

OWASP & Web Application Security – an Interview with Jim Manico – host of the OWASP Podcast

Listen to the Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Brian Contos: Joining me today is Jim Manico. Jim is a web application architect and security engineer. Jim has 11 years experience developing Java-based data-driven web applications for organizations such as Fox Media, MySpace, GE, Citibank and Sun Microsystems. Jim also volunteers for the Open Web Application Security Project (OWASP), by producing and hosting the OWASP podcast series as well as participating in Enterprise Security API or ESAPI Project.

Welcome to the show Jim.

Jim Manico: Hey, great to be here Brian.

Brian Contos: Jim, before we get going, I was wondering if you could give our audience a little bit of background about how you got into this field.

Jim Manico: Well, I feel very lucky. I've lived on the island of Kauai in the Hawaiian Islands for many years now and I was working as an educator and technologist at a series of local schools around the island. I was looking to get back deeper into the IT field and write code and get into security again. What happened was that there was an employer on Kauai, the SANS Institute and Steven Northcut was hiring. So I took a job with Steve on island where I was writing PHP, doing some Java work, getting deeper into the field of Internet security.

So it's SANS and Steven Northcut that I have to thank for dragging me into the world of security.

Brian Contos: It's funny, every time I talk to somebody in the security space and they happen to live in Hawaii, nine chances out of ten they're with SANS. [laughs] It seems like they've got the market cornered.

Jim Manico: I respect SANS for how they got me involved in the industry and for getting my interest aimed towards security but I'm an OWASP man all the way now. I'm an OWASP man and an Aspect Security man. So I respect SANS but I definitely have my eye set to other organizations that are more focused on web application security these days.

Brian Contos: For those of our listeners who, I don't know how they couldn't but possibility aren't familiar with OWASP and what OWASP does: Could you give us some background on that?

Jim Manico: Certainly. In fact, let me just get you the template answer off of our site. The open web application security project, otherwise known as OWASP, is a worldwide free and open community focused on improving the security of open web application software. Our mission is to make application security visible so that people and organizations can make informed decisions about application security risks. We are a non-profit; we are a 501-C3 non-profit charitable organization that insures the ongoing availability and support of our work. In my opinion, I think OWASP resembles the Medici effect. When you step into the intersection of all these fields, disciplines and cultures, we can combine existing concepts into a large number of extraordinary new ideas.

That's what OWASP is. We have programmers, security experts, policy-makers, folks in government. The variety of individuals who join and contribute to OWASPs all for the purpose of increasing the knowledge and power behind web applications and security tools and techniques. I don't think there's anything like OWASP in the world right now.

Brian Contos: So Jim, how big is OWASP these days?

Jim Manico: Well, if you take a look at our web site O-W-A-S-P.O-R-G. You'll see that the OWASP foundation has 130 local chapters. The thing is, it's worldwide. We have a new chapter that started up in a rural city in Africa. So we really are planet-level, a global organization trying to increase the awareness of web application security worldwide. We have, I believe, some 40,000 odd members and again, at least 130 local chapters. I'm the Hawaii state chapter lead. I'm also the lead and the founder of the OWASP podcast series for OWASP. That's the thing, it's a volunteer organization. All the members who lead a chapter or build tools or participate in leadership - all those except for a few administrators volunteer for OWASP.

Brian Contos: I've got to tell you, I think OWASP is really a great resource for information just based on the presentations that I've seen. Our CTO Amichai Shulman who is actually presenting at OWASP in a couple of months in Europe in Poland. I was just looking at a quick review of some of the presenters and some of the topics. It really is pretty amazing. I was talking to Joe White, who presented at OWASP I think back in September. He was showing me the great content that has been created. It really is a fantastic source I think, for anybody who is interested in web application security.

Jim Manico: I think when you go to an OWASP conference you're going to find that you're going to hear some of the greatest experts in the world talk about web application security, especially at the level of passion and excitement that you're not going to see at many other places. Because folks who are giving talks at OWASP and folks who are contributing and participating in OWASP. It's all volunteers; it's all coming from people who have passion for this topic and are willing to donate their time to try to help the community and improving where we are today.

Brian Contos: I'll take this moment to give you quick plug. It really does speak to the openness of the community. I would suggest, again, anybody who is interested in security, please tune into the OWASP podcast and you can find that on iTunes just like the Imperva podcast.

Jim Manico: I'd also like to say cheers to you on your podcast series. I think you're doing a great job. From one application security podcaster to another, high five Brian. Keep up the great work.

Brian Contos: Well thanks a lot Jim, I really appreciate that. So Jim, you've been around application security for a while now. Quick chronology, quick history: how has it changed, in your opinion, since you started?

Jim Manico: I come from a unique aspect of web application security. I'm a software engineer, a software architect. I was up until four a.m. writing code last night, and as soon as we're done and we get some more coffee, we're going to write a lot more code. So from a defensive coding perspective, I think that if you go back four or five years... I recommended to SANS to get into the software security space back several years ago when I was working for them. Their answer was, no way, it's an immature industry, it's a waste of our time and effort. Look at them today, and SANS is very much putting software security out front in a lot of their new initiatives just in the last six years. The real turning point happened around 2005. There are very few web application programmers I know now who don't at least have some kind of basic understanding of cross-site scripting, cross-site request forgery, and SQL injection at the very least. If we went back five or six years ago, very few developers knew what these terms even meant. So I see awareness from the programming community starting to change dramatically, and I think that's the only way we're going to crack this nut. Until we can encourage millions of developers worldwide to write code in a more secure fashion, with architectural security awareness etc., we're never going to crack that nut. I feel that that change is really starting to happen within the last couple of years.

Brian Contos: I've got to reinforce that with what I'm seeing as well. I travel around, meeting customers, prospects, and partners around the globe. I've got to tell you that for the last few years, you can't really talk about security as a general subject without getting into application security and database security. It's just a piece of the equation. I think a new breed of security analysts are starting to evolve. They are becoming much more application and database-savvy. Perhaps they don't have the hardcore software engineering architecture credentials of somebody like yourself, but they need to be able to understand what the threats are, and what some of the mitigation capabilities are. It's just the world we live in today. Classical network security, perhaps what you might have thought of from SANS several years back, it's not enough to address today's threats. Jim, in your opinion, what do you think the greatest risks to IT are? Is it network, web, database, people themselves, or something else? Where do you see the greatest risks?

Jim Manico: I think without any doubt the key risk today, the number one risk to most organizations, is application security issues. There's no question about it. I'm an OWASPer. Most folks are either writing web applications, or porting to the web. The major threat to most organization is web application security issues. Programmers for many years have been taught to write code fast: "Get it out the door", "Are you done yet?", "Is it deployed yet?", "Let's just push it out." I used to work for WebMD and one of the senior VPs told me clearly, "Well, look, I don't care if you make mistakes. I want you to push this out the door. They're going to forgive us." That may have been the case in the Dot Com era, but when we saw 2004 or 2005 go by, and the awareness of web application security exploded, we can't just push it out anymore. We now need to build our applications in a more secure fashion, or the risk that we're giving to our organizations is so dramatic that it's going to be a game-changer in many cases.

So yes, without any doubt, I feel it's web application security that is the number one issue that should be on an CISO's mind today.

Brian Contos: When I first started getting into web application and database security, coming from the network security side, I was amazed how rapidly and how complex as well

some of these web applications were. They were very sophisticated, with very sophisticated backend database configurations etc. To your point, they had to get these systems up and running, out and customer-facing, world-facing as soon as possible. Security, application security anyhow, is a very small portion of their budget. They roll these out very quickly by engineers that perhaps didn't have any SDLC background. Security just wasn't a concern. Because of that, they are very vulnerable. So I don't think it's surprising to anybody in our industry when you just think about how many systems have been compromised, all the standard attacks, from standard SQL injection to clickjacking and CSRF, and all these other acronyms out there. I'm actually interested in some of these things where we don't know if they're happening, because so much is vulnerable about there, and we know that. It's just a question of when the axe is finally going to fall and people are finally going to understand.

This is an entry point into your most critical assets, your most sensitive data, and you simply don't have the right security controls in place. The code is not written right, you haven't done vulnerability assessment, you haven't reviewed it, and you're not using web application firewalls or similar technologies. You're just bringing a knife to a gun fight.

When we're talking about things like web application security and database security, a lot of people split these things in half. I'm from that ilk the two actually need to go hand in hand. They have to be addressed in tandem. Where do you stand on this? Do web application and database security need to be addressed in tandem, or do you feel it is something that can be separated?

Jim Manico: Brian, I would say that it really depends on your specific organization. I would say that organizations need to start by identifying the most critical risks to their business and then defend against those risks. So it depends on your application architecture. Typically this requires a combination of network security and application security, software security analysis, and doing database reviewing. Securing data in and of itself is not the same thing as database security. Database security requires a lot of things, actually. It requires configuring your database right. It requires hardening, secure coding, process, people, the whole nine yard. I want them to focus on some of the low-lying that everyone gets wrong. They get their database configuration wrong. They get their code wrong. Writing code that is not vulnerable to SQL injection is trivial. It is not a difficult issue, but still a lot of people get that wrong. They get some of their basic processes of deployment wrong, or the basic processes of separation of duties allowing coders to release production codes easily without review.

It's those things we've got to get right first. Once we have some of those basics right first, then some of the more high-end data-based monitoring technologies become apropos, I think, especially if you're in finances.

But I don't want to focus on some of the more high-end, newer forms of data-based intrusion monitoring and stuff, because if they don't get the basics right, they're done any ways and it doesn't matter.

So again, let's go back to the basics: database configuration, database hardening, secure code, process, people, building a secure architecture for your server farm environment. I think it's those things that OWASP preaches to make sure that those deploying complex web applications get the fundamentals right before we start focusing on some of the more advanced live data-based monitoring technology.

Brian Contos: I definitely get your perspective on that. One of the things that I've -- I'm sorry to see it a bit analogous to network security versus application security -- the fact that

network and app and database, it's all under that umbrella of security or maybe more so even risk. And a number of....

Jim Manico: Totally. Totally, Brian.

Brian Contos: I'm just seeing people that are trying to say, "Well let's just secure the web front-end," and they have horribly insecure database backends. Not only vulnerable to privileged user abuse, but perhaps insiders that are just standard users. There's just not the level of appropriate control. It's just one of those things that I tell people, when you're thinking about security and you're sort of breaking it into buckets, it's never one or the other. I'm a firm believer in defense and depth.

I really believe that if you're going to truly address "data security," you really need to look at the web applications, you need to look at the database side and you also have to look at the IT infrastructure, whether that's network, whether that's security pieces, et cetera, even physical controls.

Jim Manico: I think you're right on the money, Brian. Because at the end of the day, what is a web application? That's a fancy word for a very complex database application. That's all your web app is. It's some kind of custom layer between the outside world or your customers or your internal users and your most sacred IT resource, your internal corporate database. So if someone is thinking about database security that it's outside of the circle of building a secure web application, they are flat-out wrong. These things need to be dealt with together. You need to do your code right AND you need to lock your database down AND you need to do hardening et cetera, et cetera.

These things all need to be done correctly if you expect to build yourself a web application with significantly reduced risk.

Brian Contos: Yeah, well put. Given that, when we look at application security and how it's evolved and what the future might hold, what do you see over the next 5-10 years? What do you see as the big changes? Or what do you see as some of the gaps that you just don't think are going to be addressed?

Jim Manico: It's really this simple: I think if we can't change our mindset, to change it to a positive approach to web application security, we're done. We can't hack ourselves secure. We can't secure our current web applications by this "patch and pray." By finding holes and patching them and hoping that we solved the problem. So I think it's less "hack yourself secure" and more "positive approach." More building secure pieces and secure frameworks and secure components that can be reused. I'm personally a big fan of the ESAPI project from OWASP, the Enterprise Security API, which is a free set of Java PHP and ASP.NET libraries to make security much, much easier for your average developer.

It's those kinds of projects, positive approach, building secure applications from the ground up, less "hack yourself secure." These are the efforts that I believe we're going to see evolve over the next 5-10 years that will actually help us truly win the battle against web application security vulnerabilities, which we're losing today, in my opinion.

Brian Contos: That's funny. The whole "builder versus breaker" thing, I was just talking about that to a colleague the other day. It's amazing how many people are putting their research efforts into finding the next flaw as opposed to putting their research efforts to, well, how do we provide holistic protection? As opposed to saying, "Look what I can do on this obscure piece of code using this obscure buffer overflow." I hope that the balance starts

to switch to more builders. Right now I think there's definitely a disproportional amount of breakers.

Jim Manico: I agree with you 100% and breakers are important; we need to point out vulnerabilities. We need to do assessments. But we're not going to hack ourselves secure. We need to shift to a more positive approach if we're going to win, if we're going to break out of the cycle of the attacker's advantage that we have now.

Brian Contos: So, Jim, we have just a couple of minutes left. I just wanted to get a wrap-up from you and some closing thoughts on today's topics.

Jim Manico: Join OWASP, the Open Web Application Security Project. Help us change the world. We have individual consultants, there are vendors that participate, there are researchers. There's such a varied community of individuals that care about we application security. I encourage you to join us to both increase your knowledge but also to share your own knowledge about this topic. Our goal at OWASP is simple: We want to change the world to make a more secure world and we need your help to do it, so please join us.

Brian Contos: Well, Jim, this was amazing. Thanks very much for joining the podcast today and hopefully we'll be able to chat again very soon.

Jim Manico: I'm glad to. Thank you so much for your time, Brian.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.