OWASP 2012 Board Interviews – Matt Tesauro

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

Matt: That's a very interesting question. As a project leader, OWASP live CD has sort of morphed now into what I'm calling OWASP WTE or the web testing environment. That's been going since 2008 and I've kept it updated. It needs a little care and feeding right now but generally speaking that's been a good thing for me. In more the board level kind of things, one of the bigger things that came to mind when I read this question was the rack space hosting agreement and donation I negotiated with rack space about 2 years ago, maybe it's pushing 3, where they donated 5 cloud servers to OWASP to host our IT infrastructure on and move it up into a little more enterprise class environment and out of the server rack in one of our board member's offices. Which wasn't bad, it was actually wonderful that they donated that for years, but if we could get a free upgrade why not do it.

One of the other things that I felt was particularly cool, was my meeting Ivan Butler and helping to get the partnership set up with hacking lab, which is a website plus a network environment where people can go in and do hacking challenges, pen testing type challenges and we partnered with them to put all of the OWASP top 10 examples up there and Martin has been running that programme and has really done wonderful things with it. I'm pretty happy when I got the treasurer hat last – I guess it was at the last OWASP US, that we did a lot better budgeting and trying to more formalise our spending and making sure that we're making the best of the donations that come in to OWASP since we are the stewards of the money that is donated. I wanted to make sure we're making the best of it and I think we're doing a good job of that. We've been able to add employees to the payroll which has been fantastic. And right now that it's sort of in process we're close but not quite done with them is we're about to migrate all of our rack space hosts into a managed programme where rack space will actually keep them up and running and there's an SLA and all those good things, monitored and what not. Because we're mostly a volunteer organisation so finding ways that we can sort of solve problems and make them somebody else's problems, like rack space in this case, keeping our servers up and patched is a good thing because tons of us donate tons of time to OWASP but it comes in bursts and it's not consistent and it's not 24/7/365. So trying to get some of those systems set up for OWASP that are a little more formal.

And then the final thing that I've been working on just of late, is trying to get retirement plans, like an employee contribution retirement plan set up for the couple of employees that we have. Because OWASP wouldn't really be working without the several employees that we have and I'd like to as a board member be able to show the appreciation that I have for all the work employees do that keeps the lights on and running by allowing them to save for their future so they can retire at some point in time, hopefully in no time soon because we're desperately needing them, but those are the big things that kind of came to mind when I read this question.

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

Matt: I'd say a number 1 is growth which is actually kind of a great problem, but it still is presenting some challenges. When I started with OWASP several years ago it was a much smaller organisation and we've continued to grow year over year in great stride if nothing else even just looking at the sizes of the conferences and how well they're attended, it's been amazing in the exponential growth. So that's caused a lot of problems. The systems that worked fine when we were a much smaller organisation aren't really working that great now. And we've had a little bit of contention and struggle trying to find the right level of sort of, I hate to use the words, but process and procedure rights so that people know how to get things done, but it's done in such a way that it's light weight and it doesn't dis-empower people from contributing to the community and feel like Jesus this is just a whole lot of bureaucratic mess, I don't want to deal with this it's not worth it. We have to make sure we find that right level where OWASP can make sure it's healthy and vibrant but without dissuading people and make it like going to the DMV and getting your driver's licence where you wait in line for 3 hours and you fill out 10 forms and 6 weeks later you get a driver's licence. We want to avoid that at all costs and I guess the biggest thing is like in this transition from a smaller board to a larger one, right.

The other key thing I'd like to do is have OWASP start looking at how to be sort of self sustaining. Historically OWASP has relied on, and this has been fantastic, contributions from board members and others to help with various and sundry pieces like the original OWASP credit card was in the name of one of the board members. Well that was awesome they were willing to sort of put their financial self on the line for OWASP, but it sure made our lives a lot easier and it's time that we're big enough and they are actually working on getting credit cards issued to the foundation. That sort of thing that they're not tied to an individual they are tied to the foundation itself, so that ideally it'll keep growing without having to be reliant on any single point of failure or any single individual.

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

Matt: This is a tricky one because I know what I want to do. I think one of the big things to do particularly as a board member is to sort of help yourself and help others to reach out to other groups and kind of let them see what OWASP has to offer. We've been a little bit insular and kind of only with our own comfort area, OWASP has been of late. But I'd like to see us reach out to developers, ideally people writing frameworks, where if we could get them to sort of "do the right thing" about security saying defaults, those kind of things, secure configurations initially, that would be a huge win for security globally, I mean it's just for everybody. And that's something that I don't know that we've done a very good job of, of late and I'd like us to see more. And things like the partnership that I started with hacking lab and the ties to the universities is really a fantastic thing. Because the universities are where the next batch of developers and security professionals are gonna come out of and if we can kind of catch them early and make them security aware before they get out into the marketplace and start actually writing code for a day job, we'll be way ahead of the ball. So the recount to these groups is probably the A number 1 big thing for me.

Secondly I would say probably getting the OWASP – and this is unfortunately somewhat boring but it's really important work – getting the OWASP financials in shape. And I don't mean to say that we're financially in trouble, but we don't have really good systems in place to keep track of how our budgets are going month after month. How to best allow – like we have a lot of pain points around international conferences, how could we better help the OWASP volunteers in other countries how to conference and have the foundation provide the support they need to make that successful without a lot of pain and a lot of trauma on both sides. Some of the non US countries get pretty interesting trying to do financial transactions in the US. The US regrettably has some ugly financial laws right now that don't help. So trying to work through those issues and then just even simple things like getting a standard process of doing budgets year on year which we started last year and we're reviewing them right now for next year. And that's been a really good thing to make sure that we're making the most of the contributions that have come into OWASP. I don't remember but I think I said this, I don't know who I said this to, but one of the email threads on one of our lists, I remember commenting and I got a couple of props back for this, but I remember saying that I want to make sure that OWASP is around and available for my kids. If they turn out to be geeky pen testy developer types like me, I would want them to have an OWASP, have OWASP, not an OWASP, have OWASP around for them to be contributors to and if we're not sort of unfortunately having to watch our p's and q's in keeping the lights on, that's not gonna happen. So I want to make sure we have sort of reliable and resilient systems in place for our financials.

And then the other thing that has been a pain point of late, and this is another just an outgrowth of our growing as an organisation, is our IT infrastructure has been sort of ad hoc developed by volunteers which has been fantastic and god bless them that they've done this for us, cause we wouldn't have the growth problem if they hadn't volunteered their time. But we're at a point now where we need to get a little more formal with this, get it more documented and get away from any single points of failure. So for example, I'm the treasurer for the board and when I go and approve payroll, I don't log in as Matt Tesauro, I log in as the OWASP treasurer. And any time we set up a new system, we want to make sure that there's multiple people who can log in with the same level of privilege so that if one person is unavailable there's a backup and we're not sort of creating single points of failure that have been problems in the past. And those are my big 3. I could go on but that's probably enough.

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

Matt: That's interesting. I used to be on the global projects committee and I wouldn't have thought, I mean I'm the same dude who was on that global projects committee, and I wouldn't have thought of being able to say, yeah, I'm on the board and it made that much of a difference, but I've been sort of surprised when I went to talk to rack space there's an internal guy who was an OWASP community member who worked there and he introduced me to a couple of people inside of rack space and when we did that discussion around the donation, I was surprised at how blown away they were like oh look an OWASP board member is here. And I thought I'm just some guy who likes apps sec man, this is nothing exciting, but in those places it's been really nice to sort of be able to wear the board member hat and be able to solve those more larger global issues. Same thing with hacking lab. It was a bit of happenstance that I bumped into Ivan Butler at the Appsec DC conference, but I was able to take that interaction and turn it into a wonderful partnership that's benefited both us and hacking lab.

And the other thing that I like as a board member is the ability to sort of find the pain points in the community and be able to solve them. I've had lots of interactions with people in the community where there's some silly something that's hindering them from being a productive community member and being on the board sort of allows me to work to remove those roadblocks so we can have the community vibrant and functioning and contributing which is what drives OWASP. The other fun thing that is a bit selfish of me, but interacting with the chapters and the committee members and the people I bump into at conference and being able to sort of give them the hey, this is what OWASP big picture is thinking about. The times that I get to go to my non-local chapters or meet people at conferences or what not, it's nice to be able to sort of spread the message and tell people, hey, this is what we're thinking at a high level. Cause a lot of time when you're in a global committee, you're really worried about your committee's charge and what your committee's mandate is and the problems you're solving there, and it's been really fun to be able to focus at the next level up and how can we provide a platform where OWASP can allow everybody to contribute and be able to get something back.

And then basically I'm, as boring as it sounds to say, I'm willing to do the boring, non-sexy, behind the scenes work because I'm convinced that if I do that work, we'll have an even more vibrant community and if I have to do the un-sexy boring stuff and it allows OWASP to thrive, that's a small price to pay to help the world increase its appsec. This is just something I believe in so it's fairly easy to sign up for the un-sexy jobs.

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

Matt: Like most people I have a fairly diverse and interesting past. I'd say probably one of the top things that comes to my mind is I've been a long time user, contributor, advocate of open source, free libra, open source software, whatever you want to call it. And as a user and contributor, to various and sundry open source projects, I've got, I think, a pretty good feel for how interaction works, particularly at a distance cause we're all – we have local chapters and that's a great aspect of OWASP, but there's also geographical dispersion of all of us and we have to sort of figure out how to make things work when we're not face to face and we can't walk over to the other guys desk and just chat him up for a bit. I think that my experience in various open source communities has really helped me get a feel for how to interact with and most effectively work with people that aren't face to face, that are usually over a mail list or otherwise geographically dispersed. Then just my work life, I've worked at a bunch of different environments, the commercial business world, I've been in government, I've been in academia. I've been a developer assistant, been a pen tester, I've been an external consultant basically a hired gun, and I've also been an internal security guy sort of championing security from the inside. And I think the variety of roles I've had in my work history have helped me to sort of see more sides than if I had been sort of siloed into one particular field.

And then although this may lose me some geek cred, my first degree was in economics so I have a bachelors in economics from Texas A&M University and although I wouldn't have thought this, it's actually a fantastic thinking structure to have around solving problems and looking at the incentive structures, that proposed solutions provide to the participants. The idea of opportunity cost which is probably not greatly understood outside of the geeky economist types, but not only looking at just the financial cost, but one of the external, not the external necessarily, but what are you foregoing by choosing to do one thing. So if we spend x dollars on video cameras for all of the conferences, what can we not spend with that money. And then that sort of perspective has been useful for me as a board member. My period of time in academia, I was a lecturer and I taught several classes and I still love doing teaching and training and I think OWASP is just another great venue for me to go out and sort of spread the message of the importance of security and doing things "right". I've also managed a bunch of people. I've had at various and sundry times, people working for me, up to 30 direct reports in one job and I enjoy the management challenge of trying to find a way to get the most out of people and make them shine. I've always enjoyed that challenge of what is it that I can do to help this person find within themself the ability to really do some awesome work, and I've been lucky to have some great people working for me and there's nothing more rewarding as a manager, than to have one of your employees stand out and look awesome. Because that's just a wonderful thing and I love that about OWASP, the ability to sort of let people who want to be contributors provide a way to shine. That's a wonderful thing.

And then one final thought. I had a manager who told me this after I was no longer working for him. And this was a quote that really stuck in my mind. He had said "I never realised how much Matt did until he left" and I'm very happy being one of the behind the scenes get it done people who will do the ugly and unfortunate stuff so the rest of us can have fun, and the board lets me do that. I get to help numerous people in different ways that is just rewarding for me to see them succeed and that's probably one of the best things and most unexpected things about being on the board. Being able to say you're on the board, that's whatever. From a professional career point of view I guess that's nice but that's not really why I do it and why I divert a chunk of my personal time away from other things. It's because I believe in the OWASP mission and I really – the times that I've been able to interact with community members and watch them start from a small project to something that's really flourishing. Like Simon in Zapp, it's been fantastic. He kind of came out of nowhere and has just been doing wonderful work. And those are the type of things that knowing that I had some small part in helping him shine is a fantastic thing.