OWASP 2012 Board Interviews – Justin Derry

You are listening to the open web application security project with your host Adam Bosso. Thanks for listening to the OWASP Foundation Board candidate interviews. Over the last couple of weeks I spoke with OWASP Foundation Board candidates Justin Derry, Matt Tesauro, Tom Brennan, Jim Manico and Eion Keary. Each candidate was asked the same 5 questions which were provided in advance. The interviews are provided in this podcast unedited.

The OWASP Foundation was established in 2001 as an open community and software security resource. Since then OWASP has grown to be globally recognised as a credible source for application security standards. Individuals typically find OWASP when searching the internet for information about software security and they're happy to find a reliable source of knowledge built by an extremely open and passionate community. OWASP is open to anyone. Anyone can attend at OWASP's vendor agnostic local chapter meetings, participate in regional and global conferences and contribute to the many OWASP projects. And anyone can start a new project, form a new chapter, or lend their expertise to help an OWASP global committee. The OWASP Foundation Board of Directors consists of 6 elected volunteers. These unpaid volunteers dedicate themselves to the organisational mission supporting the OWASP global communities and playing a pivotal role in the software security community. OWASP conducts democratic elections of its board members and committee chairs to enable bottom up advancement of its mission. Each year half of the board seats and all of the committee chair seats are up for election by the then current registered members. To learn more about the candidates and the 2012 OWASP Foundation Board election being open for e-voting October 12, visit www.OWASP.org and look for the 2012 election information link.

Here is my interview with Justin Derry:

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

Justin: I suppose with OWASP I've been actively involved with the community for quite a period of time. I suppose in the last 3 years from about 09/10 through to this year I'm probably more well known in the eyes of Pacific Rim for the role of the conferences chair for the OWASP Asia Pacific conferences that run here in Sydney. I normally try to run that as many years as I possibly can. I think that's a great way to get out there and certainly evangelise the need for application security in general. Definitely the conferences' chair would be one of my key initiatives that I'm actively doing inside OWASP.

The other side is I try to work alongside as many projects as I can. I obviously actively work in the industry as well so the time that I do have on my hands is sort of limited. But outside of the conferences, working on some projects, I have in many years previously submitted and actively been involved in projects – run projects myself. I suppose the most recent one is working alongside ??(sounds like provea) that I know very well. The most recent period is on the open sand project that's actually something that I'm very passionate about. I think I look back at the last 10 – 12 years and look at how application security in general and web application security has gone on by not really solving the problem so much by doing all ?? (sounds like spanatranic) testing. It's really about making sure that we actually set some compliance and more guidelines around how organisations can actually think.   And I think that was an absolutely critical need for open sand to be developed and I was fortunate enough to actively be quite involved with that project back when I was working with ??? (sounds like waterfine) and obviously directly with provea. I've been actively involved in a number of other projects and conferences and spoken

around. But I suppose if I were to pick a couple of core ones that would be the core projects that I've actually been involved with.

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

Justin: That's an interesting one. I suppose I've sat back a little bit, been actively involved in OWASP for quite a period of time and I think OWASP has a number of challenges that they are faced with. One of the biggest things that I suppose is the reason why I put myself forward is application security. It is not unique to a specific country and the problem that we have and OWASP's mission is to really be a global organisation that is focused on trying to address the risk associated with application and security and being a source of trusted advice to the community and to organisations on application security initiatives. So I really think that the biggest challenge that OWASP is faced with at the moment is really being a true global organisation. We'll talk a little bit further down in some of the other questions that we have around my feelings around that, but I really think that one of our key goals here is that OWASP needs to become a global organisation. We really need to tackle a lot of problems that we have with language barriers, especially in the Asia Pacific Rim and really try to reach out into the community.

It's great to be able to have conferences and get our community, which is the OWASP community, together to foster great knowledge, great advice, experience, and get it documented. But I also think we've got to be able to take that message and be able to go and take it out and really I think that's your key challenges with OWASP – making sure we're really a global organisation. But on top of that we're actually reaching out into the community outside of what we are currently touching which is application security and really trying to establish further outside of that into developing communities, into organisations and so on. And I think that's a challenge in itself because that's a big ask and we've got a lot of work on our hands with that. But it's definitely possible to do and definitely we've got the trusted advice. I think in OWASP we just need to also focus on being able to evangelise that out within the industry.

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

Justin: I think we've sort of covered 2 of them already Adam. The first one is definitely global outreach. One of the things I've been actively involved in – I was since 2002. So I've been around about 10 years, most of the time behind the scenes, sometime, mostly in the Asia Pacific Rim. There is a massive amount of software that is developed down in India, for example, China, Japan, Australia, New Zealand, Thailand, Singapore, the list goes on. The biggest challenge is that a lot of our community at the moment and a lot of our knowledge and experience that we gain is coming out of Europe and coming out of the US. Now, that's not unusual and that's very, very common. However, to be a true global organisation, we really need to start considering global outreach across the board and if we take the current board, I think we've got a great group of people on the board, but I don't think that we're globally represented because we don't have people in the Asia Pacific Rim or at least people that understand the problems associated with the Asia Pacific Rim that are down here. So I think that global outreach is definitely one of them. I think application security in regards to evangelism, we touched on before as well and I really do think we ought to start thinking outside the box a little bit more. And we are doing that. We're doing I think a lot of great outreach into universities. We're doing a lot of great outreach and I know there's a number of chapters around the world that are reaching out to develop the groups. I know here in Australia it's something that we're actively doing as well is fostering

spreading the word outside the norm. But I really think that that needs to be taken to a whole new level and one of the things that I definitely would want to focus on is global outreach, but also evangelism and talking about OWASP and taking the message of OWASP to people outside of the traditional OWASP community. And there's so much great material and so many great opportunities where we should be going to development conferences and taking the opportunity to actually talk about the problems that are actually out there. And I suppose the third one is a little bit more tricky to deal with and that's around OWASP transparency. I think any community in an organisation has its ups and downs and I think it's important to ensure that as a leader in general, i.e. a chapter leader, or a OWASP leader to a board member really needs to foster the ability to be transparent and respectful of each other but at the same time being transparent as an organisation in general. And that goes to play not so much about whether or not we feel that we're transparent right now, it's got a lot to do with the fact that OWASP was really seen as a trusted source out there and to remind the trusted source not only do we need to be investing time in our intellectual property and really creating great content for everyone and evangelising it out there, but ensuring that we've also got the mechanisms in place to remain as the trusted source so that we don't have problems with people questioning our content or having a look at that. So I think that is a lot of investment in working together as a team. But also putting initiatives in place that ensure that people can look and go wow, that's a very switched on organisation and it's very open, extremely transparent, evangelises and really puts the message out there and is absolutely the respected, and remains the respected, source in application security. And I suppose the reason why that one's there a little bit is in Asia Pacific, I don't think across the board, but in certain areas OWASP is struggling and there isn't enough focus on it and it partly has to do with our outreach as well as our evangelism as well as making sure that we're transparent in those cultures and that we reach out to the relevant people in the area. I think that would probably be the 3 key things.

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

Justin: I've pretty well worked out that, as we talked about, I've been actively involved in OWASP as a project leader to contributors to conference chairs to I actually sat on a committee for awhile. The challenge that exists, and the challenge that is here in Asia Pacific, is that if OWASP wants to be a true global organisation we really need to have some representation in the Asia Pacific. Board members, the reason why I would want to assist OWASP by getting more actively involved and sitting on the Board, is to really focus on fixing some of those problems that we have here in Asia Pacific. I'm not saying that we need to re-divert all of our resources over to APAC. What I'm saying is that APAC is just another area like the US and Europe. We have a lot of things like culture/language and we've tried pretty hard to try and introduce language specific criteria into projects and being able to set key initiatives that would really help foster and raise awareness within the Asia Pacific Rim. It's a bit of a struggle when the Board is there and the organisation is a little bit US/UK centric. And you know what, there's nothing wrong with that, but if we want to be a true global organisation then we really do need to pay some attention to APAC. I think that needs to be done at the top – down. And if I – I obviously work in the industry – I own my own information security company with a bunch of business partners and you know what, when we want to enact change like this we know it doesn't work at the bottom level and I've spent a lot of time investing in the community to help raise awareness about OWASP, talk about OWASP and spread and evangelise the word. However, OWASP really does need to reinvent itself from the top down as being more of a global organisation to achieve that we really need to do that from a top – down approach. I honestly believe we need to have our board and the global committee

has already got an international representation so that's really good, but I think obviously having a look at the board helps to set direction. But at the same time helps to glide funding strategies, set initiatives, help to put focus into places and Asia Pacific is sort of left off the umbrella a little bit at the moment. We've got a struggling chapter up in Japan at the moment that's got a lot of people who want to help out but not a lot of mandate to push it in the right direction and it's an area that we should be doing and could be doing a lot of great stuff. So I think that's really important. I think the OWASP board needs to be there, not only to do its core mandates but to also help guide the organisation in its mission from a global standpoint.

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

Justin: This was an interesting one that I suppose you can interpret the question multiple ways Adam. I suppose my past experience, it's up on line if anybody wants to have a quick read of it. You know what, I'm an ex-developer from 20 years ago. I have spent all my life or a very large chunk of it in IT. As I mentioned before, I've been actively involved in OWASP for a long time. And actively involved in the information, in the security industry, for a long time as well. I suppose if you have a look at my background, I've grown very much from a technical background I still have a lot of very technical experience, but I moved more into upper level roles where I tend to have conversations that facilitate industry events as well as communicating with more on a governance and more on a compliance and organisational approach and to me that's a transition. But I think it's actually very important for OWASP as well is that I've got a lot of very solid technical background and I've been in the industry for a very, very long time, but I've definitely moved more into more a leadership role where it's become really good for me to be able to evangelise, especially even OWASP to 3 large banks and being able to help steer them down directions of tackling this problem associated with software security. So, I think I've definitely got a substantial amount of experience and from a business acumen standpoint, for the past 4 or 5 years now had my own company, currently the CEO and actively involved in not only evangelising OWASP, but also helping to solve the problem associated with software security from an upper management standpoint as well as from a technical standpoint. Definitely from both avenues which is good.

Adam: That concludes my interview with Justin Derry. Again to learn more about the candidates and the 2012 OWASP Foundation Board elections being open for you voting October 12 2012 visit www.OWASP.org and look for the 2012 election information link. I'm your host Adam Bosso in Minneapolis. Keep making application security visible.