OWASP 2012 Board Interviews – Tom Brennan

Adam: What are your most notable accomplishments over the past 3 years as an OWASP contributor?

Tom: I've been an evangelist for the OWASP Foundation since about 2004. I started with the New Jersey chapter with 5 people and discussions about 2 or 3 architectures and sequel injection. After that our monthly meetings grew by word of mouth and combining with the New York City chapter in 2007 has grown to be one of the largest chapters in the world. Today we boast really large meetings, pioneer working groups, working with universities and also working with outreach groups with ISSA, infoguard, ISC², and Issaca. When I joined the board in 2007, I was actually appointed to head one primary objective. I was recruited in by Jeff Williams and Dennis Cruz and one of the objectives that was laid out initially was because of all the work we did at the local chapter trying to structure it and creating a democratic board etc. It was trying to drive the organisation, OWASP Foundation, to more of a democratic process. So one of the notable accomplishments that I have been involved with in my tenure with OWASP has been driving a democratic process. That kind of has changed over the board structure and has actually put in the elections that we're going through now. So again, in 2007, I was appointed to the board and I'm now the last person on the cycle to actually run for election by the membership. So it is a pretty long process to try to get a lot of people to buy into the conversation about a democratic global organisation.

In 2008, I helped organise the AppSec USA in New York City, which not only raised awareness, but also raised about $150,000 in profit not with any sort of split to the local chapter because it was simply the right thing to do. And this was one of the majority funding opportunities that led to the 2009 Summit. So again, working with the Summit moving forward to 2009. Another initiative that was pushed forward was actually formation of global committees. This was actually a very large endeavour to try to have focus groups from around the world give us their best 7 people from the region and promote those 7 people to the committees which would then focus on things that structure around the Asia Pac region or the US region or South America etc., and that's actually grown quite nicely. Over the last 2 years I think, in addition to lots of contributions and evangelism, I'm also one of the founders of the OWASP European entity. Myself, Sebastian and Owen felt it was required and very important for OWASP long term goals to create a legal entity in the EU in response to issues we had with the VAT tax and also trying to help shepherd some of the other regions around the world to do the same, and trying to grow that global component for OWASP. In addition to being obviously an OWASP contributor for lots of projects, one of the most notable, I think, has been being involved in the testing guide. I released an HTB post tool for denial of service testing back in November 2010, worked on the RFP criteria project and certainly a few evangelists and flagware for open sand. So that's probably a good summary but day to day, will there be a board meeting, will there be a local chapter meeting, a lot of these accomplishments are just as an active OWASP contributor.

Adam: What are the most significant challenges OWASP is facing?

Tom: Really good question. As a global organisation I think the number one thing is remaining vendor neutral. Regardless of what company anyone happens to work for this year, next year, or in 5 years, understanding that service on the board of directors of OWASP, whether it be a local chapter, whether it be working in a local committee, just simply wearing the OWASP badge, it's really about the individual. So it's critically important that members of the OWASP board and

committees, for the best interests of the community really not focus on any self interest, but really focus on the ability to help the organisation and community grow. So, for example, if you worked for let's say company A, and company B directly via a reseller agreement or any sort of joint work or opportunity puts money in your pocket, I think that's a huge conflict of interest, and I think that from the vendor community side today we have several members of the organisation, including myself, that work for service providers and it's extremely important to be selfless in the OWASP organisation and mission wherein if you have those sorts of conflicts of interest that you need to excuse yourself from certain conversations because that would certainly be a conflict of interest.

Another area of challenge I think is OWASP global growth. Global growth, something I've witnessed personally over the last couple of years, travelling to different events, travelling to different conferences and even local chapters, is cultural differences. We have a very interesting perception of what OWASP was, what OWASP is and what OWASP will be. Reminding people outside of the echo chamber of let's say the OWASP leader's list, kind of what the organisation is really about. This is really important. So being focused on being open to anyone to get involved and participate, that's critical. Being focused on software security, that's critical. Because honestly, what a web application was in 1999 is not the same thing as it is today, although there are some standards that are in place. But what will an "application" look like in 10 years? Or 15 years? And I hope that as we build the organisation long term and globally, that we take a look at a professional association of peers that are all focused around software and helping software security continue to be an important part is very critical.

Finally, growing OWASP as a non-profit is unlike any commercial business that I have either owned, operated, sold or am a part of. As a non-profit it's very important to look at the organisation with its volunteer contributors. Perhaps have subject matter expertise in various different areas. And some of those areas, quite frankly, may not be operational. They may be phenomenal in the technical space, they may be builders or breakers or defenders and have a very large competency in one or more of those areas, but sometimes operational of a large organisation is not its core competency. I think scale is important. I think we've shown that we've brought on some new OWASP project managers, we've promoted coordinators to be empowered recently, Sarah Baso. We've also gone ahead and brought on people like global membership coordinator Kelly Santalucia. As we continue to grow in operational staff, balance with volunteer efforts is really, really critical. And OWASP needs to look at that from a board perspective, making sure that we stay on stride. It's not about a quick win. It's really about long-term planning so we can make sure we can be self sufficient.

And lastly, the other challenge for OWASP is facing right now is decisions. A lot of the things that the board works on that I've been a part of since 2007 are really not that sexy, quite frankly. So they are not always tied to sometimes popular opinion. But I think it's a responsibility of the organisation and its elected board members that have the confidence of their constituents to be able to make sometimes hard decisions without any sort of prejudice for the organisation and to ensure that these are being made in the best interests of the committees, the different chapter leaders, the project folks involved and kind of having that information be put on the record. Hence why all the global board meetings are not only open to anyone who wants to join, but we also do our best to dictate minutes and record votes for history sake. So I hope everyone has a chance to take a look at some of the historical stuff for different folks that have been involved or voted, and certainly for any of the new candidates, it's very important that they potentially join some of these meetings and understand some of the complexities of the monthly meetings.

Adam: If you are re-elected, what would the top 3 things be that you would focus upon?

Tom: For me it's a little hard. I would continue operational focus as I have since 2007. What this means is to really stay focused on the financial oversight for the organisation, focus on operational workflow, to do more with less. We have some staff members and a lot of volunteers. There's a lot of process and workflow that can certainly be automated with technology. I've implemented some sales force stuff and others have implemented other workflow tools, but trying to do more with less is really critical. And again that's one of those not sexy jobs, it's behind the curtain that things just happen in the work. We've actually coordinated after a period of time to move our website, from a physical closet to a hosting company, and these things take time, take energy and certainly take people's volunteer efforts to get done. If I was to be re-elected I would continue to focus on industry and evangelism in this space. I think I have a proven track record of evangelism with industry and governments around the world – everywhere from China to Mexico to here in the states working with DHS etc. But being focused on industry is important because when the organisation was founded, it was very much a collection of information that appears around the world. This was back in 2001, so people like Bill Pennington and Jeremiah Grossman and Dennis Groves that were involved in the organisation in the early days, that organisation continued to grow.

In 2004, Jeff Williams picked up the gauntlet if you will, incorporated the organisation and drove it. There was an awful lot of energy and time put into it by Jeff and Dave and as we continue to grow, making sure that industry gets involved is very critical. I'm really happy to see organisations like Fed Ex, UPS, Best Buy, DHS and many universities and other non service providers get involved in this association. Because truly we all have the same problem. There's a thirst for knowledge. There's a lot of collaboration that happens in the app sec world, unlike the network world that a lot of us had grown up in. And coming from a developer background, certainly making sure that we collaborate with peers and exchange ideas is important, but again, that goes back to one of our challenges.

One of our challenges is remaining vendor neutral, understanding that there are some cultural differences and just because somebody's from one part of the world as an example, they're hungry for knowledge and creativity in the same way that your fellow developer is. We are a global organisation with over 200 and something chapters these days and growing quickly, and we are certainly being recognised around the world with all the efforts of the volunteers that have contributed time. In addition to that, I would say that we also need to look at focusing on some of our technical projects and staying in step with the community that I live in during the daytime is really kind of moving all our technical products potentially over to git up. I think it's a really good initiative. I think being able to have components there which is what we will be doing with mod security with my day job, but moving technical projects there, allowing them to be forward and re-committed to the tree is just a great initiative that has kind of proved itself with linex and certainly as more and more technical projects utilise git, I think it really helps foster some of the collaboration efforts that OWASP relies on.

Adam: What do you want to do as a board member that you can't do as an OWASP leader or a committee member?

Tom: Another great question. I think locally as an individual I always tell everyone that OWASP has no roadblocks, it's about the individual. So coming out of university you have some volunteer

cycles, you contribute to a project and that project gets legs and that project is with you for the rest of your life. So there's nothing that anyone can't do. OWASP was certainly one of the organisations when someone says, "hey why don't you guys do it this way", usually the answer is "great why don't you pick up the pitch fork and go do it". And then we love to see kind of how that works. So with that said, I agree with many who have said that the board as an example doesn't have any power, cause technically we don't. We are speakers or voices or puppets or people that are involved in the organisation to help represent the global community. However, being elected to the board, as a voice, especially globally, you represent a much larger community than yourself. You don't speak for yourself. You don't speak based on your opinion, you try to speak on behalf of what has been collectively discussed. And when you are representative of a large community, I think that is the single largest thing that you can do as a board member, is collaborate and actually make some initiatives that are global opposed to individual. So again, everyone, including myself, can spend time as individuals on projects or things that they find passion for, but at the board it's really important for you to understand that you have to change a bit. And you have to take into consideration global cultures, global aspirations of growth and whether it be doing a conference in some location that doesn't have a lot of local attraction to raise visibility. Whether it be to help fund and bootstrap some projects to get some revisions in place, it's really important to look at the organisation as a global picture.

Adam: And finally, how does your past experience relate to this position?

Tom: So I guess that's an easy one for me. Since 2004, as I said, I've been involved in lots of projects, lots of trackers, lots of evangelism. Prior to OWASP, I was on the board of directors for the FDA info guard programme. So standing that organisation up and understanding where the non profit was really supposed to be. It was important and that goes back to everything from legal structure, to taxes, to reporting, to a democratic board. That really continues to serve my local efforts. I'm very active in my own space. In my private life I guess in things like the American Legion, a veteran organisation of the US military here in the United States. And of course the United States Marine Corps. So working with other non profits outside of OWASP is important, because as an organisation that is a non profit, there are certain expectations, there are certain understandings, there are certain privileges quite frankly that the non profit is awarded and it's important to operate with that integrity and to ensure that the organisation stays on mission. And when it doesn't stay on mission or when there's some changes that can be made, again, it's really important to have a strong voice to say no, this is wrong, and here's why and get some collaboration from potentially the other board members or the committee members or whatever it may be to make sure we stay on track. My wife and 4 kids have been very supportive of my efforts with OWASP. I kind of attribute that to a couple of different things. The first thing is that software is in everything that we touch. At least for me, since '83 when I was doing Pasquel stuff. It's not going to change, so any sort of mark on the world that we can make that can allow a long term marketing is very important. And then also I believe software security is very important, not only due to this critical infrastructure, but quite frankly to humanity. So 20 years from now, I expect OWASP will still be a collective group. What is an application, what will it look like? Who knows. But having collections of folks that have worked on systems that are helping with humanity, whether it be medical systems or travel systems or financial critical infrastructure systems, everything that we touch, that we're passionate about and we get paid for, because this is what we do most of us for a living. At the end of the day, this collective group has had a lot of experience to give to the world. So with that, my past experiences have been embedded in this space. And I think that as some people have noted, when I'm done with my day job, what I do for fun is I work for OWASP.