

## Introduction to Web Application Security – an Interview with Joe White – Imperva Customer and Application Security Practitioner

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](http://Imperva.com), check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at [blog@imperva.com](mailto:blog@imperva.com).

**Brian Contos:** Joining me today is Joe White. In addition to working for a large SaaS provider in northern California, which is a customer of Imperva, Joe is president of Cyberlocksmith Corporation and specializes in information security and technology risk. He is a subject matter expert in Internet, extranet, and intranet security risks and network penetration techniques. He has 15-plus years of information technology experience, including SOA, SaaS and information security and systems.

Joe has focused expertise in securing web applications and extensive knowledge of networking routing protocols, switching and remote access methodologies. Over the years, Joe has participated in numerous penetration tests and ethical hacking engagements. He comes to web application security after spending many years involved in traditional infrastructure and operation security.

Finally, with 10-plus years of business development experience, Joe offers a unique perspective on the marriage between business and technology.

Welcome to the show, Joe.

**Joe White:** Hey, Brian. I'm incredibly excited to be invited to your podcast.

**Brian Contos:** I'm sure; I get a lot of that. [laughs] Joe, before we get started, I know you're working on some pretty cool projects and some new and innovative things over there. Can you give me a quick little update? What's new in your life?

**Joe White:** Not sure how cool the projects are, but I can definitely tell you that there's been a lot of time involved. I've been very, very busy, certainly for the last two or three weeks. I'm focused currently on a very risk adverse deployment of web app firewall and figuring out which vulnerabilities that I'm aware of that I actually want to plug in to the web app firewall. Along with the other day-to-day stuff, you know, design reviews and other fire-fighting adventures. So it's been a very, very action-packed two or three weeks, for me anyway.

**Brian Contos:** Joe, as a security practitioner and one who's this new breed of security practitioners, if you will - who has responsibility for security related to data and then specific web applications - what is your perspective on the general state of web application security?

**Joe White:** I'm a little bit out of the Pen-testing realm, but the guys who I talk to who still do that, to the extent that they're able to share with me, they'll say - with NDAs and stuff - that it's much worse than they expected it to be. It's much worse. For me, as I dive into my

daily tasks, there are just a lot of moving parts. There are a lot of pieces that, unless you're focused, it gets very, very complicated. Just being able to get visibility into what the problems are and then trying to come from a position of knowledge, as opposed to uncertainty, is a what I'm wrestling with in my little world at the moment.

**Brian Contos:** You know, Joe, if you had to quantify - I don't know - the top two, three, ten or whatever core problems there are, what are some of the biggest issues? Are they technology issues, political issues or awareness? Where are you finding the big problems?

**Joe White:** You know, I think a lot of it is related to the state of maturity of where we are with web application security. I think even though it's come a long way in the last couple of years, it's still pretty apparent to me that there are still some gaps. There is a lack of awareness of the foundation that needs to be in place in order to be successful. I find myself doing battle with the operations security guys a lot, because they don't quite understand this notion that maybe the deployment of security that they've worked so hard to build isn't exactly where you need to be focusing your time in the web app security world. There is the focus of kind of overall security awareness inside of the developers' engineering community.

The hardest part, I think to a certain extent, is one that every company is wrestling with being-cost effective with their security purchases. Companies, I think, don't realize or don't know enough software to 'fess up or admit to the fact that maybe some of the expenditures that they've spent so much money on in the past maybe aren't exactly correct in a web app security focused world.

It's difficult. If you're coming in late in the game and you're telling people that maybe they need to reconsider this, sometimes they shut down; they don't want to listen to you.

**Brian Contos:** I wish I could say that's an isolated case. You hear about that more and more. I'm hoping that over time these worlds will eventually collide or, shall I say, merge and these things will be a little bit easier, these battles that we're fighting. We're talking about the actual technology. There are a lot of different avenues you can take when you're looking at web application security. You can either take a singular perspective, or you can take a multi-faceted perspective.

Maybe you could give me some background on some of the technologies that I know you're intimately familiar with, things like web application firewalls, web application vulnerability assessment, code review and these types of things. Give me your perspective on how these play into the solution and where some of the major gaps are.

**Joe White:** That's a good question. About a year and a half or so ago, I started my current engagement. I'm responsible for web app security for a large SaaS company. I was kind of thrown in late in the game with a lot of legacy issues. In an effort to really figure out what I needed to do, I fleshed out what I thought were the most important priorities. From that I built what I called a roadmap to communicate the vision internally. Ultimately, I ended up vetting that into a local security community, a guy that I know. It turned out that a kind of sanitized version made its way into a recent conference.

In there are basically the steps that I think are important; our technology piece is built into that. For example, I think the most important piece is, of course -- If I can be a little colorful, you know your pants are down, but you don't know if they're down to your knees or your ankles. So you need a vulnerability assessment piece to actually figure out where you are.

Once you've figured out, and you've isolated some of the findings, then you'll need to figure out some way to address them. Ultimately, you definitely want to address them in the code level, for sure.

But maybe there's another way where you can buy yourself some time. It's great knowing your problems are there, but having 10 or 100 different findings and you have to prioritize them getting fixed, you can't just fix them overnight. You're going to have to buy yourself some time to fix them.

That's where maybe firewall comes in handy for certain folks as well. What I've found is exactly where that firewall is becoming incredibly important in terms of just getting visibility and to Layer Seven traffic. You have companies that are basically based upon web applications for their cost generation points. No one's really opened the hood to look underneath and figure out what's happening with the web application. What are the issues?

You may think you know, but we've coined this expression called HSM where the holy [beep] moments. So you look under the hood and there's all kinds of stuff that you see once you're looking at the traffic. You see recon. You see all kinds of things. You see escalated privileges, potential poking and prodding from your users. It's that kind of stuff that I think you just really need to become aware of. Then you can move on from there.

**Brian Contos:** It's funny, a lot of the people that I've talked to in the industry that have been here for a while, there used to be this -- and I guess in some cases there's still -- this battle between code review and vulnerability assessment and WAF. It seems like most people are saying it's certainly a combination of a number of different avenues. It's defense and depth, just like we've been doing on the network side for decades.

**Joe White:** I would agree.

**Brian Contos:** Another piece of it that I find is just general awareness, being an organization that... At Imperva we have a web application firewall and a database activity monitoring solution. We focus on data security. It's what we do. But I'm at conferences talking to people and they say, "I've heard all this fud out there and all this marketing from various organizations about something like, say, virtual patching. It's almost like we're under the impression that we don't need to patch our systems anymore, we can simply just run virtual patching on our WAF, and that's going to save the day and do everything." I say, "Whoa, you really need to step back and take a look at what the technology really does."

I think there are some great things virtual patching provides, such as integration with vulnerability scanner so you can scan your web applications for these vulnerabilities. We've discovered them and now there's links back to the WAF so you can protect against some of those attacks while you're in the patching mode.

A number of organizations, including us, will actually take patches from vendors, reverse engineer them, look at the difs between a patched and an unpatched machine, and try to build some protection mechanisms as well. That's never 100%. I'll be the first one to tell you it's not a replacement for patching.

I think maybe the early days of the WAF industry, there might have been a little bit of, maybe, overstating by some companies about what you should expect and what these tools actually provide. But now I think we're getting to the perspective where people like you, real practitioners, say, "Look, it can do firewalling. We can use it for auditing. We can use it for troubleshooting." It's a tool in the arsenal; it's not a replacement necessarily for other tools.

**Joe White:** I think you're right. There basically is no panacea. The web app firewall is not the elixir to happiness. It basically is one more tool. It's another arrow for your quiver, if you will. It's just one other tool to get visibility to help you become more effective and more successful. I think the key point that needs to be understood here is that not just one type of web application. If you really think about this, an e-commerce site, there's probably -- you know, if you have a store front or something, so even if you've got a burnt proxy or a parallel -- you have a high degree of confidence that if someone is doing that then that's probably bad.

But there are other types of web apps. There's like a CRM web app, or there's maybe a wiki. There's times when in a wiki you actually want to paste, "OK, well we did this particular...." So you want to paste the code in. In that case, the web app needs to actually value, to port would might otherwise be harmful.

The point I'm trying to make is that there's different kinds of web apps. There's actually no one perfect solution, I think, that works for all web apps. I think that 's the part that people are missing. I don't think the web app firewall... I don't know. I guess we didn't give ourselves any favor when they call themselves a firewall because that confused people to a certain extent.

For the most part, I think the realization is getting there that it does offer you one more tool, and it does offer you visibility into the traffic. With that visibility, you can do what it is that makes the most sense for you.

**Brian Contos:** You know, I sort of liken this to the network side. When I first started playing with Snort years and years ago -- not focusing on anything on Layer Seven, just simple, general Snort -- I first just started running TCP dumps and looking at data. I wasn't doing anything really all that fancy, just trying to do basic analysis. Then as you kind of get a feel, maybe set up some alerts, maybe set up some triggers that talk to the firewalls, maybe connect to a SIM. There's a whole bunch of other things you can do.

But, again, it's something that you can learn and grow with the organization. This whole notion, I've never seen -- in the whole time that I've been in security -- any silver bullet that says slap this in and this will solve all your problems, make your kids taller, make you smarter, and everything like that. It's just doesn't happen. I don't think it happens anywhere, but especially security.

**Joe White:** Your point's taken there, because I find that the more traditional security approach is to do this, do this, and do this, and then get a SIM. Then make sure that you've got everything collated and you're in actionable data out of this, or whatever. What I try and convince, or try and share with people is that, fine you're collating all of your data but do you really have all the data in there that you need for that to be actionable in a web application security context. That's not always the case.

It's great to have, maybe, all of your logs correlated or all of this, maybe the perimeter is correlated. But unless you're getting visibility into Layer Seven -- and that's also coming into this kind of pot that's trying to be your basis for actionable data -- then you need to step back and make sure that, before you start putting so much focus into collecting all the data and timelining it and making it to where it's actionable for forensics point of view, make sure that you actually have the web app-specific data in there if you're a web app focused company.

Oftentimes I don't think that the web app-specific data is in there. Then you have to step back and say, maybe I ought to start collecting it. How do we collect that data that makes us more actionable? Does that make sense?

**Brian Contos:** Yeah. I think it also goes back to the people that are actually the security practitioners today. 10 years ago we were all sitting around reading "TCPIP Illustrated," volume one, maybe we looked at two, I doubt three. Hacking Exposed came later and there was a Unix System Administration Guide, and you know, packet fragmentation attacks to bypass firewalls, and whitepapers like that. That's what we were consuming back then. Today, security practitioners, I'm not saying they have to be experts at Java or web application development or Python even, although Python is pretty straightforward, and these types of things, but you definitely need to understand how it works, and you need to be able to speak the speak.

To be effective now, if you don't know Layer Seven, you are really doing an injustice, I think, to the organization that you are trying to protect because at the end of the day, it is about people interacting with your data.

And that is really where the criminals are targeting. Those are the areas that we need to protect, and I think that is a level of awareness that security engineers are just going to have to adapt to and accept.

**Joe White:** I think you're right. At the end of the day, I think there is no shortage of passion within the security community, and the passion sometimes comes across as being emotional. So we have all these little religious battles about this versus that or whatever, but at the end of the day, I think every security practitioner or professional really, really strives to protect the end user. And as we get into more of a web app-centric world, at the end of the day that really boils down to data. And there are some changes. There is some adapting, but there is a different kind of a paradigm shift from a traditional perimeter focus as we get more into the cloud.

I don't mean to come out a little bit for myself. I do come from security from a traditional operations and a systems background and I've done many pen tests, but three, four, five, a certain number of years ago, I realized that landscape was changing. So I kind of forced myself to become more focused on web application security.

So if anything, I think if I can do it, anyone can do it. So there's really no time which is too late to understand the web application security risks and what it takes to actually be successful. It's all about building a foundational force of being successful with web application security, and sometimes you just have to understand what those changes are.

**Brian Contos:** Yeah, I think some people need an "aha" moment. And for any network security people there that are interested in application security, just really getting into the nuts and bolts of it, I'd say go check out OWASP, check out things like WebGoat, and look at SQL Injection. Figure out how, with the use of the apostrophe key, you can do things you never thought you could do.

**Joe White:** That's an excellent point. I don't mean to interrupt you, but that is an excellent point because I can so vividly remember reading about cross-site like scripting and I remember reading about cross-site request forward and I remember reading about all of these types of things. But until you actually see it, either on a pen test or you actually do it, for me though, and I understand the problems of forums and the web world, but when I actually saw it on my web application that I am responsible for, it just blew me away.

It blew me away that something could happen just by shared cookie space that you didn't even know because you had a valid session ID, and the ramifications of that were huge. It was really mind blowing.

So those "aha" moments that you are talking about, you're right. Everyone has to just somehow digest at their own pace, but those are huge. Those are very, very - those are epiphanies.

**Brian Contos:** Well, Joe, we have about time for one more question that I wanted to run past you. There are a lot of areas that we have talked about today that you and I will have on future podcasts, where we'll really start drilling down into these a little bit deeper and get into some more of the technology. But, what I'd love to do, and maybe we'll even do this for every episode. We'll have to figure it out. But, you've been exposed to this world for so long. Are there one or maybe two, if you think there's time, stories that you can sort of tell us of some of the pitfalls that you have run across either from a technology or political perspective or whatever when fighting these battles?

**Joe White:** I think what's important for others to realize is that if you are being looked at as the evangelist for web applications security, the important thing is to put together your vision and communicate it in such a way that there are no "gotchas," the expectations are clear that you have to do this in order to be successful. I'll try to communicate that we need to address all of our web application security exposure. If you think about it, maybe you have a web app that uses the same domain as your WWW site. Perhaps there's a same source issue for that particular domain, so you need to be looking at your web app security as well as your WWW site exposure, and maybe you even have some more sites that you're using.

The point I'm trying to make is that sometimes it's very hard for people to recognize that you need to be looking at your entire web application, Internet facing exposure. Those have been some tough battles, and only recently have I been successful in expanding our assessment capability beyond just maybe what you would think would be what you should be focusing your effort on.

The other point, you're going to need the help of the development community, of your developers as well, so you'll need to be looking for some evangelists which can help with that better than they can sign on board.

I find that the developers themselves are very, very helpful. And they get it once you show them. They understand what needs to be done to fix the problem. You just need to find the right people that can spearhead and make it successful. As a group, they are very, very helpful.

**Brian Contos:** Well, now, I think that painted a good picture of some of the high level points for sure. On other episodes we'll certainly pick a couple of those and drill down into them. We'll drill down into some of the technology. I think having you on the show really gives some nice flavor in terms of what is the practitioner's perspective. I mean, me, at the end of the day, I work for Imperva. And hopefully, you and I can do many more of these podcasts together to get that message out.

**Joe White:** I agree with you entirely. We may work at for a particular company, but this is not about us. This is way bigger than us. This is about protecting our users. This is about protecting the security, trust and integrity that end users have in web applications. At some point, we all have to step aside and recognize that we have to think of this properly as a

## Introduction to Web Application Security with Joe White

unified security issue and not something where we have these fights and vendor issues. This is bigger than all of us.

**Brian Contos:** Agreed. Well, Joe, thank you so much for being on the show today.

**Joe White:** Thank you, Brian, for inviting me. I look forward to the next time we talk.

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



North America Headquarters  
3400 Bridge Parkway  
Suite 101  
Redwood Shores, CA 94065  
Tel: +1-650-345-9000  
Fax: +1-650-345-9004

International Headquarters  
125 Menachem Begin Street  
Tel Aviv 67010  
Israel  
Tel: +972-3-684-0100  
Fax: +972-3-684-0200