

## WAF and VA Unite – an Interview with Jeremiah Grossman CTO and Founder of Whitehat Security

Listen to 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).

Joining us today is Jeremiah Grossman. Jeremiah is the founder and CTO of Whitehat Security, an Imperva partner. He is considered a world-renowned expert in web security, is co-founder of the Web Application Security Consortium and was named to InfoWorld's top 25 CTOs for 2007.

Grossman is a frequent speaker at industry events and universities around the globe. He has authored dozens of articles and white papers, is credited with the discovery of many cutting-edge attack and defense techniques, and is a co-author of Cross-Site Scripting Attacks. Grossman is often quoted in business and technical press. Prior to Whitehat, Grossman was the Information Security Officer at Yahoo.

Well, welcome to the show, Jeremiah.

**Jeremiah Grossman:** Thanks, Brian, for having me.

**Brian Contos:** So Jeremiah, I guess it's been a week or so since RSA. What'd you think of the conference this year?

**Jeremiah Grossman:** Yeah, actually, I thought it was pretty good all things considered, considering the economy and people's budgets being cut. The people we were running into there seemed to really get security and people that are really looking for solutions to their problems.

**Brian Contos:** So one of the things we did while we were there is we shot a little video, a little five minute video that people can check out on our website, about WAF and VA but today, we're going to dig into that a little deeper. I really wanted to start off with a very simple question: why WAF and VA and why now? Why is this such a hot topic?

**Jeremiah Grossman:** Good question. You know, the web application firewalls is actually interesting and predates website vulnerability assessment products. One of the interesting things is vulnerability assessment kind of proves out the need for web application firewalls. But about up until two years ago, I was a staunch opponent against web application firewalls - I didn't think they got to the root of the problem, until I saw how big the problem actually was, from our work at Whitehat.

## WAF and VA Unite with Jeremiah Grossman

That we have a tremendous number of websites, a tremendous number of vulnerabilities in each of those websites and the security guys, who are responsible for securing those websites, don't have a lot of control over the fix and the developers don't work for them.

So, they needed additional options. So whether or not web application firewalls, you know, functioned as a general concept, didn't really matter to me at all, at that point. That we needed to make them work, and how best could I help out that process.

So, what I did know is: I do know our websites are vulnerable, too; I know specifically what types of issues because we find them on all these websites; and that I might be able to bring that information to a web application firewall, so they can act upon it. Our job is to find vulnerabilities. A web application firewall's job is to prevent them from being exploited. I thought that was a really good relationship to be made there in the technology.

**Brian Contos:** What do you think is really driving this though, in the field? Are there specific early adopters that have said, "Look, this is absolutely a requirement for us to do business," are there regulations, are people just becoming more aware of application security vulnerabilities? What do you think is the chief driver behind that?

**Jeremiah Grossman:** Websites have been around for a while, so have vulnerabilities. So I haven't found just the existence of a vulnerability to be a gigantic driver or at least, get the business to move and act upon it. So I think, there's actually, going forward over the last 18 months, two big drivers. One is the PCI regulations that says you must do code review or have a web application firewall. The other one is just simply the bad guys. All the network layers have become a lot more secure and so all the easy stuff to exploit and monetize has been driven up to the web application layer.

So I think, in a lot of ways, unfortunately, the bad guys are actually forcing awareness of web application security. It's either you're going to take care of it or you're going to get exploited.

**Brian Contos:** Yeah. And definitely, there's been a kind of paradigm shift from network security to application security probably or I should say data security. And probably over the past couple of years, most organizations, I think, have a relatively good grasp, hopefully, on their network security perimeter, maybe even putting some steps inside to address insider threats - but when it comes to the application and database security -- actually protecting your data, there seems to still be a relatively large disconnect.

I don't know if I want to say it's like network security was in the early 90's, but it certainly isn't at the level of most network security solutions today. Would you agree with that?

**Jeremiah Grossman:** Oh, yeah. Actually, I think that I wouldn't hedge on that one. I think that's exactly what it is and we're going to go through the exact same evolution that network security did in the way that solutions are adopted, the way that people think about the particular problems. I think the history is going to repeat itself with the application security layer. I won't say that's a good or bad thing, only that that's the way it'll actually happen.

**Brian Contos:** So let's get into some of the nuts and bolts. What are the major impact points of web application firewalls and VA working together, when you're looking at application security?

**Jeremiah Grossman:** I think they actually can work in two ways. The first phase, what we want to do - what we're doing with Imperva-- is that when Whitehat finds a vulnerability,

we can point out the exact spot of where the particular issue is and how it can be best defended. That way a web application firewall can take its most restrictive rule set and apply it to the spot that you're vulnerable to. This is a bit different than a generic kind of deployment, where you go, "I'm going to block all SQL injection attacks against all parts of the site, whether I'm vulnerable or not." That can work, but there's more problems with false positives in that regard.

The other one we want to get to is, when we scan websites, we can never be 100% sure that we found all the links or all the functionality and get to all the nooks and crannies of the website. So there's a constant comprehensiveness problem with regard to black box testing.

What we want to do is, since the web application firewall will see all user traffic, they get a very different view of the web application than an outsider does or one outsider does. So what we want to do next phase forward is for a web application firewall to relay back to us what to scan and when to scan and I get more timely with our assessment results.

**Brian Contos:** So when we look at our companies, not necessarily the technology, but, you know, that's to say to the industry that we've got Imperva, a WAF provider, a DAM provider, working with Whitehat, such a well-known vulnerability assessment organization, what's that say to the industry, now that we've got these two organizations actually working together, so closely?

**Jeremiah Grossman:** It's an evolution. We both mean maybe not only for defense in depth, but to virtually patch issues that we know we have. So that's value there. So now when people are looking at a holistic approach to website security, whether it's SDL, is it training, is web applications firewalls and VA. It's all these things, and the better we can inter-operate these technologies and these processes, the better it is.

**Brian Contos:** Are there any specific vulnerabilities or maybe even more generally, any specific threats out there that you think the integration of WAF and VA is particularly well-suited to address?

**Jeremiah Grossman:** Sure. I think, as far as the web applications and firewall side alone, the things that technology can find... Let's say Black box testing kit is really good at finding cross-site scripting a SQL injection. We're really good at those particular things. And it just does happen those are the particular things that the bad guy are exploiting the most. Probably because we can - automated finding is really easy in those particular cases.

Now as technology can find it, technology can also block it really well. So that's where the web application firewalls come in. So it takes a lot of those issues off the table, the ones that are giving us immediate problems right now. But by the same coin automaton also can't find everything, find all problems in a 100 percent automated fashion.

So you if you can't find them all in a 100 percent automated fashion, you probably can't say that you can defend them all in an automated fashion. But we're getting there, we're understanding more about the particular problem at taking this and taking a more scientific approach.

**Brian Contos:** You know web application security has been evolving. The vulnerabilities have been changing. Certainly the attackers, they've matured and they've become more organized etc. What do you see as the future of web application security, and perhaps the future of WAF and VA integration? Let's say five years out.

**Jeremiah Grossman:** So five years out is tough, I'm struggling for the next 18 months out, truth be told. But I think the issues that we're dealing with now, we're going to have really good solutions for wiping out today's issues. The thing that we're keeping an eye on here at Whitehat are the more rich Internet applications; the Flash the heavy AJAX, the heavy, heavy JavaScript, the Silver Lights and things like that.

I think those are going to have some really real world challenges to them three to five years from now. Because they are getting deployed now, and we really don't have a good sense of what their security posture is, and what they are going to do or how they are going to affect the entire landscape of website security, browser security, and the co-mingling of the two.

And what we do know is assessing flash applications in a black box, or even white box fashion is extremely difficult. It presents entirely new challenges. SO those are the ones that we are looking three to five years out.

Unfortunately, by the time we understand what the problem are, there's probably going to be world-wide deployments of these things. And we're going to get into a large scalability issues in those as well.

**Brian Contos:** Certainly. And if history is any indicator, as well all know a lot of these web application developers, especially when they use new technologies are under pretty strict deadlines to get this code out there, get these systems public facing, get the operations turned up. And even though we think we've matured a little bit as an industry, security tends to be an afterthought for a lot of groups, unfortunately. And that means there are going to be a lot more vulnerable systems.

**Jeremiah Grossman:** You know, I used to come down hard on that particular philosophy. Security as an afterthought, we generally don't like that, but honestly there is a really valid business concern to get out there, make money, "We'll deal with the security issues later." Maybe because we don't really know what the security issues with technology we're using anyway. And you really can't wait to learn what they are.

Are we really going to expect companies to fully R&D and fully vat out Flash as a technology and everything we understand about it before actually deploying. That gonna put them way behind, and we can't expect businesses to do that.

That's why I've been an advocate of that, the way we approach web security is to be more agile in our security defenses, that we're not going to know everything ahead of time. But when we do know something, to be able to react accordingly.

To be able to react faster, so we don't have to recode the entire web just because we learned something new. That's the struggle that we're in now.

With click jacking for instance, all of a sudden we find this sort of new thing. Are we really going to recode the entire web to prevent it, or cross out request forgery? No, we're going to need point solutions to take care of it on a more world-wide basis.

**Brian Contos:** Yeah, that makes a lot of good business sense. I actually liken it to earlier in my career when I used to work for Bell Labs. And at that time, Bell Labs was developing voice over IP solutions. And one of their competitors was, at the time, Cisco was doing the same thing. So Bell Labs took a very telephony specific perspective, were they wanted five order of nines built in to their voice over IP solution. And they just wanted to make sure it was as rock solid, and as hardcore as the traditional POTS lines, plain old telephone services.

## WAF and VA Unite with Jeremiah Grossman

Cisco said "Ah, it's like a router, like a switch. We're going to get it out there; I'm sure it will have bugs and flaws, but we'll fix them and people will forgive us, and we'll just get out there and get it up and running." And let's look at the market today. How many of us are running Bell Labs voice over IP telephones, and how many of us are running Cisco? Right?

**Jeremiah Grossman:** Right, exactly.

**Brian Contos:** So, very interesting. So we have about it me for a few last comments. What type of parting thought would you like to leave the audience with today?

**Jeremiah Grossman:** Oh, that's a really good question. I guess don't get stuck in the ideologies out there. Understand what your web security challenges are. Understand what they are going to cost you, not only to integrate new solutions, but also how much are they going to reduce for your organization over time. And at the end of the day you want defensible position when and if something bad happens. Because that's - I'll take a page out of Hoff's book; 100 percent security is never guaranteed. So you have to look at also your survivability. When and if bad things happens, how best can you reduce the impact when it does happen.

So that's what I want bring more of to web security is a more realistic and more practical approach to the whole problem.

**Brian Contos:** Very well stated. Well Jeremiah, thanks so much for joining us.

**Jeremiah Grossman:** My pleasure, thank you very much Brian.

**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