use of Database.ExecuteSqlCommand**: https://github.com/caioketo/QIERP/blob/master/QIERPDatabase/VerpContext

These one allows callers to create SQL Injection (which means that whoever is consuming those APIs need to be VERY careful)

- https://github.com/revolutionaryarts/wewillgather/blob/master/src/Libraries/Gather.Data/GatherObjectContext.cs#L69
- https://github.com/philpeace/PointyPointy/blob/master/PointyPointy.Web/Data/StoryContext.cs#L51
- https://github.com/samandmoore/GetRDoneWeb/blob/master/GetRDone/GetRDoneContext.cs#L25
- https://github.com/slask/MVCArchitectureTemplate/blob/master/Solution/DataAccess/Context/ScrabbleClubContext.c

This one look OK (on diagonal reading)

- https://github.com/JayBeavers/ChronoZoom/blob/exceptionalIo/Source/Chronozoom.Entities/Storage.cs#L122 (Ok, because timelinesMap.Keys are GUIDs). There are multiple other uses of Database.SqlQuery which look ok because either the parameters options were used, or the string concats where done on GUIDs)

Idea for Cat.NET workflow

Now wouldn't it be great if we could automate an Cat.NET (or another SAST scanner) to do this type of analysis automatically?

For example an Bot ot TeamCity workflow that:

1. cloned/pulled a repo
2. compile it
3. run cat.net on it (with default or custom rules)
4. automatically package the issues discovered
5. send issues to repo owner
6. allow rules to be customised (maybe as an XML file somewhere in the repo), for example, wrappers around ***Database.SQLQuery*** need to be marked as sinks)
7. go back to 1

[26] http://blog.diniscruz.com/2013/07/another-example-why-sats-technology.html
[27] https://github.com/search?q=Database.SqlQuery&type=Code&ref=searchresults

I also would like a mode to create UnitTests based on the vulns discovered (using SAST and DAST techniques), but that is a topic for another post :)

Ideally all this would be linked to Developer friendly guidance (like TeamMentor[28] or OWASP content) in order to help the developers to easily understand the issues and write the required fixes

[28] https://teammentor.net/

5.4 Guidelines of OWASP

OWASP got a great quote on this EU Regulations document which is *aimed at laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative)*[29]

18.11.2011 EN Official Journal of the European Union L 301/3

II

(Non-legislative acts)

REGULATIONS

COMMISSION IMPLEMENTING REGULATION (EU) No 1179/2011

of 17 November 2011

laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

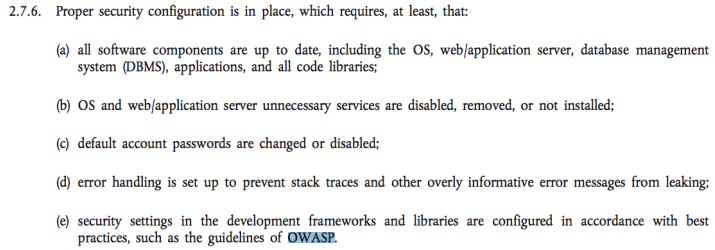
Having regard to Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative (1), and in particular Article 6(5) thereof,

After consulting the European Data Protection Supervisor,

(5) Implementation by the organisers of the technical specifications should guarantee certification of the online collection systems by the Member States' authorities, and contribute to ensure the implementation of the appropriate technical and organisational measures required to comply with the obligations imposed by Directive 95/46/EC of the European Parliament and of the Council (2) on the security of the processing activities, both at the time of the design of the processing system and at the time of the processing itself, in order to maintain security and thereby to prevent any unauthorised processing and protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

30

Do a search for OWASP and you find 2 references, with the 2nd being this one:



2.7.6. Proper security configuration is in place, which requires, at least, that:

(a) all software components are up to date, including the OS, web/application server, database management system (DBMS), applications, and all code libraries;

(b) OS and web/application server unnecessary services are disabled, removed, or not installed;

(c) default account passwords are changed or disabled;

(d) error handling is set up to prevent stack traces and other overly informative error messages from leaking;

(e) security settings in the development frameworks and libraries are configured in accordance with best practices, such as the guidelines of OWASP.

31

This is great, but what are these ***'Guidelines of OWASP'***?

Ideally we should should have a series for very explicit and focused 'Guidelines' to answer this question :)

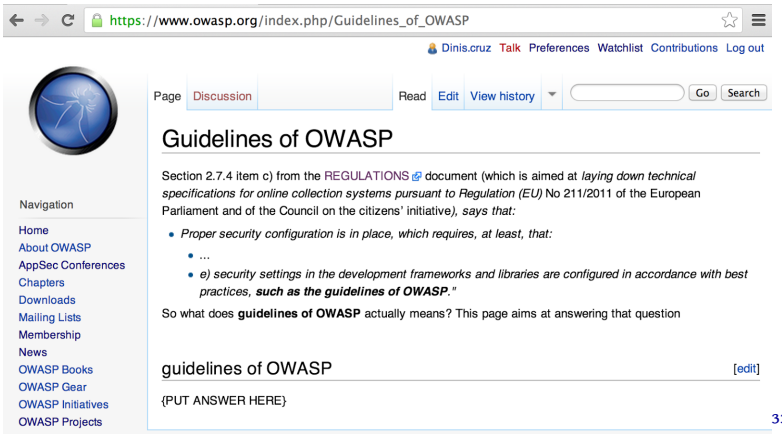
To kickstart this process I created the Guidelines of OWASP[32] page at the OWASP Wiki, so if you have some cycles, please chip in with your views:

[29] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:301:0003:0009:EN:PDF

[30] http://2.bp.blogspot.com/-XbL-gkseuNQ/UkAm3WNW8oI/AAAAAAAADgY/4zbpFK0WdBA/s1600/Screen+Shot+2013-09-23+at+12.28.50.png

[31] http://1.bp.blogspot.com/-XC8RKf88oO8/UkAm3QVEyJI/AAAAAAAADgU/gopGCkVkqVc/s1600/Screen+Shot+2013-09-23+at+12.29.07.png

[32] https://www.owasp.org/index.php/Guidelines_of_OWASP



[33]

[33] http://2.bp.blogspot.com/-uFAEHzlaj_c/UkAm5O_TUSI/AAAAAAAADgk/7E-BMiWkeoY/s1600/Screen+Shot+2013-09-23+at+12.29.34.png

5.5 Hack Yourself First: Jeremiah at TEDxMaui

Jeremiah was recently at TEDxMaui[34] presenting Hack Yourself First[35] which is an interesting development for WebAppSec and OWASP since I think it is the first time that a member of our community gets to present at TED (which is one of the best conference-series in the world)

Couple comments:

- he was quite nervous, which shows the 'pressure to deliver' that TED has.
  - See Jeremiah's Written Speech[36] (i.e. what he wanted to say) and his personal comments about the experience[37])
- I really like the concept of 'Hack yourself first' but I wished Jeremiah had given more examples on how to do it an a personal, corporate and organisational level
- there was FAR too much FUD for my taste. I would had been better if he found a more positive way to deliver the message
- It is also quite obvious by Jeremiah performance that he really cares about WebAppSec and wants to make the world more secure
  - Of course that he owns a company that helps companies to 'Hack themselves first' so there is a lot of vested interest in there too :)
- I think that OWASP doesn't get one mention, which is not Jeremiah's fault. I just shows the weakness of the OWASP Brand

Here is the Video:

[34] http://tedxmaui.com/
[35] http://tedxtalks.ted.com/video/TEDxMaui-Jeremiah-Grossman-Hack
[36] http://jeremiahgrossman.blogspot.co.uk/2012/04/written-speech-tedxmaui-hack-yourself.html
[37] http://jeremiahgrossman.blogspot.co.uk/2012/01/tedxmaui-hack-yourself-first.html

5.6 I think the time as come for OWASP to have its own secure browser(s)

The idea is to create a customised version of a popular browser (like Chrome or Firefox) that has been customised to be secure out-of-the-box.

It could even be something like http://www.srware.net/ but I want to leverage the trust-network that OWASP has (and its potential to peer-review) to create a piece of software that I actually trust (or that it can earn my trust with time)

We should also add extensions that improve its security (after doing a security review on them).

This will not be an easy road since creating secure apps is very hard, but I think that doing this in a public forum (like OWASP) will help to sort out a lot of the current (workflow and technological) problems.

I finally reached this conclusion by being (again) in Starbucks with the potential of my blog being compromised[38]

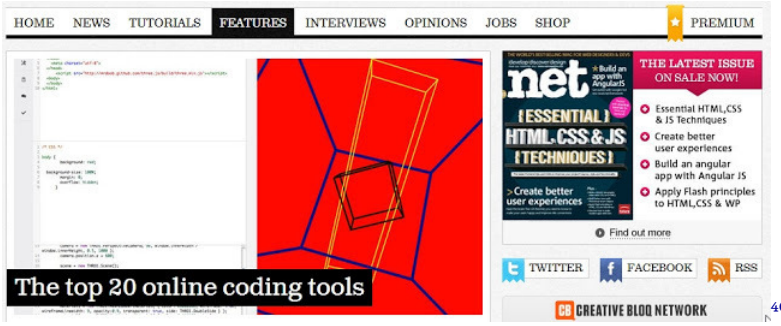
[38] http://blog.diniscruz.com/2012/10/so-if-my-blog-account-is-compromised.html

5.7 Nice list of 20 online coding tools

There is definitely a lot of innovation happening in this space, check out the list at The top 20 online coding tools[39] from .Net magazine.

And if we want to enable the next generation of developers to code securely we need to integrate our knowledge into their IDEs (like these ones). Humm …. I wonder how hard it will be to add TeamMentor integration to these IDEs?

Note that this is on a mainstream developer magazine and (predictably) a search for '*security*' or '*owasp*' has 0 hits on that page:



[40]

[39] http://www.netmagazine.com/features/top-20-online-coding-tools

[40] http://3.bp.blogspot.com/-H_4PNLrhkwY/Ulk5l1hJDeI/AAAAAAAAAnI/UivTV9YyMcw/s1600/CropperCapture%5B41%5D.jpg

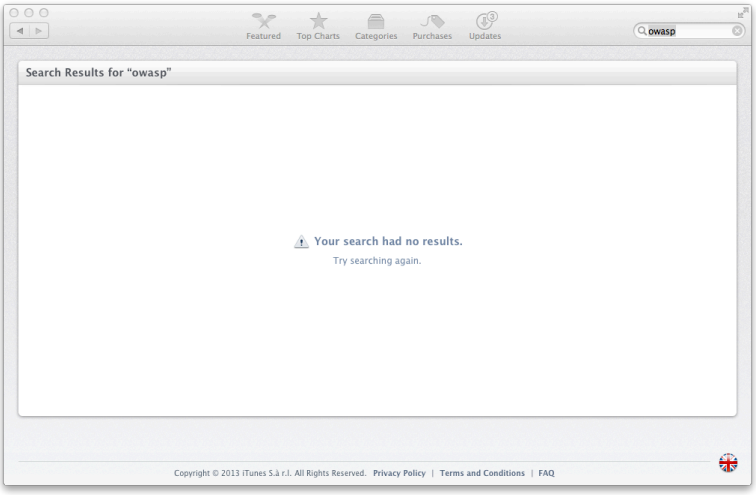
5.8 No OWASP app on the OSX AppStore (Nov 2013)

Definitely a missed opportunity here :)

What types of App should exist?

At least we should have a couple that expose OWASP materials (books, wiki pages) , projects and events.

I will be a happy guy when this page doesn't look like this:



[41]

[41] http://2.bp.blogspot.com/-RyR-2qVT38s/UpU9mm3Xn9I/AAAAAAAAExw/HqpHtFaK6zo/s1600/Screen+Shot+2013-11-27+at+00.32.16.png

5.9 OWASP and Privacy issues, we need to be involved

Following the original post of https://www.owasp.org/index.php/User_Privacy_Protection_Cheat_Sheet[42] and an owasp-leaders thread on 'OWASP should not have a political voice', I wrote this:

Well we can't ignore reality. That CS (CheatSheet) raises a lot of good points and provides very valuable information to devs who want to support their users that way.

I don't think that the solution for OWASP is to curate the content based on political sensitives (since they vary around the world).

The solution is surely to present the multiple points of view (maybe even on different CS) and cross-link them. Why don't we have a CS on 'User Privacy protections accepted by governments" or "User Privacy for the user that has nothing to hide"

Privacy is very important topic , but due to trying to be 'politically correct' OWASP has failed to be involved. I'm glad this is starting to change, the politics are coming to WebAppSec so we need to accept that, and present technically correct analysis and guidance on 'hot' topics

And remember that the beauty of OWASP's open and Wiki-driven model is that if you don't like something, you can create a better one next door, and with time, the best one will gain the limelight/credibility/reputation (which is why 'Reddit like threads' are SO important for OWASP)

Edit: Here is a reddit page for this CheatSheet[43]

[42] https://www.owasp.org/index.php/User_Privacy_Protection_Cheat_Sheet

[43] http://www.reddit.com/r/OWASP_CheatSheet/comments/10xmm2/user_privacy_protection_cheat_sheet/

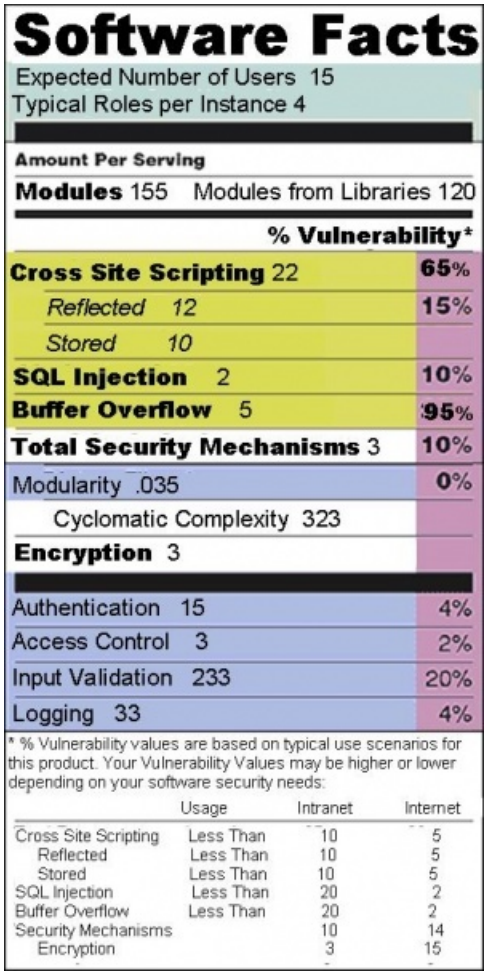
5.10 Software Labels – Jeff's OWASP AppSecDC 2010 presentation (another dropped good idea)

An old idea from Jeff Williams (which is spot on) is the need to apply Labels to Software and Web Applications.

The concept is simple, but its implementation is really hard, because of the lack of quality standards/metrics in our industry

Here are Jeff presenting his idea two years ago: Don't Judge a Website by its Icon - Read the Label![44]

> This is a really important concept, and its complete lack of adoption (and traction) speaks volumes for our industry
> For example, how am I supposed to make informed decisions as a software/website user if I cannot be exposed to something like this:



Also related is the idea o Idea for OWASP Standard for public rating of an WebSite's security profile[45] which could also create these useful labels:

[44] https://www.owasp.org/index.php/Don%27t_Judge_a_Website_by_its_Icon_-_Read_the_Label!

[45] http://blog.diniscruz.com/2009/12/idea-for-owasp-standard-for-public.html


OWASP
OPEN
SECURITY PROGRAM
OWASP
SHARED
SECURITY PROGRAM
OWASP
PRIVATE
SECURITY PROGRAM
OWASP
"TRUST US"
INSECURITY PROGRAM

6 Philosophy

This section has the following chapters:

Table of Contents[5]

[1] /manuscript/6.Philosophy/Happiness_makes_business_sense.md
[2] /manuscript/6.Philosophy/The_power_of_not_being_in_power_(and_being_ignored).md
[3] /manuscript/6.Philosophy/We're_all_mortals,_so_lets_make_the_most_of_it.md
[4] /manuscript/6.Philosophy/Why_do_others_think_that_I'm_hard_to_deal_with_and_that_I_don't_listen.md
[5] ../../Table_of_Contents.md

6.1 Happiness makes business sense

This TED talk by Shawn Achor "The happy secret to better work"[6] makes the case that positive energy and 'happiness' make us more productive and effective.

Not only his presentation style is great, I think he is completely right.

Specially on the part that 'happiness' is a habit and needs to be constantly exercised.

From a business or organisational point of view, this means that it should be a 'corporate' objective to deliver happiness to its players (employees, members, clients, partners, etc…)

They should do this not because it is 'nice', but because it makes business sense.

For example when I was working with Paulo on OWASP projects and initiatives, it was always amazing to see how a little bit of encouragement or contact/email, would motivate an owasp leader to get something done.

The problem is that creating these 'happiness' environments are very hard, take considerable commitment and can't be done by people who don't believe in it.

One of the reasons why I really believe that OWASP needs to have a lot more human resources, is because they need to have the time to deliverer 'happiness' to owasp leaders and community :)

Just to re-enforce the concept. OWASP should do this because it will increase OWASP productivity, synergies, serendipity, deliverables and community.

[6] http://www.ted.com/talks/shawn_achor_the_happy_secret_to_better_work.html

6.2 The power of not being in power (and being ignored)

I think helps a lot to give clarity and focus to ideas when the 'idea maker' doesn't have enough power to 'force' their execution (or adoption)

I've talked about this before in You will not have your best ideas when you are in a position of Power[7] and it is something that more and more fell that is needed.

As somebody who has a lot of opinions and ideas (see I wish that OWASP in 2014 ….[8]) I think it is very healthy that once I Stepped down as Board Member[9] I was able to (eventually) write freely about An Idea of a new model for OWASP[10]

The same applies to the O2 Platform[11] which I've been working on for the past 5 years. As I mention in Where Is .NET Headed? and the cost for Microsoft of ignoring the O2 Platform[12] and Responding to Andrew's O2 Platform feedback on the OWASP Leaders list[13] I still think that the O2 Platform has a huge amount of innovation and great ideas for Application Security and development.

But isn't the O2 Platform really hard to use? Yes, and part of the reason is that it has been designed to ***'allow problems to be solved'*** not to ***'work outside of the box'***.

That said there are quite a lot of examples out there on to use it, this post for example 'How to start using the O2 Platform and its scripting capabilities?' (and how I used the O2 Platform to solve a hard integration problem in May 2013)[14] shows the O2 Platform's powerful scripting capabilities, here are 39 videos[15] and here is the begining of a book on the O2 Platform web scripting capabilties[16].

So in a weird way, I think it has been quite healthy for the O2 Platform to have a slow (but steady) adoption, since that means that its growth is quite solid and based on real merit and added-value (ironically the lack of real users also allowed me to make major changes to O2's architecture and APIs which would had been very hard to do if its user-base quite large (for example the FluentSharp API's would probably never had existed with the ability to perform major refactorings to the O2 Platform codebase).

The bottom line is that **in the inter-connected world we had today**, **good ideas and tools will always have the opportunity to grow organically** (linearly or exponentially[17]). And a great idea, is one that will eventually reach exponential effects (where most of the growth happens in the last iterations (see Chapter 3: Exponential Growth[18]))), so in a way, what really matters is ***what part of the exponential curve some of my ideas currently are?*** :)

[7] http://blog.diniscruz.com/2012/10/you-will-not-have-your-best-ideas-when.html
[8] http://blog.diniscruz.com/2012/11/i-wish-that-owasp-in-2014.html
[9] https://lists.owasp.org/pipermail/owasp-leaders/2011-February/004664.html
[10] http://blog.diniscruz.com/2012/10/an-idea-of-new-model-for-owasp.html
[11] http://blog.diniscruz.com/p/owasp-o2-platform.html
[12] http://blog.diniscruz.com/2013/05/where-is-net-headed-and-cost-for.html
[13] http://blog.diniscruz.com/2013/05/responding-to-andrews-o2-platform.html
[14] http://blog.diniscruz.com/2013/05/how-to-start-using-o2-platform-and-its.html
[15] https://www.blogger.com/are%20http://blog.diniscruz.com/2012/04/39-o2-platform-videos-with-12k-youtube.html
[16] https://github.com/o2platform/Book_WebAutomation/blob/master/O2Documentation.md
[17] http://en.wikipedia.org/wiki/Exponential_growth
[18] http://robotswillstealyourjob.com/read/part1/ch3-exponential-growth

6.3 We're all mortals, so lets make the most of it

Just heard today that a very good friend lost her husband to a 5 year cancer battle :(

I can't image what she has been through and it does show how the lottery of live can sometimes be quite harsh.

It's in times like this that one really must think about what we are doing with our time and make sure that we are having a positive impact.

In a way that is what I like so much about OWASP. It is a great community, made of amazing people, and each one of us, can be proud of our contributions, since we are having a positive impact on the solution of a big problem.

I fell very fortunate that I am able to spend my time doing what I am really passionate about, so if you are currently stuck in a job just because it 'pays well', or it is the 'right thing to do', get out of there.

Life's too short to spend it on things we don't believe and are not passionate about.

Lets make sure that we have a positive impact while we are still around

6.4 Why do others think that I'm "hard to deal with" and that "I don't listen"

Here is a bit of self-analysis for you :)

One of the common complains that I've heard about me, is that I'm *"hard to deal with"* and that I *"don't listen"* (to others opinions).

Apart from the fact that I can also complain about that myself (I don't always listen to me too, and my 'instinct opinion' does usually takes over), I think that it is important to analyse the root causes and see if there are solutions to improve it.

My instinct (who I tend to trust a lot), is kinda pointing me to this:

- I do a lot of public activities and actions that open the space for others to comment
  - I also proactive ask for comment (i.e. inviting 3rd party participation)
- In a lot of these activities I'm not 100% in charge, or at least am avoiding to play the game *'my way or the highway'*
- This means that the '*others*' participating in the conversation, and providing comment/advise on the questions asked, have an '*expectation*' that their comments will be '*listened to*':
  - Here is the first problem, ** a lot of people (me included) think that *'listening to somebody' _is the same as '_doing what they said'*.** And this creates an expectation problem where if what '*they said*' doesn't happen, they think that the recipient didn't '*listen*' (which is usually not the case, just that they didn't agree with the proposed solution/comment)
  - The 2nd problem i**s that most comments are made without a proper understanding of the problem at hand** (and its multiple variables). Now sometimes this is great, since a fresh perspective can bring something new, but in other cases it just raises ideas that have already been discarded by previous experimentation and analysis (see next point)
  - The 3rd problem is that the** '*others*' providing the solution will NOT have to deal with the side effects of that solution**. I.e there will be no direct implications for them if their solution is accepted/implemented. This is important, since I usually have to deal with the implications/side-effects of those ideas/solutions, which again makes me much more resolute and focused.
- Usually when I '*pick a fight/path*', I tend to do my homework, and take the time to find good solutions. Here is my usual workflow:
  - **DefCon A) I have a problem to solve!**
  - **DefCon B) I start to go in all sorts of different directions** (some of them massive tangents) in order to figure out a solution (every idea is a good one at this stage). I also try to think as many steps ahead as possible (and in 3D)
  - **DefCon C) **For the promising options/ideas**, I try to create (as much as possible) **working PoCs** (very important since in technology, a lot of _'this sounds like a good idea' _stuff will not work, and the _'humm this might not work' _stuff will actually work!
  - **DefCon D1) For the issues that I don't have a solution** (or don't like my approach),** I ask the question to a wider audience,** or
  - **DefCon D2) When I have a solution that I like, I present the issue ****to a wider audience**
  - **DefCon E) I have a final solution and am implementing it at full speed**

- The problem is when the '*others*' (who say that I "*don't listen*" to and am "*hard to deal with*"), come into the conversation, I'm usually at **D1** or **D2 DefCon mode**, which means that I have already done a LOT of thinking and experimentation about the problem at hand.
  - This means that unless the guys on the other side really found a blind spot in my thinking/logic, it is very unlikely that they will find (in 5minutes) a solution that I have not considered.
  - Of course that if they DO spend the time, and do some experimentation and PoCs, there is a very high-possibility that they will find a good/better solution (but it will take time)
  - If the '*others*' start the dialog by expecting me to '*listen*' to them, the conversation will not last very long (this is actually my fault and loss, since sometimes I should be more diplomatic)
  - Usually the **D2 DefCon** mode is actually part of a **B DefCon **thread, which will also give to the '*causal observer'* a feeling that I'm going in a really weird direction and am not doing things 'the right way'
- And since I have done so much thinking about the problem, I'm really hard to argue against, because I usually already have good/strong answers for the first-batches of objections / issues / questions.
- Another problem that I know I have, is that I trust my instinct a lot (i.e. my inner brain has found a good solution but I haven't rationalised it).
  - In practice this means that I will make a decision or choose a particular path (on my way to **DefCon D2** or **E)** and when asked, initially I will struggle to give a good explanation (even to me)
  - But after (usually a couple hours of) some debate, I am able to present a number of clear and objective reasons that defend my ideas and that the recipient gladly accepts (not by '*giving up on the conversation*' but because my point of view now makes sense)
    * In fact, usually the complaint I get at this stage is "… **Hey man, why didn't you give me THOSE XYZ reasons 2 hours ago, I would had understood it immediately!!!" **, and my reply is usually_** "… well 2 hours ago I didn't have them :) , I just knew that the right path was that one…"_**
- I also have been right so many times in the past, that I have an inner confidence to just do it. In fact, what I found recently is that I have more and more confidence to go outside my confort zone, since too many times in that past, the returns (and final results) have been amazing.
  - I also have tons of cases where those '*others*' that disagree with me, come back years later saying *'…you know what … you were right on that one…'*
  - And yes, there as been a couple of _'…I told you so….' _:)
- Another thing that I tend to do, is on the cases when I do change my mind (which btw I'm happy to do), I also tend to '*move on*' very quickly from there, and start looking at the next batch of problems (i.e. pressing down the accelerator even more)
  - This is also very disturbing for the '*others*' since, although they are happy that 't_heir idea*' won, they expect some '_peace time*' where the status quo stays on that idea (and don't like the fact that I already accepted it and evolved it into the next set of issues/questions/problems)
  - I also think that one of my best assets is to be able to VERY quickly change my paradigms, and be able to quickly start thinking under the new reality (this is probably a side effect of programming, since that happens all the time when we're trying a new technology/technique, which suddenly '*works*'!!)
- In terms of accepting ideas, I like to think that I do accept others ideas, in fact I'm a big believer in the '*standing in the shoulders of giants*' concept, and always try to put the '*global objective/mission*' ahead of anything any personal feelings.

  - for example when I was organising the last OWASP Summit, my vision was to create the most '*productive place on the planet for the OWASP community*' , so any idea that helped with that, was accepted (and any that didn't, was strongly opposed)
- I also take the view that only 75% (or less) of my ideas are any good, the problem is that usually when I have those ideas, I don't know which ones are good (and will stick) , so the only way to find out, is to try them out, to drop the bad ones and to evolve the good ones
  - Also my experience is that '*good ideas*' don't just happen. They are an evolution / refactoring of good and bad ideas, up until the moment where it 'just feels right'
- On the topic of *'choosing the moment/timing'* that ideas should gain a wider audience (i.e. when to 'officially' ask for an opinion):
  - If I ask the questions during the **DefCon B)** mode, I usually massively confuse the other side, and they think that I'm crazy and lack focus (i.e. going on all sorts of different directions)
    * This is usually made worse but the speed that I tend to operate at **DefCon B)** mode, when by the time they see my question , I've already tried a bunch of solutions/ideas and most likely are already with another set of chalenges
  - If I ask the questions during the **DefCon D)** mode, I already have a lot of thinking about the problem, and have raised a lot the bar for somebody to productively collaborate.
  - If I ask the questions during the **DefCon E)** mode, its even worse.

A final point I would like to make, is that sometimes the complain made is a variation of _'Dinis is not listening to us and is blocking out our ideas'. _

I'm going to be blunt on this one, but this is usually BS:

- Most of the stuff that I do is in an open environment, so if somebody thinks that their idea is better, they can just get on and do it (and prove me wrong)
- If I (Dinis) was the reason why those ideas never happened (i.e. it was me the blocking factor), then surely, in the cases where I step-down or were not involved any more, those ideas would flourish and eventually happen:
- What usually happens when I leave, is that '*Nothing (major) happens*' (or at least those ideas '*that I was blocking*' dont happen)
- This means that my energy and drive were being used as an excuse for the '*others*' lack of productivity, focus or energy.
- It also means that those ideas '*not accepted by me*' where probably not that good in the first place
- Finally '_not accepting half-baked ideas that dont make sense and (in my view) will not work' _is something that I am VERY guilty off :)

I would also like to add that I always try to do the most ethical and morally-right thing. I'm sure I don't always get it right, but I do genuinely like to help others, and really enjoy making connections and serendipity (i.e. when you grab two separate persons/activities and put them together in an environment where something special happens).

I also like to live by the '*Karma*[19] *points'* model (as in "*...if one sows goodness, one will reap goodness;...*") and never really expect anything directly back after doing a good deed, helping others or just being kind.

[19] http://en.wikipedia.org/wiki/Karma

I guess after all this, I'm not sure how I should change :)

I work hard for the things I believe, I do put in the time/effort, I am still helping others, and I do have good track record of creating 'stuff' that makes a difference.

So I guess, I'll use this post in the future to point to somebody that currently thinks that I'm "*hard to deal with" _and* I "don't listen"_, and just say:

... hey this is how I am....

...sorry about not 'listening' to you...

... got any more ideas about the problem we're trying to solve... :) ....

References and related material

- The Surprisingly Large Cost of Telling Small Lies[20]

[20] http://boss.blogs.nytimes.com/2014/03/11/the-surprisingly-large-cost-of-telling-small-lies

7 Application Security Industry

This section has the following chapters:

Table of Contents[15]

---

[1] /manuscript/7.Security_Industry/Secure_coding_(and_Application_Security)_must_be_invisible_to_developers.md

[2] /manuscript/7.Security_Industry/Blogger_in_HTTP_only_What_Happened_to_HTTPS.md

[3] /manuscript/7.Security_Industry/CI_is_the_Key_for_Application_Security_SDL_integration.md

[4] /manuscript/7.Security_Industry/Etsy.com_-_A_case_study_on_how_to_do_security_right.md

[5] /manuscript/7.Security_Industry/Open_question_to_Etsy_security_team_-_How_can_OWASP_help.md

[6] /manuscript/7.Security_Industry/FLOSSHack_TeamMentor_and_the_sausage_making_process_that_is_software_application_development.md

[7] /manuscript/7.Security_Industry/I_never_liked_the_term_Rugged_Software_what_about_Robust_Resilient_Software.md

[8] /manuscript/7.Security_Industry/Is_there_a_spreadsheet_template_for_Mapping_WebServices_Authorization_Rules.md

[9] /manuscript/7.Security_Industry/The_next_level_App_Security_Social_Graph.md

[10] /manuscript/7.Security_Industry/Trustworthy_Internet_Movement_and_SSL_Pulse.md

[11] /manuscript/7.Security_Industry/Where_to_have_AppSec_Q_n_A_threads_(what_about_Reddit).md

[12] /manuscript/7.Security_Industry/Is_the_TeamMentor_OWASP_Library_content_released_under_an_open_License.md

[13] /manuscript/7.Security_Industry/Reaching_out_to_Developers,_Aspect_is_doing_it_right_with_Contrast.md

[14] /manuscript/7.Security_Industry/My_comments_on_the_SATEC_document_(Static_Analysis_Tool_Evaluation_Criteria).md

[15] ../../Table_of_Contents.md

7.1 Secure coding (and Application Security) must be invisible to developers

At OWASP a while back we come up with the idea that _'…Our [OWASP] mission is to make application security visible…' _and for a while I used to believe in the idea that if only everybody had full visibility into 'Application Security' then we would solve the problem.

But after a while I started to realize that what we need to create for developers, is for 'Application Security' / 'Secure Coding' to be INVISIBLE 99% of the time. It is only the decision makers (namely the buyers) that need visibility into an application secure state

We will never get secure applications at a large scale if we require ALL developers (or even most) to be experts at security domains like Crypo, Authentication, Authorization, Input validation/sanitation, etc…

Note that I didn't say that NOBODY should be responsible for an Application's security. Of course that there needs to be a small subset of the players involved that really cares and understands the security implications of what is being created (we can call these the security champions).

**The core idea is that developers should be using Frameworks, APIs and Languages that allow them to create secure applications by design **(where security is there but is invisible to developers).

And when they **(the developers or architects) **create a security vulnerability, at that moment **(and only then), they should have visibility into what they created **(i.e. the side effects)** and be shown alternative ways to do the same thing in a secure way.**
**

**This is how we can scale, which is why it is critical that OWASP (and anybody who cares about solving the application security problem) needs to focus in improving our Framework's ability to create secure apps.

One key problem that we still have today (April 2012) which is preventing the mass 'invisibilitycation of security' at Framework level, is that we are still missing Security-focused SAST/Static-Analysis rules
**

****How we fixed Buffer Overflows**

A very good and successfully example of making security 'invisible' for developers was the removal of 'buffer overflows' from C/C++ to .Net/Java (i.e. from unmanaged to managed code).

Do .NET/Java developers care about overflowing their buffers when handing strings? No, since that is handled by the Framework :)

THAT is how we make security (in this case Buffer Overflow protection) Invisible to developers

The Cooking Analogy
**

**If you are looking for an analogy, "a chef cooking food" is probably the better one.

Think of software developers that are cooking with a number of ingredients (i.e. APIs).

Do you really expect that chef to be an expert on how ALL those ingredients (and tools he is using) were created and behave?

It is impossible, the chef is focused on creating a meal!!!

Fortunately the chef can be confident that some/all of his ingredients+tools will behave in a consistent and well documented way (which is something we don't have in the software world).

I like the food analogy because, as with software, one bad ingredient is all it takes to ruin it.

Related Posts:

- "Making Security Invisible by Becoming the Developer's Best Friends"[16] presentation
- Security evolution into Engineering Productivity[17]

[16] http://diniscruz.blogspot.co.uk/2012/04/making-security-invisible-by-becoming.html
[17] http://diniscruz.blogspot.co.uk/2012/04/security-evolution-into-engineering.html

7.2 Blogger in HTTP only? What happened to HTTPS?

Now that I'm blogging more, I'm finding the need to blog from insecure locations (like a coffee shop or conference).

But unfortunately it doesn't seem to be possible to use SSL with Blogger? WTF! in 2012?

After this 2009 letter[18] Google moved some of its web apps to SSL (see Google's answer at HTTPS security for web applications[19]) but blogger seems to have been missed!

At the moment it doesn't seem to be a way to write a blog post (like this one) without risking my sessionID being compromised. Am I missing something obvious?

Here is are thread Can I use an HTTPS connection for editing and posting on Blogger?[20] (which points to a non-existing thread) that implies that Google doesn't do this due to performance issues.

Also annoying is the fact that https://diniscruz.blogspot.co.uk/[21] doesn't work! So how can I know that this blog's content is read as it was written (ie. without its content being tampered with)

On the topic of OWASP, note how there is no mention to it on the letter[22]. Yes this letter is from 2009 but if it was written today, would OWASP be there? (this is what I'm now calling OWASP MIA (Missing In Action))

On that topic, why don't we write another letter to Google asking for them to extend their security efforts into blogger!

Also, if Google doesn't care about this and give us no solution, what other options do we have? What about a 'cloud' service that gives me secure access to this blog?

[18] http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf
[19] http://googleonlinesecurity.blogspot.co.uk/2009/06/https-security-for-web-applications.html
[20] http://webapps.stackexchange.com/questions/13568/can-i-use-an-https-connection-for-editing-and-posting-on-blogger
[21] https://diniscruz.blogspot.co.uk/
[22] http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf

7.3 CI is the Key for Application Security SDL integration

The more time I spent with CI[23] (namely with TeamCity[24]) the more my instinct is saying_ 'this is how we should be delivering and automating security knowledge!'_.

CI environments (namely its scheduling capabilities) could be use to:

- Create scannable artifacts (i.e. projects, dlls, jars, etc...) for SAST engines
- Create *'live versions'* of the target site (in a clean and pre-populated-with-data states) for DAST engines (and pentest activities)
- Automatically run SAST engines (like cat.net for example)
- Run Unit-tests with further analysis
- Trigger security actions (based on events like Git commits)
- Trigger 'consolidation' analysis (for example of results from multiple tools) and publishing to results into other SDL tools (namely bug tracking systems)
- Modify source-code (to automatically inject security guidance and fixes) – see Fixing/Encoding .NET code in real time (in this case Response.Write)[25] for a cool PoC
- Inject security guidance into the application (maybe even exposing developers to it in the source code :))
- Create and sent reports to multiple stake-holders
- Be the receiving end of security reports

Its the ability to create schedules and triggerable actions that is really getting me excited :)

So maybe what we (app security teams) should be doing is to start our engagements by setting up an CI environment (which would be integrated with the client's CI environment if they had one)

This also goes to the core of the idea that "If we want to fix Security .... we have to fix Development"[26]

In a way that is why was so I interrested in the idea of integrating IBM's AppScan products with their Rational Jazz[27] tools (which have a number of CI/Collaboration capabilities). In fact that is exactly what I described in my IBM AppScan 2011[28] post.

Isn't it amazing that IBM and HP have all the tools needed to create a real powerful (and effective) security remediation ecosystem, but just can't do it for cultural and political reasons?

And btw, OWASP is also completely MIA in the CI field

[23] http://en.wikipedia.org/wiki/Continuous_integration
[24] http://blog.diniscruz.com/search/label/TeamCity
[25] http://o2platform.wordpress.com/2011/11/07/fixingencoding-net-code-in-real-time-in-this-case-response-write/
[26] http://blog.diniscruz.com/2012/10/amazing-presentation-on-integrating.html
[27] https://jazz.net/
[28] http://blog.diniscruz.com/2009/11/part-i-ibm-application-security-related.html

7.4 Etsy.com - A case study on how to do security right?

First a quick disclaimer that as far as I can think of, I don't know anybody at Etsy.com[29] or had any conversations with them in the past.

Following from Nick's presentation on Amazing presentation on integrating security into the SDL[30] , my look into Etsy's Code as Craft [31]blog and my experiment with Graphite[32] (see Measure Anything, Measure Everything, AppSensor and Simple Graphite Hosting[33]).

I have to say that I have been more and more impressed with Etsy's pragmatic and focused approach to application security.

For example check these out:

- Scaling User Security[34] (where they described their experience in: *'Rolling out Full Site SSL'* and '*Two factor authentication'*
- Announcing the Etsy Security Bug Bounty Program[35]
- Couple more posts tagged as 'security': http://codeascraft.etsy.com/category/security/[36]
- Etsy has been one of the best companies I've reported holes to.[37] (reddit thread)
- Effective approaches to web application security[38] (haven't read it but looks like another really 'must see' presentation'

This is 'real-world' stuff and its what happens when there is a good awareness on the importance and need for doing security.

As you can see, here is a team (from management to engineering) that 'gets' application security, and these are the guys that should be driving a number of OWASP's initiatives, since they represent the 'real-world'. Please correct me if I'm wrong, but a google[39] and owasp[40] search (for 'OWASP Etsy') didn't show a lot of joint activity (the best ones where Nick's participation in the AppSec USA and this job post mentioning the OWASP Top 10[41]). It would be great to see Etsy's guys pushing projects like: AppSensor, ESAPI, Zap, Testing+Developer+Code-Review guides, O2, Exams/Certification, etc...

We (OWASP) need to find ways go get these guys more involved and put them on the driving seat.

In fact, for the next OWASP Summit, we have to make sure these guys are there, working collaboratively with the best minds in Application Security :)

[29] http://etsy.com/
[30] http://diniscruz.blogspot.co.uk/2012/10/amazing-presentation-on-integrating.html
[31] http://codeascraft.etsy.com/
[32] http://graphite.wikidot.com/
[33] http://diniscruz.blogspot.co.uk/2012/10/measure-anything-measure-everything.html
[34] http://codeascraft.etsy.com/2012/10/09/scaling-user-security/
[35] http://codeascraft.etsy.com/2012/09/11/announcing-the-etsy-security-bug-bounty-program/
[36] http://codeascraft.etsy.com/category/security/
[37] http://www.reddit.com/r/netsec/comments/vbrzg/etsy_has_been_one_of_the_best_companies_ive/
[38] http://www.slideshare.net/zanelackey/effective-approaches-to-web-application-security
[39] https://www.google.co.uk/search?q=owasp+etsy
[40] https://www.owasp.org/index.php?title=Special%3ASearch&search=etsy&go=Go
[41] http://hire.jobvite.com/Jobvite/Job.aspx?m=n16bCfwE&o=34&j=ouNHVfwD

7.5 Open question to Etsy security team: How can OWASP help?

Since I don't have a direct contact at Etsy[42]'s security team (apart from security-reports@etsy.com), here is the question I would like to ask them (which hopefully will reach the right person).

_Dear Etsy security team, _

How can OWASP help?

By Owasp, I mean OWASP Community (it's projects, chapters, people, ideas, activities, energy).

_From the information posted on your website and presented at conferences, you really take security seriously. _

You have been able to create a productive environment where secure code 'happens', and more importantly, there is a productive and pragmatic relationship between you (the security team), your developers and your management.

So, assuming that you still have a couple things you would like to do better, is there a way (or place, or activity) where OWASP's community can help?

- *Maybe it is in creating better documentation or education materials for your developers/testers?*
- *Maybe its an improved schema for AppSensor that would allow your multiple teams to create even better data (or metadata) for your amazing graphs?*
- *Maybe it is a an special Summit on an topic that you care about? (see the amazing talent that we were able to gather in our last one)*
- *Maybe is better SAST or DAST rules for your tools?*
- *Maybe is better technical (and security focused) information on how Frameworks work and its security implications? (which will help with code reviews and code standards)*
- *Maybe its a working group on CSP (Content Security Policies) to share best-practices and ideas on how to implement them? (with the key players from the browser vendors participating)*
- _Maybe creating a series of events (or even a tour) around OWASP chapters and conferences where you can present your latest ideas and challenges? (the format is up to your imagination and availability) _
- *Maybe its better connectors, parsers or data-transformations for the data you collect using StastD?*
- *….fell free to propose your own (these are just ideas to kickstart the dialogue)*

The idea is to start a collaboration with you.

There is a lot that OWASP can learn from what you are doing, and the more we are able to capture it, the more we can help others who also want to protect their customers, business and applications.

Thanks for your time

Dinis Cruz

Owasp Contributor

---

[42] http://codeascraft.etsy.com/

_Related Etsy posts:

- Etsy.com - A case study on how to do security right?[43]
- Amazing presentation on integrating security into the SDL[44]
- Measure Anything, Measure Everything, AppSensor and Simple Graphite Hosting[45]

[43] http://diniscruz.blogspot.co.uk/2012/10/etsycom-case-study-on-how-to-do.html
[44] http://diniscruz.blogspot.co.uk/2012/10/amazing-presentation-on-integrating.html
[45] http://diniscruz.blogspot.co.uk/2012/10/measure-anything-measure-everything.html

7.6 FLOSSHack TeamMentor and the 'sausage making process' that is software/application development

OWASP's FLOSSHack[46] events are a really powerful initiative.

_"...Free/Libre Open Source Software Hacking (FLOSSHack) events are designed to bring together individuals interested in learning more about application security with open source projects and organizations in need of low cost or pro bono security auditing. FLOSSHack provides a friendly, but mildly competitive, workshop environment in which participants learn about and search for vulnerabilities in selected software. In turn, selected open source projects and qualified non-profit organizations benefit from additional quality assurance and security guidance...." _

_
_See FLOSSHack_One[47] for the details (and vulnerabilities discovered) of the first event.

OWASP's FLOSSHack[48] is one of those 'magical' spaces where the OWASP's community and its projects can come together and add a lot of value.

In fact I remember the idea of doing something like this at the last Summit(s) but we couldn't find a FLOSS or commercial vendor that wanted to 'play the game' :)

And, just for record, I will be happy to help if an OWASP chapter (or University) wants to do a similar FLOSSHack on TeamMentor[49]

Although TeamMentor (TM) is not OpenSource, it is very close, since the source code is available[50] and SI allowed me to 'open it' as much (if not more) as other OpenSource projects (note that TeamMentor uses O2 Platform's FluentSharp APIs[51], and there has been significant changes/features in the latest version of O2[52] which are a direct consequence of my TeamMentor development activities (for example the O2 VisualStudio Extension[53] or the Real-Time Vulnerability Feedback in VisualStudio[54] PoC)).

I'm quite proud of the level of openness that TM has, and I hope that other commercial tools follow these ideas/activities. Here are a couple blog posts I wrote about TM's Security:

- TeamMentor Vulnerability Disclosures: CSRF , ClickJacking and Get Password Hash from Browser Memory[55] - checkout the emdeded pdfs with details of the vulnerabilities
- Couple XSS issues and XSS-By-Design (in TeamMentor)[56] - and why they were not fixed in the current 3.2 release
- 'About' page broken due to ClickJacking protection[57] - good example of the Security TAX that we (developers) have to pay due to security fixes

[46] https://www.owasp.org/index.php/FLOSSHack
[47] https://www.owasp.org/index.php/FLOSSHack_One
[48] https://www.owasp.org/index.php/FLOSSHack
[49] http://owasp.teammentor.net/
[50] https://github.com/TeamMentor-OWASP/Master
[51] https://nuget.org/packages?q=fluentsharp
[52] http://diniscruz.blogspot.co.uk/p/owasp-o2-platform.html
[53] http://visualstudiogallery.msdn.microsoft.com/295fa0f6-37d1-49a3-b51d-ea4741905dc2
[54] http://diniscruz.blogspot.co.uk/p/real-time-vulnerability-feedback-in.html
[55] http://diniscruz.blogspot.co.uk/2012/10/teammentor-vulnerability-disclosures.html
[56] http://diniscruz.blogspot.co.uk/2012/10/couple-xss-issues-and-xss-by-design-in.html
[57] http://diniscruz.blogspot.co.uk/2012/10/about-page-broken-due-to-clickjacking.html

- Creating an TeamMentor Security Bounty Program[58] - still need to publicly launch this, but for all practical purposes it is active
- Test and Hack TeamMentor server with 3.2 RC5 code and SI library[59] - lastest 'please hack TM' invite
- "...O2 in Seattle..." and "...Please Hack TeamMentor (beta)..."[60] - first 'please hack TM' invite sent last year
- On Testing TM WebServices
- Documenting how to test WebServices using scripts - the story so far[61] - see how hard it is to test WebServices in a real-world app
- Creating a spreadsheet with WebService's Authorization Mappings[62]
- Roadmap for Testing an WebService's Authorization Model[63]
- What is the formula for the WebServices Authentication mappings?[64] - spreadsheet template with Authorisation mappings
- Testing TeamMentor 2.0 security using O2[65] - how I used a mix of Static and Dynamic Analysis to test the security of the first TM WebService's refactoring
- SecDDev - Security Driven Development[66] - an interesting idea :)

Note that we really embraced Git and GitHub as part of TeamMentor's development and workflow:

- Pretty cool visualisation of the 'GitHub based' TeamMentor Development+QA+Release workflow[67]
- Master source code: https://github.com/TeamMentor/master[68]
- Bugs and issues: https://github.com/TeamMentor/master/issues[69]
- Version with OWASP Top 10 Library (https://github.com/TeamMentor-OWASP/Master[70]) which you can see in action at http://owasp.teammentor.net[71] (note that this is the full engine with the OWASP LIbrary content released under a CC License[72])
- Bunch of misc code repositories: https://github.com/TeamMentor[73]

My objective is to create a super secure+powerful application, with maximum visibility+openness, while creating documentation on how it happened (which you can see by the current blog posts)

I think that TeamMentor is a good case study for the challenges of writing secure code, since it is a real-world app, with real-world complexity, real-world legacy stuff and real-world security compromises. This is a great

[58] http://diniscruz.blogspot.co.uk/2012/10/creating-teammentor-security-bounty.html
[59] http://diniscruz.blogspot.co.uk/2012/09/test-and-hack-teammentor-server-with-32.html
[60] http://diniscruz.blogspot.co.uk/2011/12/o2-in-seattle-and-please-hack.html
[61] http://diniscruz.blogspot.co.uk/2012/05/documenting-how-to-test-webservices.html
[62] http://diniscruz.blogspot.co.uk/2012/05/creating-spreadsheet-with-webservices.html
[63] http://diniscruz.blogspot.co.uk/2012/05/roadmap-for-testing-webservices.html
[64] http://diniscruz.blogspot.co.uk/2012/05/what-is-formula-for-webservices.html
[65] http://diniscruz.blogspot.com/2012/04/testing-teammentor-20-security-using-o2.html
[66] http://diniscruz.blogspot.co.uk/2012/10/secddev-security-driven-development.html
[67] http://diniscruz.blogspot.co.uk/2012/11/pretty-cool-visualisation-of-github.html
[68] https://github.com/TeamMentor/master
[69] https://github.com/TeamMentor/master/issues
[70] https://github.com/TeamMentor-OWASP/Master
[71] http://owasp.teammentor.net/
[72] http://creativecommons.org/licenses/by/3.0/
[73] https://github.com/TeamMentor

learning opportunity to **look at the 'sausage making process' that is software/application development** (with a bunch of .Net, Asmx, jQuery, Javascript, and xml files which can be easily deployed to the 'cloud'). We always talk how OWASP needs to engage with developers, work with them, help them to secure the app…. well here is a good opportunity to do just that.

I want/need help in securing TeamMentor, and Its not an easy task :)

One area that I really want to move next, is the implementation of AppSensor-like-capabilities so that malicious activities can be detected and mitigated

Oh, and I could really do with a good layer of .NET ESAPI controls/capabilities :)

7.7 I never liked the term 'Rugged Software', what about Robust/Resilient Software?

I still have not fully rationalised why I don't like (as security professional and as a developer) the term (and some parts of the concept) of the Rugged Software[74]

Recently when talking about similar concepts (i.e. writing secure code/applications) I found myself talking about the need to create **Robust/Resilient Applications**.

Isn't **Resilient Software** a better term to describe applications/code that are able to correctly handle, mitigate and react to malicious behaviour/input?

[74] http://www.ruggedsoftware.org/

7.8 Is there a spreadsheet/template for Mapping WebServices Authorization Rules?

What is the best way to map/document the Authorization Rules? (for example of WebServices)

I'm looking for a spreadsheet/template that allows the business-rules (i.e. 'who has access to what') to be mapped, visualized and analyzed.

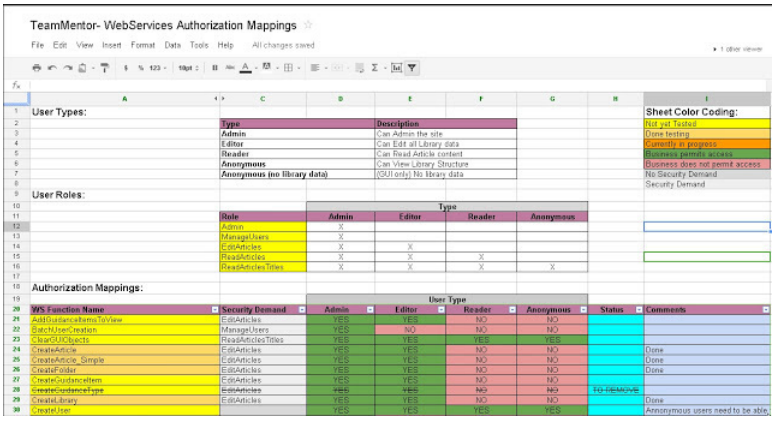
I looked at owasp.org[75] and this is what I found (did I missed something?)

- Guide to Authorization[76]
- Codereview-Authorization[77]
- Testing for Authorization[78]
- Reviewing Code for Authorization Issues[79]
- Cheat Sheets[80] (no Authorization one)

In the past I have created a couple of these (some even with O2 Automation), but NDAs prevented me from sharing. So today, since I'm helping Arvind[81] to create a set of Python scripts to test TeamMentor's WebServices, I took the time to create a model which I think came out quite well.

You can read about it here: Creating a spreadsheet with WebService's Authorization Mappings[82] and this is what it looks like:

https://docs.google.com/a/owasp.org/spreadsheet/ccc?key=0AhHDFVmo550dDZUcDU5eXpGVGFKWDZjS3VGUHdUTXc[83]



Inline images 1

[75] http://owasp.org/
[76] https://www.owasp.org/index.php/Guide_to_Authorization
[77] https://www.owasp.org/index.php/Codereview-Authorization
[78] https://www.owasp.org/index.php/Testing_for_Authorization
[79] https://www.owasp.org/index.php/Reviewing_Code_for_Authorization_Issues
[80] https://www.owasp.org/index.php/Cheat_Sheets
[81] http://diniscruz.blogspot.co.uk/2012/05/creating-spreadsheet-with-webservices.html
[82] http://diniscruz.blogspot.co.uk/2012/05/creating-spreadsheet-with-webservices.html
[83] https://docs.google.com/a/owasp.org/spreadsheet/ccc?key=0AhHDFVmo550dDZUcDU5eXpGVGFKWDZjS3VGUHdUTXc

Since I'm going to integrate this with O2 next, it is better to change it into a better format/standard now (vs later).

I also think that we should have a couple of these templates in an easy to consume format on the OWASP WIki (I have lost count the amount of times that I have tried to explain the need for 'such authorization tables/mappings' without having good examples at hand).

Note that creating these mappings is just one part of the puzzle! Also as important is the ability to keep it well maintained, up-to-date and relevant.

7.9 The next level App Security Social Graph

My core belief is that openness and visibility will eventually create a model/environment where the *'right thing'* tends to happen, since it is not sustainable (or acceptable) to do the '*wrong thing'* (which without that visibility is usually not exposed and contested). See the first couple minutes on the Git and Demoracy presentation[84] for a real powerful example of this *'popular/viral awareness'* in action.

When I look at my country (Portugal and now UK) or my industry (WebAppSec) I see countless examples of scenarios where if information was being disclosed and presented in a consumable way, A LOT of what happens would not be tolerated.

For example, we (in WebAppSec) industry know how bad the software and applications created every day are. And we (and the customers) have accepted that vulnerabilities are just part of creating software, and that the best we can do is to improve the SDL (and reduce risk).

But, if the real scale of the problem was known, would we (as a society or industry) accept it? Would we accept that large parts of our society are built on top of applications that very few people have any idea of how they work? (might as well if they are secure).

So while OWASP is busy booking meetings to have meetings, the rest of the world is moving on, and is trying to find ways to connect data sets in a way that 'reality is understandable/visible', so that what is really going on, is exposed in a easy to consume and actionable way.

For example take a look at the Next Level Doctor Social Graph[85] for an attempt at driving change while trying to figure out a commercially viable way of doing it (check out their '"Open Source Eventually"[86] idea)

[87]

From that page, here is is their description of the problem:

_"It is very difficult to fairly evaluate the quality of doctors in this country. Our State Medical Boards only go after the most outrageous doctors. The doctor review websites are generally popularity contests. Doctors with a good bedside manner do well. Doctors without strong social skills can do poorly, even if they are good doctors. It is difficult to evaluate doctors fairly. Using this data set, it should be possible to build software that evaluates doctors by viewing referrals as "votes" for each other." _(see related reddit thread here[88])

[84] http://diniscruz.blogspot.co.uk/2012/10/a-must-watch-ted-talk-about-git-and.html
[85] http://www.medstartr.com/projects/82-next-level-doctor-social-graph
[86] http://www.medstartr.com/projects/82-next-level-doctor-social-graph
[87] http://3.bp.blogspot.com/-uPYAjZ3sdwc/UI_B3aBGM8I/AAAAAAAABHQ/aIuOMiT-UEs/s1600/Screen+Shot+2012-10-30+at+11.50.18.png
[88] http://www.reddit.com/r/programming/comments/12aocr/doing_hacktivism_right_i_am_crowdfunding_the/

_
_This is what they call the _Next Level Doctor Social Graph _, and when I was reading it I was thinking about doing the same for software/apps under the title: **The next level App Security Social Graph**

Here is the same text with some minor changes (in bold) on what the **The next level App Security Social Graph **could be:

*"It is very difficult to fairly evaluate the quality of __**software/application's security**_* in this country. Our *_**regulators**_* only go after the most outrageous *****incidents/data-breaches*****. The **product/services** websites are generally popularity contests. *_**Applications**_* with a good *_**marketing do**_* well. *_**Applications**_* without strong *_**presentation**_* skills can do poorly, even if they are *_**secure applications**_*. It is difficult to evaluate *_**security**_* fairly. Using this data set, it should be possible to build software that evaluates *_**application's security**_* by viewing *****..... (to be defined)***"_

_
It would be great if the current debate was on that _..... (to be defined) bit (ideally with a number of active experiments going on to figure out the best metrics) … but we quite far away from that world ….

… meanwhile another ***8763*** vulnerabilities (change this value to a quantity you think is right) have just been created since you started reading this post. These 'freshly baked' vulnerabilities are now in some code repository and will be coming soon to an app that you use (and your best defence is to hope that you are not caught by its side-effects)

7.10 Trustworthy Internet Movement and SSL Pulse

Ivan[89]'s interesting work at Qualys continues with the launch of the Trustworthy Internet Movement[90] (TIM) and SSL Pulse[91] at RSA.

There are a number of interesting developments here:

- Great presentation and message
- Real nice project page for SSL-Pulse: https://www.trustworthyinternet.org/ssl-pulse/[92]
- Good funded project: Its looks like they started with 500k USD investment[93] from Philippe Courtot[94]
- Some efforts at creating a community (with a Join the Movement[95]) although it doesn't say what happens next
- Reuse of Ivan's SSL Labs great work gives this 'Movement' a good momentum
- Now look at they fundamentals (*'Innovation, Collaborate, Individual Expertise'*), principle (*'TIM's mission is to resolve major lingering security issues on the Internet, such as SSL governance and the spread of botnets and malware, by ensuring security is built into the very fabric of private and public clouds, rather than being an afterthought.'*) and Target Audience (*'Experts, Innovators and Technical gurus, Stakeholders, Corporations, Academic institutions and non-profit organizations, Angel investors and VCs'*)
  - Quite a targeted audience
  - Will be interesting to see who joins and provides financial backing
  - Its quite SSL focused, there is a lot more to cloud security than SSL :)
  - No reference to openness :)
  - It sounds a lot like the model Mark Curphey wishes OWASP would follow[96] :)

So at the moment this is basically a good Qualy's branding exercise, and will help a bit to improve the WebApp security world, but the key question is if there will be community adoption/participation and if others will join the party.

There is nothing wrong with what Qualys is doing, and the fact that this investment (on Application Security) is happening outside of OWASP shows that OWASP doesn't currently have a model/structure that promotes this type of collaboration. And that is very unfortunate, since in terms of worldwide community and reach there is SO much OWASP could do to help this type of initiative.

[89] http://blog.ivanristic.com/
[90] https://www.trustworthyinternet.org/
[91] https://www.trustworthyinternet.org/ssl-pulse/
[92] https://www.trustworthyinternet.org/ssl-pulse/
[93] http://www.networkworld.com/news/2012/030512-courtot-internet-security-256945.html
[94] https://www.trustworthyinternet.org/philippe-courtot/
[95] https://www.trustworthyinternet.org/join/
[96] http://www.curphey.com/category/owasp/

7.11 Where to have AppSec Q&A threads (what about Reddit?)

Note: I wrote this a while back but somehow was stuck on my 'Drafts' folder (but the question is still relevant in March 2013)

So it looks like StackExchange Security is not going to work for WebAppSec and OWASP (since this question is exactly the type of question we should would like to see there How to implement url encryption on .xsl page using OWASP ESAPI?[97] and that has been closed)) . That said, there are a couple good Q&A on the OWASP tag: http://security.stackexchange.com/questions/tagged/owasp[98]

/div>

And yes we have theSecurity 101[99] maling list but that is not really working (look at the traffic) and, practically mailman sucks for this kind of things since we really need something with a threaded/social discussion environment (like StackExchange or Reddit)

**So what about Reddit? **I really like its GUI/Workflow, already use it quite a lot and we already have a nice home there: http://reddit.com/r/owasp[100]

For example I just posted this question there: http://www.reddit.com/r/owasp/comments/10ayls/secure_-spring_frameworkuser_management/[101] (and in Security StackExchange[102])... let's see what happens :)

For this to work we need to make sure that owasp reddit community gets some viewing and that there is a way to create regular updates on what is going on in there.

What do you think?

---

[97] http://security.stackexchange.com/questions/18925/how-to-implement-url-encryption-on-xsl-page-using-owasp-esapi
[98] http://security.stackexchange.com/questions/tagged/owasp
[99] http://lists.owasp.org/pipermail/security101/
[100] http://reddit.com/r/owasp
[101] http://www.reddit.com/r/owasp/comments/10ayls/secure_spring_frameworkuser_management/
[102] http://security.stackexchange.com/questions/20534/secure-spring-frameworkuser-management

7.12 Is the TeamMentor's OWASP Library content released under an open License?

Following the FLOSSHack TeamMentor[103] thread, Jerry Hoff asked *"Is the content in http://owasp.teammentor.net/teamMentor[104] creative commons? Can we use it to freely fill out more of the cheat sheets and use in tutorial videos and so forth?"*

And the answer is: **YES**

Here is the repository for the XML files: https://github.com/TeamMentor-OWASP/Library_OWASP[105]

There are a bunch of (O2 based) tools to consume this content directly, or alternatively you can use the TeamMentor CoreLib from NuGet[106] (which has all the classes and APIs needed)

Note that you can also link directly to the content (articles, libraries, folders or views) :

- by title https://owasp.teammentor.net/article/How_to_Protect_From_Injection_Attacks_in_ASP.NET[107]
- by title https://owasp.teammentor.net/article/How_to_Encrypt_Configuration_Sections_in_ASP.NET_-Using_DPAPI[108]
- by title (on articles with the same title):
- https://owasp.teammentor.net/article/All_Database_Input_Is_Validated[109] (Asp.Net 3.5 version)
- https://owasp.teammentor.net/article/All_Database_Input_Is_Validated[OWASP]Java[110] (Java version)
- by GUID: https://owasp.teammentor.net/article/56b0552d-2ceb-4714-a8f1-20a6a8609874[111]
- by View or folder: sometimes is more user friendly to only expose to the end user (for example) the articles in the A08: Failure to Restrict URL Access[112] view (instead of the whole TM GUI: https://owasp.teammentor.net[113])

In addition to the 'article' pages (linked above) you can also see/consume the content using:

- **raw**:https://owasp.teammentor.net/raw/All_Database_Input_Is_Validated[114] (this is what the xml file stored in disk looks like)
- **html**: https://owasp.teammentor.net/html/56b0552d-2ceb-4714-a8f1-20a6a8609874[115] (direct html page with no AJAX loading or editing capabilities) - TM suports wikitext, xml and xsl content, but I think that all articles in this library are HTML based

[103] http://diniscruz.blogspot.com/2012/11/flosshack-teammentor-and-sausage-making.html
[104] http://owasp.teammentor.net/teamMentor
[105] https://github.com/TeamMentor-OWASP/Library_OWASP
[106] http://nuget.org/packages/TeamMentor.CoreLib
[107] https://owasp.teammentor.net/article/How_to_Protect_From_Injection_Attacks_in_ASP.NET
[108] https://owasp.teammentor.net/article/How_to_Encrypt_Configuration_Sections_in_ASP.NET_Using_DPAPI
[109] https://owasp.teammentor.net/article/All_Database_Input_Is_Validated
[110] https://owasp.teammentor.net/article/All_Database_Input_Is_Validated%5EOWASP%5EJava
[111] https://owasp.teammentor.net/article/56b0552d-2ceb-4714-a8f1-20a6a8609874
[112] http://owasp.teammentor.net/teamMentor#load:e07b04c5-67f9-49a4-88fe-1b9ee8511da3&showFilters:false&showTree:false&centerGuidanceItems:true
[113] https://owasp.teammentor.net/
[114] https://owasp.teammentor.net/raw/All_Database_Input_Is_Validated
[115] https://owasp.teammentor.net/html/56b0552d-2ceb-4714-a8f1-20a6a8609874

- **content**: https://owasp.teammentor.net/content/56b0552d-2ceb-4714-a8f1-20a6a8609874[116] (the article's Html content with no TM Branding)
- **jsonp**: https://owasp.teammentor.net/jsonp/56b0552d-2ceb-4714-a8f1-20a6a8609874[117] (to allow the easy consumption of TM content without worrying about that annoying ***same origin policy*** security protection :))
- **wsdl**: http://owasp.teammentor.net/aspx_pages/tm_Webservices.asmx[118] - note: if you want to fuzz this, I can set-up a dedicated cloud version for you (on AppHarbor or Azure)

For reference the TM Documentation is at: https://docs.teammentor.net[119]

The page https://docs.teammentor.net/xml/Eval[120] contains 4 videos and a download link (that points to the GitHub version) which allow you to run TM locally (btw look at the source code of that page and see some XML+XSL foo action :))

[116] https://owasp.teammentor.net/content/56b0552d-2ceb-4714-a8f1-20a6a8609874
[117] https://owasp.teammentor.net/jsonp/56b0552d-2ceb-4714-a8f1-20a6a8609874
[118] http://owasp.teammentor.net/aspx_pages/tm_Webservices.asmx
[119] https://docs.teammentor.net/
[120] https://docs.teammentor.net/xml/Eval

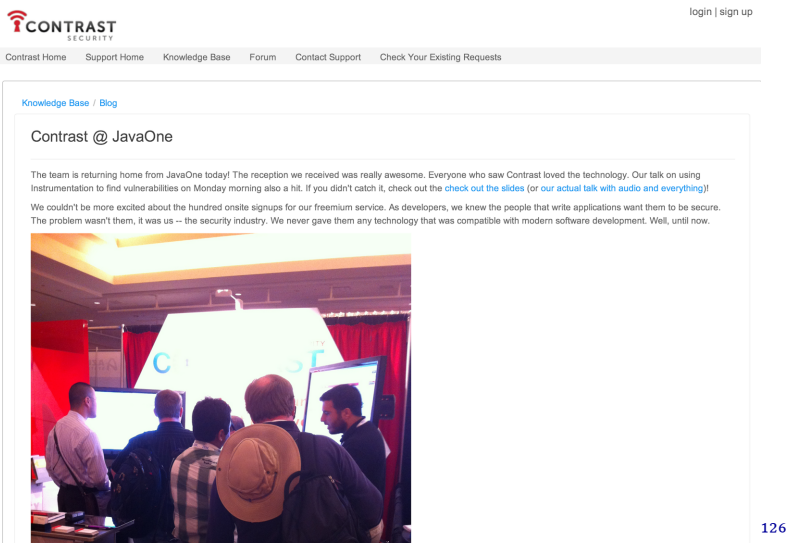
7.13 Reaching out to Developers, Aspect is doing it right with Contrast

UPDATE: I got the dates wrong when I posted this. The Contrast blog post and presentation are from 2012, it is the award that is from 2013:

In case you missed it OWASP's long time contributor Aspect Security [121]were at Java One[122] conference in presenting their (commercial) product Contrast[123].

I was not there, but from the noises I'm hearing it was quite a successull event, with lots of developers reached.

Here is a cool picture from their Contrast @ JavaOne[124] post (which contains a link to their presentation [125](also embedded below));



126

The presentation is a good overview of how their technology works, and although those 'fake tweets' are bit too much me, this is a great 'soft' sales pitch for their product.

I wished they had resisted the cheap-shots at the other Dynamic/Static products/solutions, since to solve the web application security problem, we need all available technologies to work together (not against each other).

It would also had been amazing if this technology was open source, but that is another example of the failure of Open Source to create viable business models for companies like Aspect.

That said, compared with the other tool vendors Aspect and Contrast are a breath of fresh air (and I still have to follow up on Jeff's and Arshan's offer to get a proper demo of Contrast (I need to find a project to use it)

[121]https://www.aspectsecurity.com/
[122]http://www.oracle.com/javaone/index.html
[123]https://www.aspectsecurity.com/contrast/
[124]https://support.contrastsecurity.com/entries/22113601-Contrast-JavaOne
[125]http://myexpospace.com/JavaOne2012/SessionFiles/CON6071_PDF_6071_0001.pdf
[126]http://3.bp.blogspot.com/-iBd_SlIgjU8/UkF4sd2ul_I/AAAAAAAADh0/odecfKQp9VY/s1600/Screen+Shot+2013-09-24+at+12.33.06.png

So congratulations to Aspect for focusing on developers, for trying to inject security deep into the SDL (where it needs to be) and for winning a 2013 Duke's Choice Awards[127]:

2013 Duke's Choice Awards

Duke's Choice Award 2013

Oracle Announces Winners of the 2013 Duke's Choice Awards!

Winners Demonstrate Diverse, Java-Powered Technologies to the Java Community at JavaOne San Francisco 2013.

In conjunction with JavaOne San Francisco 2013, Oracle and the Java Community are recognizing 11 organizations and developers as the winners of the 11th annual Duke's Choice Awards for their creative and innovative uses of Java technology. The 11th annual Duke's Choice Award winners were selected by a multi-part process. First, the Java community was asked to submit nominations to this year's judges. Next, the judges selected nine Duke's Choice Award winners and five candidates for the Community Choice Award. Finally, Community Choice Award nominees were posted on java.net, and all members of the Java community were invited to vote for their favorite. This year's Community Choice Award was received by two companies in a tie decision. The winners were JFrog for its Bintray social network for developers, and Contrast Security for its Java Platform, Enterprise Edition (Java EE) security plug-in, Contrast.

The winners of the 2013 Duke's Choice Award are:

Contrast Security
One of two Community Choice Award recipients, Maryland-based Contrast Security uses Java EE for its Contrast security plug-in, which leverages the Java Virtual Machine (JVM) to invisibly monitor applications and automatically identify security vulnerabilities.

DEVOXX
Devoxx4Kids is a program from the team behind one of the world's largest Java developer conferences, DEVOXX. Through the program, children ages 8 to 14 can attend sessions to learn computer programming and logic in languages other than English, in order to create computer games, program robots and learn about electronics.

[128]

**Presentation: Using ****Instrumentation to Find Security Vulnerabilities in JaveEE Applications **

…. as used by commercial product: Contrast

… I wonder if there are open source alternatives of this technique :)

[127] https://www.java.net//dukeschoice

[128] http://2.bp.blogspot.com/-sG8ET_KYi_8/UkF8YigalMI/AAAAAAAADiA/qm8oPshvyHk/s1600/Screen+Shot+2013-09-24+at+12.46.03.png

7.14 My comments on the SATEC document (Static Analysis Tool Evaluation Criteria)

(submitted today to the wasc-satec@lists.webappsec.org list)

A bit late (deadline for submission is today) but are my notes on the version currently at http://projects.webappsec.org/w/page/4

My comments/notes are marked as *Conted to add in underscore, bold and Italic* or ***[content to be deleted in red]***

When I wanted to make a comment on particular change or deletion, I did it on a new line:

DC Comment: … a comment goes here in dark blue

Of course that this is my opinion, and these notes are based on the notes I took in 'analogue mode' (i.e. on paper :))

Table of Contents:

Introduction:

Static Code Analysis is the analysis of software code ***[without actually executing the binaries resulting from this code]***.

> *DC Comment: we don't need the extra definition, since it is possible to do static code analysis based on information/code/metadata obtained at run-time or via selective execution/simulation of the code/binaries. The key concept is that static analysis is about analysing and applying rules to a set of artefacts that have been extracted from the target application. From this point of view, we can do static analysis on an AST (extracted from source code), an intermediate representation (extracted from a .net or java binary) or run-time traces (extracted from a running application). We can also do static analysis on an application config files, on an application's authorisation model or even on application specific data (for example the security controls applied to a particular asset)*

Static code analysis aims at automating code analysis to find as many common ***[quality and]*** security software issues as possible. There are several open source and commercial analyzers available in the market for organizations to choose from.

DC Comment: it doesn't make sense to add 'quality' to mix (in fact the more I read this document the more I thought that the word 'security' should be part of the title of this document/criteria. Quality is a massive area in its own right, and apart form this small comment/reference, there is not a lot of 'software quality' on this document. This is a a document focused on Software security issues :) , and yes security is a sub-set of quality (which is ok if referenced like that)

Static code analysis analyzers are rapidly becoming an essential part of every software organization's application security assurance program. Mainly because of the analyzers' ability to analyze large amounts

[129] http://projects.webappsec.org/w/page/41188978/Static%20Analysis%20Tool%20Evaluation%20Criteria

of source code in considerably shorter amount of time than a human could, __**and the ability to automate security knowledge and workflows**__

—
—

DC Comment: The key advantage of static analysis is that it can codify an application security specialist knowledge and workflows. By this, I mean that for the cases where it is possible to codify a particular type of analysis (and not all types of analysis can be automated), these tools can perform those ***analysis in a repeatable, quantifiable and consistent way****. Scanning large code-bases is important, but more important is the ability to scale security knowledge, specially since I've seen cases where 'large code scans' where achieved by dropping results or skipping certain types of analysis-types (in fact most scanners will scan an app of any size if you delete all its rules :))*

The goal of the SATEC project is to create a vendor-neutral document to help guide application security professionals during __**the creation of an** __source-code driven security __**programme**__ ***[assessments]***. This document provides a comprehensive list of features that should be considered when __**evaluating**__-***[conducting]*** *_** **a security code ****__Tool__** ** ****[review]**_. Different users will place varying levels of importance on each feature, and the SATEC provides the user with the flexibility to take this comprehensive list of potential analyzer features, narrow it down to a shorter list of features that are important to the user, assign weights to each feature, and conduct a formal evaluation to determine which scanning solution best meets the user's needs.

The aim of this document is not to define a list of *requirements* that all static code analyzers must provide in order to be considered a "complete" analyzer, and evaluating specific products and providing the results of such an evaluation is outside the scope of the SATEC project. Instead, this project provides the analyzers and documentation to enable anyone to evaluate static code analysis analyzers and choose the product that best fits their needs. NIST Special Publication 500-283, "Source Code Security Analysis Analyzer Functional Specification Version 1.1", contains minimal functional specifications for static code analysis analyzers. This document can be found at http://samate.nist.gov/index.php/Source_Code_Security_Analysis.html[130].

**Target Audience: **

The target audience of this document is the technical staff of software organizations who are looking to automate parts of their source code driven security testing using one or more static code analyzers,__**and application security professionals (internal or external to the organisation) that responsible for performing application security reviews**__. The document will take into consideration those who would be evaluating the analyzer and those who would actually be using the analyzer.

**Scope: **

The purpose of this document is to develop a set of criteria that should be taken into consideration while evaluating Static Code Analysis ***Tools [analyzers]*** for security testing.

DC Comment (and rant): OK, WTF is this 'Analysis Analyzers' stuff!!! This is about a ***Tool*** *right? of course that a tool that does software analysis, is an analyzer, but saying that it we are talking about a code analysis analyzer sounds quite redundant :) There is TOOL in the name of the document, and we are talking about tools. In fact, these static analysis tools perform a bunch of analysis and more importantly (as multiple parts of this document cover), the **Analyzer **part of these analysis tools is just **one **of its required/desired*

[130] http://samate.nist.gov/index.php/Source_Code_Security_Analysis.html

features (for example enterprise integration and deployability are very important, and have nothing to do with __the 'Analyzer' part.

_
_

If I can't change your mind to change the redundant Analyzer, them you will need to rename this document to SAAEC (Static Analysis Analyzer Evaluation Criteria), actually what about the SAAEA (Static Analysis Analyzer Evaluation Analysis) :)

Every software organization is unique in their environment. The goal is to help organizations achieve better application security in their own unique environment, the document will strictly stay away from evaluating or rating analyzers. However, it will aim to draw attention to the most important aspects of static analysis ***Tools [analyzers]*** that would help the target audience identified above to choose the best ***Tool [analyzer]*** for their environment and development needs.

Contributors:

Aaron Weaver (Pearson Education)

Abraham Kang (HP Fortify)

Alec Shcherbakov (AsTech Consulting)

Alen Zukich (Klocwork)

Arthur Hicken (Parasoft)

Amit Finegold (Checkmarx)

Benoit Guerette (Dejardins)

Chris Eng (Veracode)

Chris Wysopal (Veracode)

Dan Cornell (Denim Group)

Daniel Medianero (Buguroo Offensive Security)

Gamze Yurttutan

Henri Salo

Herman Stevens

Janos Drencsan

James McGovern (HP)

Joe Hemler (Gotham Digital Science)

Jojo Maalouf (Hydro Ottawa)

Laurent Levi (Checkmarx)

Mushtaq Ahmed (Emirates Airlines)

Ory Segal (IBM)

Philipe Arteau

Sherif Koussa (Software Secured) [Project Leader]

Srikanth Ramu (University of British Columbia)

Romain Gaucher (Coverity)

Sneha Phadke (eBay)

Wagner Elias (Conviso)

Contact:

Participation in the Web Application Security Scanner Evaluation Criteria project is open to all. If you have any questions about the evaluation criteria, please contact Sherif Koussa (sherif dot koussa at gmail dot com)

Criteria:

_
_
DC Comment: I think this criteria should be split into two separate parts:

- ***Operational Criteria **- These are generic items that are desired on any application that wants to be deployed on an enterprise (or to a large number of users). Anything that is not specific to analysing an application for security issues (see next point) should be here. For example installation, deployability, standards, licensing, etc.. (in fact this could be a common document/requirement across the multiple WASC/OWASP published criterias)*
- _**Static Analysis Criteria - **Here is where all items that are relevant to an static analysis tool should exist. These items should be specific and non-generic. For example _
- ***'the rules used by the engine should be exposed and consumable' **is an operational criteria (all tools should allow that)*
- ***'the rules used by the engine should support taint-flow analysis'** is an static analysis criteria (since only these tools do taint-flow analysis)*

Below I marked each topic with either [Operational Criteria] or [Static Analysis Criteria]

1. Deployment:** **

Static code analyzers often represent a significant investment by software organizations looking to automate parts of their software security testing processes. Not only do these analyzers represent a monetary investment, but they demand time and effort by staff members to setup, operate, and maintain the analyzer. In addition, staff members are required to check and act upon the results generated by the analyzer. Understanding the ideal deployment environment for the analyzer will maximize the derived value, help the organization uncover potential security flaws and will avoid unplanned hardware purchase cost. The following factors are essential to understanding the analyzer's capabilities and hence ensuring proper utilization of the analyzer which will reflect positively on the analyzer's utilization.

1.1 Analyzer Installation Support:** **[Operational Criteria]*

A static code analyzer should provide the following :

- **Installation manual: **specific instructions on installing the analyzer and its subsystems if any (e.g. IDE plugins) including minimum hardware and software requirements.
- **Operations manual: **specific and clear instructions on how to configure and operate that analyzer and its subsystems.
- **SaaS Based Analyzers: **since there is no download or installation typically involved in using a SaaS based analyzer, the vendor should be able to provide the following:
- Clear instructions on how to get started.
- Estimated turn-around time since the code is submitted until the results are received.
- What measures are being taken to keep the submitted code or binaries as well as to the reports confidential.

1.2 Deployment Architecture:** *[Operational Criteria]*

Vendors provide various analyzer deployment options. Clear description of the different deployment options must be provided by the vendor to better utilize the analyzer within an organization. In addition, the vendor must specify the optimal operating conditions. At a minimum the vendor should be able to provide:

- The type of deployment: server-side vs client-side as this might require permissions change or incur extra hardware purchase.
- Ability to run simultaneous scans at the same time.
- The analyzers capabilities of accelerating the scanning speed (e.g. ability to multi-chain machines, ability to take advantage of multi-threaded/multi-core environments, etc)
- The ability of the analyzer to scale to handle more applications if needed.

1.3 Setup and Runtime Dependencies:** *[Static Analysis Criteria]*

The vendor should be able to state whether the ***Tool [analyzer]*** uses a compilation based analysis or source code based analysis.

- Compilation based analysis: where the ***Tool [analyzer]*** first compiles the code together with all dependencies, or the analyzer just analyses the binaries directly. Either ways, the analyzer requires all the application's dependencies to be available before conducting the scan, this enables the analyzer to scan the application as close to the production environment as possible.
- Source code based analysis: does not require dependencies to be available for the scan to run. This could allow for quicker scans since the dependencies are not required at scan time.
- **__Dynamic based analysis: where the tool analyzes data collected from real-time (or simulated) application/code execution (this could be achived with AOP, code instrumentation, debugging traces, profiling, etc..)__**

2. Technology Support:** *[Static Analysis Criteria]*

Most organizations leverage more than one programming language within their applications portfolio. In addition, more software frameworks are becoming mature enough for development teams to leverage and use across the board as well as a score of 3rd party libraries, technologies, libraries which are used both on the

server and client side. Once these technologies, frameworks and libraries are integrated into an application, they become part of it and the application inherits any vulnerability within these components.

2.1 Standard Languages Support:** ***[Static Analysis Criteria]*

Most of the analyzers support more than one programming language. However, an organization looking to ***use [acquire]*** a static code analysis ***Tool [analyzer]*** should make an inventory of all the programming languages, and their versions, used within the organizations as well as third party applications that will be scanned as well. After shortlisting all the programming languages and their versions, an organization should compare the list against the ***Tool's [analyzer's]*** supported list of programming languages and versions. Vendors provide several levels of support for the same language, understanding what level of support the vendor provides for each programming language is key to understanding the coverage and depth the analyzer provides for each language. One way of understanding the level of suppor__**t**__ for a particular language is to inspect the ***Tool's*** **_[analyzer's]** _signatures (AKA Rules or Checkers) for that language.

DC Comment: very important here is to also map/define if these rules are generic or framework/version specific. For example do all java rules apply to all java code, or are there rules that are specific to particular version of Java (for example 1.4 vs 1.7) or Framework (for example spring 1.4 vs 2.0).

_
_

This is really important because there are certain vulnerabilities that only exist on certain versions of particular frameworks. For example, I __believe that the HttpResponse.Redirect in the version 1.1 of the .NET Framework was vulnerable to Header Injection, but that was fixed on a later release. Static code analysis should take this into account, and not flag all unvalidated uses of this Redirect method as Header Injection vulnerabilities.

2.2 Programming Environment Support:** ***[Static Analysis Criteria]*

Once an application is built on a top of a framework, the application inherits any vulnerability in that framework. In addition, depending on how the application leverages a framework or a library, it can add new attack vectors. *It is very important for the analyzer to be able to be able to trace tainted data through the framework as well as the custom modules built on top of it.*

DC Comment: No, I don't agree with the underscored line above. ***What is important is to understand HOW the frameworks work/behave***

_
_

Also this comment doesn't make a lot of sense in the way most (if not all) current static analysis is done. There are two key issues here

_
_

#1) what is the definition of a 'Framework'

#2) what does it mean to 'trace tainted data through the framework'

_
_

On #1, unless we are talking about C/C++ (and even then) most code analysis is done on Frameworks. I.e. everything is a framework (from the point of view of the analysis engine). The analysis engine is 'told' that a particular method behaves in a particular way and it bases its analysis based on that

_
_

From the point of view of a scanning engine, there is no difference between the way asp.net aspx works, vs the way the asp.net mvc framework behaves. Same thing for java, where from the scanning engine point of view there is no difference between the classes in a JRE (see _http://hocinegrine.com/wp-content/uploads/2010/03/jdk_-jre.gif_) and Spring Framework classes_

_
_

In fact most static analysis is done based on:

_
_

*- **sources**: locations of the code that are known to have malicious data (which we call tainted data)*

*- **taint propagators** : methods that will pass tainted data to one of its parameters or return value*

*- **validators**: methods that will remove taint (ideally not blankly but based on a particular logic/vulnType)*

*- **reflection/hyper-jumps/glues**: cases where the application flow jumps around based on some (usually framework-driven) logic*

*- **sinks**: methods that are known to have a particular vulnerability (and should not be exposed to tainted data)*

*- **application control flows** : like **if** or **switch** statements which affect the exposure (or not) to malicious/taint data*

*- **application logic**: like mapping the authorization model and analysing its use*

_
_

The way most analysis is done, is to have rules that tell the engine how a particular method works. So in the .NET framework, the tools don't analyse Request.Querystring or Response.Write. They are 'told' that one is a source and the other is a sink. In fact, massive blind spots happen when there are wrappers around these methods that 'hide' their functionality from the code being analysed.

_
_

*Even on C, there is usually a rule for _**strcpy*** which is used to identify buffer overflows. Again most scanners will miss methods that have the exact same behaviour as _**strcpy **but are called something differently (in fact, I can write such methods C# that are vulnerable to buffer overflows which will missed by most (if not all) current tools :)).

On the #2 point, yes ideally the scanners should be scanning the inside of these methods, but most scanners (if not all) would blow up if they did.

And even if they did it, it wouldn't really work since each vulnerability has a particular set of patterns and context.

So what does it mean *'to trace tainted data through frameworks'*? Are we talking about being able to follow taint over a sequence like this:

a) **request starts** on a **view** that is posting data to a

b) **controller** that sends the data to the

c) **business/db layer **which does something with it, and sends the result to a

d) **view** that **displays** the **result** to user?

THIS is what I think it is important. I.e. we are able to analyze data based on the actual call-flow of the application.

So in a way, we don't need to 'trace data' ***through*** the frameworks (as in ***'what is going on inside'***) but on **top of the frameworks **(as in ****'what code is touched/executed***)

This is actually where the new type of scanners which do a mix of static and dynamic analysis (like seeker, contrast, glass box stuff from IBM, etc…) have a big advantage (vs traditional AST or binary-based scanners), since they can actually 'see' what is going on, and know (for example) which view is actually used on a particular controller.

At large, frameworks and libraries can be classified to three types:

- **Server-side Frameworks**:frameworks/libraries that reside on the server, e.g. Spring, Struts, Rails, .NET etc
- **Client-side Frameworks**:which are the frameworks/libraries that reside on browsers, e.g. JQuery, Prototype, etc
- **__where is the 3rd type?__**

DC Comment: these 'types of framework' doesn't make sense here (i.e these are not really different 'types of frameworks', just different execution engines.

Now on the topic of **client-side and server-side code**, the real interesting questions are:

- Can the tool 'connect' traces from server-side code to traces on the client-side code?
- Can the tool understand the context that the server-side code is used on the client side (for example the difference between a Response.Write/TagLib been used to output data into a an HTML element or an HTML attribute)

Understanding the relationship between the application and the frameworks/libraries is key in order to detect vulnerabilities resulting from the application's usage of the framework or the library, and the following in particular:

- identify whether the application is using the framework in a insecure manner.
- The analyzer would be able to follow tainted data between the application and the framework.

- The analyzer's ability to identify security misconfiguration issues in the framework\library.
- Well-known vulnerability identified by the Common Vulnerabilities and Exposures[131] (CVE)

DC Comment: see my point above about everything being a framework, and in fact, what happens is that most apps are made of:

a) language APIs

b) base class APIs

c) 3rd party frameworks that extend the base class APIs with new functionality

d) in-house APIS

Which all behave like 'frameworks'

Which means, that the first important question to ask is: **What is the level of Framework support that a particular tool has?**

The 2nd (and what I like about the items listed above) is the import question of: **Is the Framework(s) being used securely?**

**

**

The 2nd point is very important, since even frameworks/apis that are designed to provide a security service (like an encoding/filtering/authentication api) can be used insecurely

In a way, what we should be asking/mapping here is: What are the known issues/vulnerabilities that the tool is able to detect?

Note: one of the areas that we (security industry) is still failing a lot, is in helping/pushing the framework vendors to 'codify how their frameworks' behaves, so that our tools/manual analysis know what to look for

2.3 Industry Standards Aided Analysis:** **

Industry standard weaknesses classification, e.g. OWASP Top 10[132], CWE/SANS Top 25[133], WASC Threat Classification[134], DISA/STIG[135] etc provide organizations with starting points to their software security gap analysis and in other cases these calssifications become metrics of minimum adherence to security standards. Providing industry standard aided analysis becomes a desirable feature for many reasons.

DC Comment: I don't understand the relevance of this 2.3 item (in this context). These 'standards' are more relevant in the list of issues to find and in vulnerability discovery __repairing

2.4 Technology Configuration Support:** ***[Static Analysis Criteria]*

Several tweaks provided by the analyzer could potentially uncover serious weaknesses.** **

- ****Configuration Files Redefinition: **** configurations to other file types (e.g. *.ini, *.properties, *.xml, etc). It is a desirable and a beneficial feature to configure the analyzer to treat a non-standard extension as a configuration file.

[131] http://cve.mitre.org/
[132] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[133] http://www.sans.org/top25-software-errors/
[134] http://projects.webappsec.org/w/page/13246970/Threat%20Classification%20Enumeration%20View
[135] http://www.disa.mil/

- **Extension to Language Mapping: **the ability to extend the scope of the analyzer to include non-standard source code file extensions. For example, JSPF are JSP fragment files that should be treated just like JSP files. Also, HTC files are HTML fragment files that should be treated just like HTML files. PCK files are Oracle's package files which include PL/SQL script. While a analyzer does not necessarily have to understand every non-standard extension, it should include a feature to extend its understanding to these extensions.

_DC Comment: The key issue here is for the Tool to understand how the target app/framework behaves. And that is only possible if the artefacts used by those frameworks are also analyzed. _

_
_

I would propose that we rename this section as 'Framework configuration support' and add more examples of the types of 'thing's that need to be looked at (for example the size of Models in MVC apps which could lead to Mass-Assignment/Auto-Binding vulnerabilities)

3. Scan, Command and Control Support:** ***[Operational Criteria]*

The scan, command and control of static code analysis analyzers has a significant influence on the user's ability to configure, customize and integrate the analyzer into the organization's Software Development Lifecycle (SDLC). In addition, it affects both the speed and effectiveness of processing findings and remediating them.

3.1 Command line support:** ***[Operational Criteria]*

The user shouldbe able to perform scans using the command line which is a desirable feature for many reasons, e.g. avoiding unnecessary IDE licensing, build system integration, custom build script integration, etc. For SaaS based tools, the vendor should be able to indicate whether there are APIs to initiate the scan automatically, this becomes a desirable feature for scenarios involving large number of applications.

3.2 IDE integration support:** ***[Operational Criteria]*

The vendor should be able to enumerate which IDEs (and versions) are being supported by the analyzer being evaluated, as well as what the scans via the IDE will incorporate. For example, does an Eclipse plugin scan JavaScript files and configuration files, or does it only scan Java and JSP files.

*DC Comment: the key question to ask here is __**WHO is doing the scan? **I.e is the scan actually done by the IDE's plugin (like on Cat.net case) or the plug-in is just a 'connector' into the main engine (running on another process or server). Most commercial scanners work in the later way, where the IDE plugins are mainly used for: scan triggers, issues view, issues triage and reporting*

3.3 Build systems support: *[Operational Criteria]*

The vendor should be able to enumerate the build systems supported and their versions (Ant, Make, Maven, etc). In addition, the vendor should be able to describe what gets scanned exactly in this context.

3.4 Customization:** ***[Static Analysis Criteria]*

The analyzer usually comes with a set of signatures (AKA as rules or checkers), this set is usually followed by the analyzer to uncover the different weaknesses in the source code. Static code analysis should offer a way to extend these signatures in order to customize the analyzer's capabilities of detecting new weaknesses, alter the way the analyzer detect weaknesses or stop the analyzer from detecting a specific pattern. The analyzer should allow users to:

- **Add/delete/modify core signatures: **Core signatures come bundled with the analyzer by default. False positives is one of the inherit flaws in static code analysis analyzers in general. One way to minimize this problem is to optimize the analyzer's core signatures, e.g. mark a certain source as safe input.
- **Author custom signatures**: authoring custom signature are used to "educate" the analyzer of the existence of a custom cleansing module, custom tainted data sources and sinks as well as a way to enforce certain programming styles by developing custom signatures for these styles.
- **Training: **the vendor should state whether writing new signatures require extra training.

_
_

DC Comment: customisation is (from my point of view) THE most important __differentiator of an engine (since out-of-the-box most, most commercial scanners are kind-of-equivaleant (i.e. they all work well in some areas and really struggle on others).

_
_

Here are some important areas to take into account when talking about customization:

- *Ability to access (or even better, to manipulate) the internal-representations of the code/app being analysed*
- *Ability to extend the current types of rules and findings (being able to for example add an app/framework specific authorization analysis)*
- *Open (or even known/published) schemas for the tool's: rules, findings and intermediate representations*
- *Ability for the client to publish their own rules in a license of their choice*
- *REPL environment to test and develop those rules*
- *Clearly define and expose the types of findings/analysis that the Tools rules/engine are NOT able to find (ideally this should be application specific)*
- _Provide the existing 'out-of-the-box' rules in an editable format (the best way to create a custom rules is to modify an existing one that does a similar job). This is a very important point, since (ideally) ALL rules and logic applied by the scanning engine should be customizable _
- *Ability to package rules, and to run selective sets of rules*
- *_Ability* to (re)run an analysis for one 1 (one) type of issue_
- *_Ability* to (re)run an analysis for one 1 (one) reported issue (or for a collection of the same issues)_
- *Ability to create unit tests that validate the existence of those rules*
- *Ability to create unit tests that validate the findings provided by the tools*

The last points are very important since they fit into how developers work (focused on a particular issue which they want to 'fix' and move on into the next issue to 'fix')

3.5 Scan configuration capabilities:** ***[Operational Criteria]*

This includes the following capabilities:

- **Ability to schedule scans**: Scans are often scheduled after nightly builds, some other times they are scheduled when the CPU usage is at its minimum. Therefore, it might be important for the user to be able to schedule the scan to run at a particular time. For SaaS based analyzers, the vendor should indicate the allowed window of submitting code or binaries to scan.
- **Ability to view real-time status of running scans: **some scans would take hours to finish, it would be beneficial and desirable for a user to be able to see the scan's progress and the weaknesses found thus far. For SaaS based analyzers, the vendor should be able to provide accurate estimate of the results delivery.
- **Ability to save configurations and re-use them as configuration templates: **Often a significant amount of time and effort is involved in optimally configuring a static code analyzer for a particular application. A analyzer should provide the user with the ability to save a scan's configuration so that it can be re-used for later scans.
- **Ability to run multiple scans simultaneously: **Organizations that have many applications to scan, will find the ability to run simultaneous scans to be a desirable feature.
- **Ability to support multiple users: **this is important for organizations which are planning to rollout the analyzer to be used by developers checking their own code. It is also important for organizations which are planning to scan large applications that require more than one security analyst to assess applications concurrently.
- **_[Static Analysis Criteria]** _**Ability to perform incremental scans: **incremental scans proves helpful when scanning large applications multiple times, it could be desirable to scan only the changed portions of the code which will reduce the time needed to assess the results.

_DC Comment: the ability to perform incremental scans is not really a 'configuration' but it is a 'capability'

_

_

_

DC Comment: On the topic of deployment I would also add a chapter/sections called:

_

_

*****"3.x Installation workflow ****__[Operational Criteria]*

*****

*****

_There should be detailed instructions of all the steps required to install the tool. Namely how to go from a _

a) clean VM with XYZ operating system installed, to

_b) tool ready to scan, to _

c) scan completed"

_

_

***"3.x Scanning requirements ****_[Static Analysis Criteria] _**

**
**

There should be detailed examples of what is required to be provided in order for a (or THE optimal) scan to be triggered. For example some scanners can handle a stand-alone dll/jar , while others need all dependencies to be provided. Also the scanners that do compilation tend to be quite temperamental when the scanning server is not the same as the normal compilation/CI server"

_
_

3.6 Testing Capabilities:** ***[Static Analysis Criteria]*

**
**

DC Comment: In my view this whole section (3.6) should be restructured to match the types of analysis that can be done with static analysis tools.

_
_

For example XSS, SQLi, File transversal, Command Injection, etc... are all '__source to sink' vulnerabilities. Where what matters is the tools ability to follow tainted data across the application (and the ability to add new sources and sinks)

_
_

What I really feel we should be doing here is to map out the capabilities that are important for a static analysis tool, for example:

- **_Taint propagation** (not all do this, like FxCop) _
- *Intra-procedue*
- *Inter-procedue*
- ***Handing of Collections, setters/getters, Hashmaps **(for example is the whole object tainted or just the exact key (and for how long))*
- ***Reflection***
- ***Event driven flows **(like the ones provided by ASP.NET HttpModules, ASP.NET MVC, Spring MVC, etc...)*
- ***Memory/objects manipulations** (important for buffer overflows)*
- ***String Format** analysis (i.e. what actually happens in there, and what is being propagated)*
- ***String** Analysis (for regex and other string manipulations)*
- ***Interfaces** (and how they are mapped/used)*
- ***Mapping views to controllers **, and more importantly, mapping tainted data inserted in model objects used in views*
- ***Views nesting **(when a view uses another view)*
- ***Views use of non-view APIs** (or custom view controls/taglibs)*
- ***Mapping of Authorization and Authentication** models and strategies*

- ***Mapping of internal methods*** *that are exposed to the outside world (namely via WEB and REST services)*
- ***Join traces*** *(this is a massive topic and one that when supported will allow the post-scan handling of a lot of the issues listed here)*
- ***Modelling/Visualization of the real size of Models*** *used in MVC apps (to deal with Mass-Assignment/Auto-binding), and connecting them with the views used*
- ***Mapping of multi-step data-flows*** *(for example data in and out of the database, or multi-step forms/worflows). Think reflected SQLi or XSS*
- **_Dependency injection _**
- ***AoP code*** *(namely cross cuttings)*
- ***Validation/Sanitisation code*** *which can be applied by config changed, metadata or direct invocation*
- ***Convention-based behaviours*** *, where the app will behave on a particular way based on how (for example) a class is named*
- ***Ability to consume data from other tools **(namely black-box scanners, Thread modelling tools, Risk assessment, CI, bug tracking, etc..), including other static analysis tools*
- ***List the type of coding techniques that are 'scanner friendly' **, for example an app that uses hashmaps (to _move data around) _or has a strong event-driven architecture (with no direct connection between source and sink) is not very static analysis friendly*
- *....there are more, but hopefully this makes my point....*

As you can see, the list above is focused on the ***capabilities of static analysis tool,*** *not on the type of issues that are 'claimed' that can be found.*

_
_

All tools say they will detect SQL injection, but __what is VERY IMPORTANT (and what matters) is ***the ability to map/rate all this 'capabilities' to the application being tested*** *(i.e asked the question of '**can vuln xyz be found in the target application given that it uses Framework XYZ and is coded using Technique XYZ' **)*

_
_

This last point is key, since most (if not all tools) today only ***provide results/information about what they found and not what they analyzed****.*

****
****

I.e if there are no findings of vuln XYZ? does that mean that there are no XYZ vulns on the app? or the tool was not able to find them?

_
_

In a way what we need is for tools to also report back the ***level of assurance that they have on their results*** *(i.e based on the code analysed, its coverage and current set of rules,* ***how sure is the tool that it found all issues?)***

–
–

Scanning an application for weaknesses is an important functionality of the analyzer. It is essential for the analyzer to be able to understand, accurately identify and report the following attacks and security weaknesses.

- API Abuse
- Application Misconfiguration
- Auto-complete Not Disabled on Password Parameters
- Buffer Overflow
- Command Injection
- Credential/Session Prediction
- Cross-site Scripting
- Denial of Service
- Escalation of Privileges
- Insecure Cryptography
- Format String
- Hardcoded Credentials
- HTTP Response Splitting
- Improper Input Handling
- Improper Output Encoding
- Information Leakage
- Insecure Data Caching
- Insecure File Upload
- Insufficient Account Lockout
- Insufficient Authentication
- Insufficient Authorization
- Insufficient/Insecure Logging
- Insufficient Password Complexity Requirements
- Insufficient Password History Requirements
- Insufficient Session Expiration
- Integer Overflows
- LDAP Injection
- Mail Command Injection
- Null Byte Injection
- Open Redirect Attacks
- OS Command Injection
- Path Traversal
- Race Conditions
- Remote File Inclusion
- Second Order Injection
- Session Fixation

- SQL Injection
- URL Redirection Abuse
- XPATH Injection
- XML External Entities
- XML Entity Expansion
- XML Injection Attacks
- XPATH Injection

4. Product Signature Update: ** ***[Operational Criteria]*

Product signatures (AKA rules or checkers) are what the static code analysis analyzer use to identify security weaknesses. When making a choice of a static analysis analyzers, one should take into consideration the following:

4.1 Frequency of signature update: ****

Providing frequent signature update to a static code analysis ***Tool [analyzer]*** ensure the analyzer's relevance to threat landscape.Hence, it is important to understand the following about a analyzer's signature update:

- Frequency of signature update: whether it is periodically, on-demand, or with special subscription, etc.
- Relevance of signatures to evolving threats: Information must be provided by the vendor on how the products signatures maintain their relevance to the newly evolving threats.

4.2 User signature feedback: ****

The analyzers must provide a way for users to submit feedback on bugs, flawed rules, rule enhancement, etc.

5. Triage and Remediation Support: ***[Static Analysis Criteria]*

A crucial factor in a static code analysis ***Tool [analyzer]*** is the support provided in the triage process and the accuracy, effectiveness of the remediation advice. This is vital to the speed in which the finding is assessed and remediated by the development team.

5.1 Finding Meta-Data: ** **

Finding meta-data is the information provided by the analyzer around the finding. Good finding meta-data helps the auditor or the developer to understand the weakness and decide whether it is a false positive quicker. The analyzer should provide the following with each finding:

- Finding Severity: the severity of the finding with a way to change it if required.
- Summary: explanation of the finding and the risk it poses on exploit.
- Location: the source code file location and the line number of the finding.
- Data Flow: the ability to trace tainted data from a source to a sink and vise versa.

DC Comment: The tool should provide as much as possible (if not all) data that it created (for each issue reported, and the issues NOT reported). There should be a mode that allows the use of the internal representations of the analysis performed, and all the rules that were triggered/used

_
_

5.2 Meta-Data Management: ****

- The analyzer should provide the ability to mark a finding as false positive.
- Ability to categorize false positives. This enforces careful consideration before marking a finding as false positive, it also allows the opportunity to understand common sources for false positives issues, this could help in optimizing the results.
- Findings marked as false positives should not appear in subsequent scans. This is helps avoid repeating the same effort on subsequent scans.
- The analyzer should be able to merge\diff scan results. This becomes a desirable feature if\when the application is re-scanned, the analyzer should be able to append results of the second scan to the first one.
- The vendor should be able to indicate whether the analyzer support the ability to define policies that incorporate flaw types, severity levels, frequency of scans, and grace periods for remediation.

5.3 Remediation Support:

- The analyzer should provide accurate and customizable remediation advice.
- Remediation advise should be illustrated with examples written in the same programming language as the finding's.

DC Comment: Ability to extend the reports and Join traces is also very __important

_
_

6. Reporting Capabilities:** ***[Operational Criteria]*

The analyzer's reporting capability is one of its most visible functionalities to stakeholders. An analyzer should provide different ways to represent the results based on the target audience. For example, developers will need as much details as possible in able to remediate the weakness properly in a timely fashion. However, upper management might need to focus on the analysis's high level summary, or the risk involved more so than the details of every weakness.

6.1 Support for Role-based Reports: ** **

The analyzer should be able to provide the following types of reports with the ability to mix and match:

- Executive Summary: provides high-level summary of the scan results.
- Technical Detail Reports: provides all the technical information required for developers to understand the issue and effectively remediate it. This should include:
- Summary of the issue that includes the weakness category.
- Location of the issue including file name and line of code number.
- Remediation advice which must be customized per issue and includes code samples in the language of choice.
- Flow Details which indicates the tainted data flow from the source to the sink.
- Compliance Reports:Scanners should provide a report format that allows organizations to quickly determine whether they are in violation of regulatory requirements or other standards. These reporting capabilities should be considered if certain regulations are important to the organization. The following list provides some potentially applicable standards:

- OWASP Top 10
- WASC Threat Classification
- CWE/SANS Top 25
- Sarbanes-Oxley (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- NIST 800-53
- Federal Information Security Management Act (FISMA)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Basel II

6.2 Report Customization:** **

The analyzer should be able to support report customization. At a minimum, the analyzer should be able to provide the following:

- Ability to include the auditor's findings notes in the report.
- Ability to mark findings as false positives, and remove them from the report.
- Ability to change the report's template to include the organization's logo, header, footer, report cover,etc.

6.3 Report Formats:** **

The vendor should be able to enumerate the report formats they support (PDF, XML, HTML, etc)

7. Enterprise Level Support: ** ***[Operational Criteria]*

When making a choice on a static analysis analyzer in the Enterprise, one should take into consideration the ability to integrate the analyzer into various enterprise systems, such as bug tracking, reporting, risk management and data mining.

7.1 Integration into Bug Tracking Systems:** **

Vendors should be able to enumerate the supported bug tracking applications, in addition to how are they being supported (direct API calls, CSV export, etc)

*DC Comment: More importantly: **HOW is that that integration done?***

***
***

For example, if there are 657 vulnerabilities found, are there going to be 657 new bug tracking issues? or 1 bug? or 45 bugs (based on some XYZ criteria)?

7.2 Integration into Enterprise Level Risk Management Systems:** **

Information security teams and organizations need to present an accurate view of the risk posture of their applications and systems at all times. Hence, the analyzer should provide integration into enterprise level risk management systems.

DC Comment: same as above, what is important here is to ask 'how is it done?'

_
_

And for the vendors that also sell those other products, they should provide details on how that integration actually happens (which ironically, in a lot of cases, they don't really have a good integration story/capabilities)

7.3 Ability to Aggregate Projects:** **

This pertains to the ability to add meta-data to a new scan. This data could be used to aggregate and classify projects, which could be used to drive intelligence to management. For example, this can help in identifying programming languages that seem to genere more findings thus better utilizing training budge for example.

DC Comment: And how to integrate with aggregator tools like ThreadFix

Another example, is to mark certain applications as "External Facing" which triggers the analyzer to perform a more stringent predefined scan template.

DC Comment: this last paragraph should not be here (Enterprise support) and would make more sense in the 'Customization section'

_
_

Projects in organizations are built using a certain set of technologies and/or frameworks. These can be commercial, open source or built in-house. Certain projects may tend to have more security flaws as compared to others based on a technology or framework used or based on the how the technology\framework is used within a given business context. Static analysis analyzers could be used to configure similar projects with additional metadata to detect these patterns. This will build intelligence around them that lends to being able to detect which application components have more security weaknesses and why.

_
_

DC Comment: this last paragraph is important, but also feels out of place here

7.4 Licensing Scheme:** **

Static Code Analysis analyzers varies in their licensing schemes. Usually, the following factors decide on the analyzer's total cost of ownership.

- Licensing Scheme Factors:
- Metered scan (pay-per-line) license: licensing fees depends on how many lines of code needs to be scanned.
- Pay-per-application license : a license would issued for a specific application and can't be used for any other applications.
- Time-based Subscriptions: one or more applications could be scanned unlimited number of times before the expiration of the license.
- Per-user licenses: a user-based license that is usually combined with one or more of the other schemes.
- Unlimited/perpetual Licenses: for scanning unlimited applications by unlimited users.
- Server costs: for client\server models.

- Licensing Scheme Enforcement:
  - License Server: dedicated server where licenses are stored and can be accessed by users on the network.
  - Local/node-locked: License is tied to a specific OS type, machine and named user.
  - User locked: license is tied to a specific username.
  - Floating: a number of licenses are shared among a larger number of users over time.
  - Trust or contract based: the licensing scheme mentioned in the contract is assumed to be honoured by the user with no extra enforcement.

–
–

DC Comment: __add question about 'Open schemas' (i.e. do they exist?), and the multiple evaluation options

Index A: Static Code Analysis Preparation Cheat Sheet:** **

Taking a decision about the correct static code analysis analyzer to acquire could be a daunting, however, preparation for such a task could be very helpful. Every analyzer is unique so as your corporate environment. The following is a set of information you need to gather which could make the decision much easier to take:

- A list of the programming languages used in the organization.
- A list of the frameworks and libraries used in the organization.
- Who will be tasked to perform the scan
- How the analyzer will be integrated into the Software Development Lifecycle
- How will the developers see the scan results
- Budget allocated to the analyzer purchase including the hardware to run the machine (if any)
- A decision on whether the code (or the binaries) is allowed to be scanned outside the organization.

**Index B: References **

- WASC Threat Classifications (http://projects.webappsec.org/w/page/13246978/Threat%20Classification[136])
- Web Applications Security Scanner Evaluation Criteria (http://projects.webappsec.org/w/page/13246986/Web%20Applica
- NIST Source Code Security Analysis Analyzer Functional Specifications Version 1.1 (http://samate.nist.gov/docs/source_ code_security_analysis_spec_SP500-268_v1.1.pdf[138])
- Static Program Analysis (http://en.wikipedia.org/wiki/Static_program_analysis[139])
- List of Analyzers For Static Code Analysis (http://en.wikipedia.org/wiki/List_of_analyzers_for_static_-code_analysis[140])

[136] http://projects.webappsec.org/w/page/13246978/Threat%20Classification
[137] http://projects.webappsec.org/w/page/13246986/Web%20Application%20Security%20Scanner%20Evaluation%20Criteria
[138] http://samate.nist.gov/docs/source_code_security_analysis_spec_SP500-268_v1.1.pdf
[139] http://en.wikipedia.org/wiki/Static_program_analysis
[140] http://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis