OWASP 2012 Board Interviews – Eion Keary

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

Eion: I tell you the last 3 years can probably be establishing OWASP Ireland as an event I did in 2009 – 2010. I established, well we held OWASP EU in 2011 which was pretty successful. I suppose something else which I'm quite proud of is I've delivered free training and workshops on behalf of OWASP to about 150 people. I suppose something else, maybe less interesting, would be the establishment of the OWASP legal entity in the European Union and I had a part to play in that. I am one of the signatories for the European legal entity which benefits OWASP greatly in terms of financial position and that type of thing. And finally would be the reboot projects which I'm quite proud of which is ongoing, it's pretty recent. Pretty much the reboot project is around trying to reinvigorate a bunch of projects which are currently a list of a bunch of flagship projects with a testing guide, with a development guide. We have a bunch of projects which we are trying to energise. Just the fact that they are getting a bit old and I think it's pretty important for OWASP to maintain at least a relevance from the point of view of problems developers are facing.

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

Eion: That's a good question. One of the things I have from my experience being with OWASP since about 2004 is relevance with developers. You are in the position where you talk to developers and they haven't heard of OWASP. They don't know all the great stuff we can offer developers. Security is more and more a requirement. It's gotten much more mainstream since I started doing application security many years ago. I think OWASP does a lot of great stuff but still we are not being adopted so I think that's a challenge trying to get adopted; but we are becoming more mainstream in terms of developers. But there's a few things which we need to do to fix that. One of them, in my view, reaching back to the OWASP reboot project, is to develop and maintain our projects. So that would be my 2nd significant challenge. Our projects a couple of years back were sort of the tip – this was leading edge in terms of guidance because it was free, it was open, the projects were developed by loads and loads of people so you know the peer review and the quality was very good. But in latter years the projects have got old, they haven't been maintained and one of the problems with that is people giving time. You know, we're a voluntary organisation, so I think it's a real challenge to try and maintain those projects. For example the OWASP dev guide is many years old, the testing guide is at least 2 – 3 years old. I think things like that are very important from the point of view of giving developers and testers and functional testers, the people within the stlc of software. If they want to test for something I have to develop something in a secure way. We need to maintain that – those particular guides for example because technology keeps moving on and new volabilities are found. New ways to break things are found, but also we need to sort of demonstrate and deliver how we fix these new problems.

I think something else which is a challenge for OWASP will be the impact on the industry as a whole. So the idea first of all of selling OWASP to people that make decisions in industry and the industry being local – local privacy law or local types of compliance in terms of say data protection. But also in terms of industry regulations, for example pti and stuff like that. I think OWASP has made some inroads in terms of influencing various industry bodies and verticals. I think the citations page is testament to that, but I think something we need to do is continue to

do that. I think the development and maintenance of our projects will obviously help that out. So from the point of view for OWASP to grow and for people to refer to it as a household name in terms of software development, I think we obviously need to have some impact in industry as well.

Something else which I think is pretty important which may be a fundamental problem we face as OWASP, is the idea around figuring out what does OWASP actually do and offer for the software development community. So what I'm talking about there is to figure out how do we deliver the message about building secure software. How do we deliver the message around building secure software is actually quite easy if you know what to do. But I suppose one of the things I will probably talk about a little later as well is the idea of trying to make software security reasonably invisible. So how to become the developer's best friend. Security people can be viewed on as auditors and people that find problems for people but can't give a solution for how to fix problems. So I think one of the challenges of OWASP is to try and deliver solutions which enable developers and people involved in software and web applications to enable those guys to do their jobs in a more secure way, rather than just point out issues to them. I still think that is a pretty significant mountain to climb for OWASP. If we can do that in a much better way, I think OWASP will grow as well as a result of that.

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

Eion: I think the first thing would be to develop our products, or redevelop them. I think spending money – if you look at our budget, we have a lot of money which sits there. I think encouraging chapters to spend money. Our mission is to help and to try and cure the cause of software insecurity. A lot of people have a lot of ideas and I think if we can fund those ideas, if we can empower those people with the ideas, I think those ideas may come to fruition. So, I think one of the first things I would do would be to encourage people to request funding from the foundation, and also encourage projects from our chapters which each have their own projects, encourage them to spend money as well on their own chapter initiatives. I don't see that happening enough. I think people may be afraid to put their money where their mouth is. But I think we can only try and that's an important thing.

The next point in terms of the top 3 things as a board member proposing to be re-elected will be to continue to try and influence tech companies and collectives such as the Java people and Oracle (formerly Sun), browser vendors, php frameworks, springs, struts, any of those collectives, the rails working group, any of those collectives which actually build these frameworks to try and influence them to talk to them around how to do things in a more secure manner. Because in a lot of languages, a lot of frameworks, there's still some ways you can inherently build things in an insecure way. I think if we could influence some of those people that drive the actual technology itself, sort of say if you do it in a particular way the margin for error reduces dramatically because developers can do it in an insecure way, I think that would be great. So, in effect, to face up with people like that and to try and help them understand why we think things should be done a certain way and try to get people to build that into their framework so that people will be utilising and implementing frameworks and systems which are inherently more secure. I think again, harking back to the previous question, I think the third thing would be to focus on making applications security easier for developers. I think having secure frameworks is one way of doing that. I think also having projects and guidance which is very high quality and covers a wide range of issues is another way of doing that. I think training is another way of doing that. I think understanding what the problems are rather than telling

people what the bug is maybe the developers will understand what those security issues are in the first place and hence code in a way which will prevent that. So I think my top 3 would be to make application security easier for developers but there is a very wide range of activities in order to do that. Again, my view around this is that if we don't do that, the foundation won't grow in the way it could grow. The foundation could be more relevant to developers if we can achieve that in the right way. By delivering great stuff, by delivering free training, by delivering workshops, by empowering the developers. I think those would be my top 3.

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

Eion: That's actually an interesting question, because in OWASP, even if you're not a board member, you can do a lot of stuff. I'm not very big on hierarchy. I think looking at the foundation since maybe 5 or 6 years ago, it's got a little bit more bureaucratic because we're getting bigger. But as a board member, I think what I would like to do is influence the strategy to tick off the previous answers I gave you. I think as a board member I'd probably be in a better position to do that, but you could probably do it in a more effective way than not being a board member. Unfortunately, hierarchies are such that people such as board members have more influence. But also I think that the perception of a board member versus a project lead or as a contributor to people outside of the organisation. I think that people outside of the organisation, when they hear the word board member they may think this person is some sort of power and influence. But in effect, the board doesn't really have that. The board is in effect a steward foundation but most of the things we do require feedback from the committees. So I think that one of the things I would like to do is try and define our strategy. We defined our first real strategy this year for 2012, we defined it at the beginning of the year and then we allocated funding to that to try and achieve that strategy. The strategy was pretty much defined as a year-long strategy but the idea would be to try and feed that strategy to a more long term strategy. As a board member you have the ability to do that and to talk to your peers on the board and try and figure out what is the foundation.

I suppose the 2nd thing I'd like to do as a board member again is to build a sustainable model from a financial standpoint. What I believe in is okay we're an open source organisation. We give things for free, we do training for free, we have free tools, we have free guides, projects, the cheat sheet series, whatever it may be. After that we have various sorts of support, things like the security 101, email lists for people who have questions or are new to application security. But the thing is in order to run this stuff, in the last couple of years we've hired some full time people which have been vitally important. So we have now 2 directors and a number of other full time people, but we are still looking to fill some gaps in that space. But in order to keep the lights on for the foundation, we need to have money to do that. So we need financial stability to operate as an entity, but we also need to be able to support people. For example, a few people building a project and it may benefit these people to in effect meet in person in a particular country. I think the foundation should have the ability to finance people to meet because they're doing something important and something great. Because they're volunteers and they're passionate. I think that as a board member, one of the goals we need to achieve is to be able to be sort of robust from a financial standpoint. I think as a board member you're probably in the best position to do that. A lot of the board decisions come down to things like profit splits between chapters and the foundation. You come down to the likes of engagement with third parties etc to try and push the OWASP message etc and all these things again require funding or have some financial impact and that adds up. That's one of the reasons why we set up the

European entity as well because it's a legal entity from a tax standpoint. It's much more effective, which means that we have more money and we can spend it on field stuff. I think those things will be the 2 things – influencing the strategy and also the attempt to try and build a sustainable financial model for the foundation. I think those are the things that could be viewed more effectively as a board member.

Adam: For our final question, how does your past experience relate to this position?

Eion: Well, my past experience, as many people know well, I'm currently a board member. And then I suppose from being a current board member I was involved in the first strategy for the foundation, and also I was involved in the first real budget we had for the foundation. So I think those experiences stand to us and to me in terms of trying to improve that for the coming years. I suppose from the point of view of OWASP, I know the organisation, I've seen it grow since 2004. It's gone from a loose collective of individuals when they joined to a powerhouse in some ways, having great conferences, having some great industry citations, having some influence and also anybody who attempts to use OWASP, attempts to see the value in it, I think we do need to improve that as I mentioned before. I suppose also in terms of my past experience, I used to lead global teams on global engagements for my previous employer, so I pretty much have experience in terms of how to manage virtual teams and global teams working across the globe, understanding different cultures, understanding people's ways of doing things and lots of people's different ways of communicating. I think that would stand to me.

I suppose the last thing is, as I've said, I've been with OWASP for a long time and it's like a treadmill. Being with OWASP in some ways is like you want to keep going because you know you can improve your time, like if you're running on a treadmill, but it's hard work and I still believe I have a lot of passion to give and ideas to contribute to OWASP. I think my passion and my history of OWASP as well would stand to me from the perspective of contributing going into the future if that was to be the case. That's pretty much it dude.