TRANSCRIPT: 10.24.2016

SPECIAL ECOMMERCE ONLINE SECURITY SERIES

What Online Store Owners Need to Know About PCI DDS (Payment Card Industry Data Security Standard)

Bob Dunn: Welcome to the WPE Commerce Show, a podcast about everything e-commerce and WordPress.

Hey everyone and welcome to our show. Bob Dunn here, also known as Bob WP on the Web. Today, we bring you episode 36, but also the third part of a 4-part series on security and e-commerce. Last week, we heard from our guest, Dre Armeda, via our sponsor, **Sucuri.net,** as he narrowed down the topic from the big picture of online security to security in e-commerce, but still a birds-eye view. Also in last week's show, Dre did give us an introduction to the PCI, or if you're wondering about that acronym, the Payment Card Industry. There's some standards there, and we're gonna be chatting about that more. We're gonna get down and dirty with

the PCI, explore it more in depth. It may not be the sexiest topic when it comes to your online store, but I'm thinking it's a damn important one.

To give you a better idea of why as a store owner, you need to pay attention to the PCI, we bring Dre back to the show. Of course, Dre may be looking forward to the day when he doesn't have to talk to me weekly, but heck, until then, hey Dre, welcome back.

Dre Armeda: Hey, thanks for having me, Bob. Look, if I could talk to you every day, it makes my day a brighter one.

Bob Dunn: Oh, man, no. You're pushing it there. I'm going to take you up on that, see just how long that lasts.

Dre Armeda: Hey, you know, we have to apply it to see what happens, right?

Bob Dunn: Yeah, really. In episode 2 of this security series, as I mentioned, you talked about, explained the high level of what PCI is. Can you cover PCI a bit more in-depth, to give the audience a good definition of PCI, its impacts and its benefits?

Dre Armeda: Well, I'd be happy to cover that, Bob. Bear with me, because I think it gets really intricate, and I don't know that diving too, too deep will be helpful for your audience here, but I do want to get a little bit more deeper-rooted, I think it's important to understand, so let's give it a go.

As we noted in the last episode, when it comes to e-commerce, it's not a matter of having more or less obvious vulnerabilities, which is kind of the intro question that we had last week. The vulnerabilities across platforms are typically pretty similar, right? The big difference, though, that we need to consider, especially when it comes to commerce, is around the motivation. The motivations are a little bit different.

I think when it comes to online commerce, as we noted last week, the motivation's pretty clear. It's access to sensitive information, or PII as it's known under the PCI standard, personal identifiable data. The other piece of that is the primary account data, which is PAN, and other cardholder

data including expiration codes, security codes, your credit card numbers, all that fun stuff. That's the important piece, people are looking for that stuff. This is the kind of compromise that we call data exfiltration, and it's the action or objective that's perhaps the most different, when you compare that to the attacks, say, on a blog or regular site for example. Unless you're a large organization, like I mentioned last week, in the health industry, which has got this whole set of other issues when you start talking patient data and things of that nature, which is really sensitive.

But I think the thing to keep in mind is the data's super important not just to the customer or consumer, but the website owner. Certainly because we need to safeguard these things, we want people to keep coming back and buying stuff from us, and that's why it's just as important to the attacker. They know it's valuable, and they're using it to ... you know, this information to go and purchase whatever else. Bitcoins to games, and what have you. Really crazy stuff.

Let's break down a little bit of history on PCI specifically. PCI is not a law, okay. It's not a government regulated entity or standard. And actually, the real name for it is PCI DSS, okay, which means "payment card industry data security standard." It's a standard that covers all of the data, it's connected to payment card information and how that's treated, how that's stored, and so on. It contains a series of security requirements that every merchant, big or small, has to follow, if they want to be in compliance. If you're processing credit cards, again, I don't care if you're this small cupcake shop or a huge enterprise with 10,000 SKUs, you need to follow PCI if you're processing any credit cards.

All merchants need to understand that PCI compliance specifically applies to all merchants that accept credit cards, regardless of how they do that. PCI was created and mandated by 5 major credit card companies. Visa, MasterCard, American Express, Discover, and JCB. It's managed by a council, the PCI Security Standards Council. They administer and update the standards, and do all that research and fun stuff. You can go check them out over at PCISecurityStandards.org. This is very important. We'll talk a little bit more about that as we get into the show here.

This was created, initially, and still is standing to provide a minimum set of security standards or regulations designed to help protect what is known as the cardholder data environment, CDE. There's 2 real major parts to an e-commerce site. One is the CDE, how you're processing credit card information. Customer comes to your site, and they go through the whole card process, and when they go to process, they send you all their credit card information. This is usually secured or encrypted with SSL, and that's sent to a third party payment processor or gateway, and then hey, this is awesome, the credit card's legitimate. We go ahead and ship you off your fun stuff once that's verified.

The other side of that is the application side of it, all right? What are you using for your cart and so on? Is it Commerce, is it ... what have you, there's plenty of titles out there, and then how does that interconnect and integrate into the CDE, the cardholder data environment.

PCI gives you a number of very good recommendations, and that's the idea behind it, right, on how to secure your online business. They'll minimize your risk of your site getting compromised and have information stolen from you. That's bad. We do not want to do that, or have that happen, so we want to reduce that risk. I'll assure you, your customers are going to be super grateful to have their information safeguarded. They're not going to be very happy if their stuff gets stolen. I think the outlying long-term impacts are pretty big, one of them being if you're not compliant with PCI, the fines can be pretty harsh. We'll talk about that a little bit in the show, but I think more importantly, it won't be worse than the brand impact and the loss of trust that you're gonna acquire from your clients by not taking this really seriously.

I think that's a bit subjective, but certainly both have their impacts. Obviously, you don't want to get fined. Monetary loss is super sad. I know I don't want to get fined, but jeez, how do people view your brand. That's crazy. The punishment could ultimately be that you're completely blacklisted from using any of these credit cards, right, or processing these credit cards. That's a super big challenge, right, if you can't accept payments. If the issuer of these cards blacklists you, how are folks going to buy your products? It's a huge domino effect. There's a lot of issues that could be involved here, and we want to avoid those altogether.

The reality is really, the cardholder breaches and theft affect the entire payment card industry. It's not just your site, but ... a breach plays on the trust of a customer, right, or cardholder, and it's merchants. It's financial institutions, like everybody's involved. A breach I think pushes a huge personal connection and fallout that can affect well beyond just your website or your commerce experience, or the commerce experience that you're providing. Think about your credibility as a merchant, and how you want to be perceived. You want to be a trusted source. What do you stand to lose with a breach? These are the things you need to be considerate of, when you're securing, and using judgment based on these standards on how you want to safeguard this information. What are the effects on your business if your carelessness leads to a credit card theft from your site? What happens then?

Bob Dunn: Yeah, I think all that information is good. It's like you said, is it too much information? But it's a standard, it's something that the commerce online store needs to pay attention to. It's like if you're a doctor, you've got the medical board, and all those things that go on, lawyers ... Everybody has the different standards, and they're kind of, I hate to say it, the dry and boring stuff. You sometimes go, "I don't even want to hear it," but it's so important.

Dre Armeda: Yeah. It could be super annoying, right, for vendors and merchants, consumers, alike. Ultimately, for me, my perspective, when I go buy something online, I damn well hope that the merchants I'm using are compliant, they're adhering to these standards, because they're safeguards put in place to protect my financial state, right? My identity. I don't want people using my credit cards.

It happened to me once. I was at a conference. Actually, it was Blog World a few years ago, and my credit card was stolen, and I had something like 15,000 dollars in a loss. I had to recoup that. I had to go through the whole process to recover that and then do an investigation. That sucks, man. That's a pretty big hit, dude.

Bob Dunn: Oh, that's huge.

Dre Armeda: Yeah. I mean, these are the things that can happen, so you want to make sure that you're protecting your customers and consumers' information, as best you can.

Bob Dunn: Yeah. If I'm a small merchant, you know, and obviously I must be responsible for PCI, or you know ... How am I responsible, or am I? What is a merchant risk level, and how do I determine where, as a small shop, fit into the grand scheme of things when it comes to this PCI.

Dre Armeda: Good question. I think it's important to understand, I don't care what size you are. If you sell one cupcake a week or a thousand an hour, every merchant has a responsibility to be compliant with PCI. Even if you don't store, manage, or transmit transactions directly from your site, you have an absolute responsibility to your user base. If you operate an e-commerce site, PCI compliance is a requirement. Compliance is not dictated by the volume of transactions, okay, or restricted even to storage, the transmission and processing, like I mentioned. It applies to any business that accepts credit cards.

What this means is even that if you're leveraging services like Stripe, Recurly, PayPal, you name them, right? There's a ton of them out there that actually do the processing for you. As a business owner, you have the obligation to follow the requirements set forth in PCIDSS. Your specific requirement, obviously, and obligations are going to be dictated by various sets of information. The compliance piece of it is not the volume of transactions, but your obligations fall into different categories.

It's divided into 4 different levels, okay. Level 1, being for organizations processing over 6 million in transactions a year. Again, this is going to fluctuate based on various things. When you start thinking beyond that, there's, again, 4 total levels, and everything in between. Level 4 being for those that process under 20,000 in transactions. They even group those into its own plan. For layers 2 to 4, you'll be able to do what's called a self-assessment questionnaire, or an SAQ. Actually, we've wrote an article, we've written a few articles on the Sucuri blog. One, specifically, navigating PCI self-assessment questionnaires, or SAQs, for e-commerce websites. That's super helpful to understand for those that aren't storing that

information or processing it on their site, because it's, again, very different compliance standards.

If you go to the PCISecurityStandards.org website, there's also an area that has documents, and they have a breakdown of the different types of assessments, and templates that you could use to see what you need to cover. There's one, it's called Self-Assessment Questionnaire A-EP, and it's in a of compliance. That one's specifically for those that are partially outsourced e-commerce merchants using a third-party website for payment processing, again, the Stripes, the PayPals of the world and such.

There's a specific breakdown for the things that you need to be checking, but it's important that you do those. Those self-assessments, they require that you go through each of the requirements that they have set down, one by one, and from there, it'll tell you whether you're eligible, or you're within standards or not. It's recommended that these are done annually, and that you're doing scans of your network every quarter. Every quarter. There's other specific steps that we're going to break down in terms of how you get started and such, and I think we'll cover a lot of the things that you need to do, but that's one of the most important things to consider, is going through these, and going through these questionnaires, and making sure that you fulfill all of the requirements broken down in these.

Again, they're very different based on the type of merchant, what you're processing in terms of volume, how you're processing and storing. Is it on your site? Is it third party, and so on. But you've still got to follow the requirements, so again, the smallest shop out there, one cupcake and you're using Stripe, there's still some requirements. Many of our clients think that PCI doesn't apply to them because they're too smal, and that's a serious misconception, and it's a very common one, but it applies to all businesses that accept credit cards.

See, I've got a couple things from the PCI website, section for small, medium businesses that explains how seriously they take it. Small merchants, you must secure cardholder data to meet the PCI rules. Small merchants are prime targets for data thieves, and it's your job to protect cardholder data and points of sale. If cardholder data is stolen, again, this is for small shops, and it's your fault, you could incur fines, penalties, and

even termination of the right to accept payment cards. Again, that's what we talked about earlier, and we'll get a little bit more depth on that.

Ultimately, what it comes down to, Bob, is if you're not taking it seriously, if you're not taking security seriously and you do get hacked and customer information stolen, you're going to face some repercussions, one way or another.

Bob Dunn: Yeah, that's so good. I'm glad you really brought up or threw the question about the small shops, because they are going to thing, "Hey, what do I need to do?" In fact, our next question kind of plays into that, because a lot of people that listen to this podcast are running these small shops, and they might be right now saying, "PCI? I've never heard of that," which, kind of scary in itself, but that's why we're trying to educate everybody. Now, it's a really important aspect of creating an e-commerce website, so those people that are thinking of doing it or have just started doing it, may be a fairly new concept for them, the standards of the PCI. Where does one start in terms of beginning to implement PCI?

Dre Armeda: Oh, man. Give me a hug. Hug it out. I think ... brass tacks, right? Let's stick to where the standard initiates from. It's out there for a reason, so going back to the website, PCISecurityStandards.org, and started to research is super important.

Implementing PCI really is about scoping, okay? This process involves identifying all of your system components, where they're located, how they're connected, how they're connected to cardholder data and that environment, the whole CDE we just talked about. It's compromised of various things, right? We talked about this in our first show. People process technology. Holy cow, even PCI covers that, and dictates it. All those moving parts are part of this, right? All those parts connect, touch cardholder data at some point, sensitive information. The authentication process. All things to consider.

Scoping, again, is an annual process, and you've got to do these self-assessments. I don't care how big you are or how small you are. Merchants and all entities got to identify all locations and flow of their cardholder data. They've got to ensure all applicable systems and components are included

in that scope, so they're understanding what is touching, what is storing, what is transmitting, et cetera, on this cardholder data. Is it within those PCI standards? Again, leaning back to those self-assessment questionnaires. Are you meeting all of those requirements that are in that self-assessment questionnaire?

There's different components in PCI compliance that fall into ... it's funny enough, like a 12-step program, right? Oh my gosh. Hi, my name's Dre, and I'm PCI compliant. Right? These are broken down into 6 groupings, and a total of 12 steps, and they're all very important.

We'll start ... I'm going to kind of break down these 6 sections and the sub-sections. The first one is building and maintaining a secure network. How are you doing that? What is your entire stack? How are you sure it's secure? One of the first things that PCI dictates is that you maintain a firewall configuration to protect all your cardholder data. That is a requirement. THere's different ways to fulfill that requirement, and there's vetted and approved vendors that can provide that to you, but that's very specific, and this is outlined right inside of the PCI compliance. You'll see this inside of the SAQs, your self-assessment questionnaires around how that's doing, how that's working, and so on. Again, there's a vetted list of vendors and so on.

The second piece of that is don't use vendor-supplied defaults for your system passwords and other security perimeters. How are you using your password management to make sure that it's not all default stuff, right? This goes back to that password discussion, and using safe password management to make sure that your credentials are not enumerated, and all of a sudden, you're hacked because you're using "password" as your password. Bad idea.

The second section to that, Bob, is protecting your cardholder data. So number 3 and 4 of that portion of that is protect stored cardholder data, and encrypt transmission of cardholder data across open public networks. What does that mean? SSL, right? If you're transmitting, anytime you're transmitting, it's got to be a secure channel. You can't just submit in the clear, that's bad news. Protecting stored cardholder data. How are you storing, if you have credentials, if you have payment information, all that fun

stuff, on your server? Is it encrypted? Is it sitting in the clear? That's a problem. You've got to, again, adhere to those steps.

Third area is maintaining a vulnerability management program. Use and regularly update anti-virus software, develop and maintain secure systems and applications. Again, some of this sounds high-level, but look, these 12 steps break into a pretty big standard, and the questionnaire can get pretty deep-rooted.

Implementing strong access control measures, so restricting access to cardholder data by business needs to know only, right? Assign a unique ID to each person with computer access, so that you can manage that. You can come in and check to see what that user is doing. And restrict physical access to cardholder data.

Regularly monitor and test networks. Track and monitor all access to the network resources and cardholder data, and regularly test security systems and processes. That's a big deal, you should be doing that anyway. You should be doing that in partnership with your host, because they've got some requirements here too, right? It's not just you, the e-commerce shop, but everything that you're using.

Maintain an information security policy. Maintaining that means addressing all these different components of security, and how you're handling that, who's responsible for all of these things, from auditing to scanning and so on.

These 12 requirements cover different business areas, obviously, but they break down into something between 200 and 300 different sub-requirements. That's just a high-level breakdown of it, and you'll find more information on that as you start reading and becoming more knowledgeable with the whole PCI security standard.

Each requirement, basically, in the SAQ, in that self-assessment questionnaire, is a check box. You have to go through and make sure that you hit all of these. They can be very simple. As an example, in 6.2, that requires all system components and softwares are protected from known vulnerabilities by installing patches. There's some really complex ones, like

in 10.2 of the standard, that requires automated audit trails implemented across all of your system components. It can get pretty robust, and again, it's going to vary based on the type of merchant you are, what you need to fulfill.

We have a blog article, PCI: Build, Maintain, and Secure Your Network on the Sucuri blog as well, that is super helpful with that. At the end of the day, every single piece needs to be documented. You need to make sure that all of this is covered, so if you're audited, you have documentation on all this stuff, and that you're putting the right policies and processes in place to make sure that you're adhering to these things.

I mentioned earlier that everybody's got a responsibility. For example, your hosting provider, if you are processing credit card data, are they PCI compliant? If they're not, through your process, when you go to get audited and you're going through you're questionnaire, they need to be audited, because they are part of your stack. They touch that information, right? You may be storing that information there, so they need to be compliant.

Is your firewall provider PCI compliant? For example, we just, over this year, got our PCI Level 1 service provider assessment completed, and we've been certified, and attested as a certified PCI Level 1 provider. If you're a level 1 merchant, and you're getting PCI Level 1 approved, and you go to put the firewall, which is a requirement in step 1 of that 12-step program, we are an accredited firewall. You can put us in your stack, and we're level 1 accredited through PCI. We do not need to get audited. That portion is fulfilled in your requirement, because we are PCI compliant. Every portion of your stack that touches credit card info, or that protects against all these things within the PCI standard, need to be accredited, or somehow audited.

Yeah. I mean, at the end of the day, that's really the initial breakdown. The SAQs, so going through the self-assessment questionnaires, and really adhering to that 12-step breakdown with over 200 plus checkboxes, if you will, to make sure that you are safe, and you're safeguarding at the best of your ability.

Bob Dunn: I think you've given us a lot of good information. I mean, this is stuff that people really need to, obviously, pay attention to, and during that time, you've talked a little bit, "This is what's going to happen if you don't do it," and touched on possible fines and all of that. I'm thinking that if you do not comply as a store owner, you could face serious repercussions. You mentioned fines, like I said, in the event the credit card is stolen. Can you talk a little bit more, without ... you know, we'll send them to a link that actually shows, probably, all of the details, but a little bit more about the consequences of not following PCI in the event of a security breach?

Dre Armeda: Yeah, for sure. I think that's super important, because it does get a little bit deeper-rooted, and there are breakdowns of how and what can happen there. I think there's two sides of it to consider, and I think under the standard, this will become very apparent as you become more familiar with it.

One is noncompliance, and the other one is the consequences of a breach. Both can happen. One can happen. Obviously, if you're breached, you're going to get checked and validated, to make sure that you're PCI compliant. If you fall out of compliance, then you certainly will have some other things to deal with. But if you experience a security breach and it's found to be noncompliant, but within the rules, the fines are a portion of that. They can be really steep. In fact, depending on the circumstances, merchants may pay between 5 and 100 grand a month, until they address the issue. If they don't resolve this satisfactorily, what ends up happening is your accepting credit cards, the ability to do that, would just get revoked by the credit card companies.

The key is to remember, PCI noncompliance fines ... merchants are not fined by the actual council. Again, we talked about PCI Security Standard Council, that actually governs this. It's the actual credit card companies, it's the credit card brands, that are penalizing the merchants acquiring this stuff, right? It's not so much the standard, the government ... it's the credit card folks. The bank has the ability to pass the loss along by assessing a fine on its noncompliant merchants, so these credit card companies are going to hit you if you are noncompliant, or if you get breached.

The enforcement structure is important for merchants, particularly new merchants, to understand, because acquiring banks bear the brunt of responsibility for merchant security efforts. They have a degree of flexibility in their PCI enforcement policies, and this adds another important consideration for merchants as they get to knowing their acquiring banks.

Fines for noncompliance vary on the discretion of the card bank. It could be different across the board. Again, 5 to 100 grand per merchant. It's a high price, right? For you being negligent. Can your company, can your business absorb that? It's a pretty big hit. Something really to consider. I think when you think about the noncompliance side of the fines, it's ... that's, jeez, I think the maximum fine levied for a breach can be up to half a million dollars. 100 grand monthly, but I think it's something like a half million dollars if you fall out of compliance. Jeez, they'll come in and do forensic research, and if you don't remediate, man, you'll keep getting nailed. Institutions are going to levy some pretty harsh punishment if you're out of compliance.

The other piece is, again, the breach and consequences there. Even if a company is a hundred percent PCI compliant and validated, a breach ... it could still happen, right? These attackers are going to find ways, and it can result in, again, stiff losses. 50 to 90 dollars per cardholder data that is compromised. 50 to 90 dollars per cardholder data, that's fined. That could add up pretty quick, so let's say you have 500 data sets that are compromised, right? That's a reasonably small number when you start talking about large e-commerce sites.

Bob Dunn: Exactly.

Dre Armeda: That adds up pretty quick, and when you start adding that up per instance, per day, that's a whole lot of tacos. Beyond that, I mean, suspension of credit card acceptance again is a potential. I think that where you start to see stuff that's outward facing, it's loss of reputation with your customers, your suppliers, and your partners, because you're all put at risk. You start to see the potential and possibility of civil litigation from your breached customers, and then ultimately, loss of customer trust, which affects any future sales.

Take the preventative measures. It's to better protect your business. The standard doesn't exist just to make rules and regulations to be enforced by penalties. That's pretty stupid, right? It's because it's a serious issue. It's an important and very valuable thing that we're trying to protect here, and it'd be highly rewarding, really, to your business, if you choose to conform with these standards. That's a trust factor that you're building with your client base. Your customers, your suppliers, and your partners. As a minimum, standard for these payment processing industry standards, PCI is ensuring that your system's stronger and better protected from these breaches. It's in your best interest to really adhere to them.

In short, security of your cardholder data affects everyone. It's not just you, it's everybody that's interconnected there. It reduces trust across the entire Internet and commerce space. Even think of non-commerce sites like the LinkedIns of the world, that have been nailed, and hundreds of millions of accounts have been exploited. How do you feel about doing work online? It affects you. It's important that we're doing our best to minimize this. You're going to save yourself money, you're going to save yourself time, which are probably 2 of the biggest and valuable assets to your business online.

Bob Dunn: Yeah, I didn't want to end it with the last question of all doom and gloom, you know, here's these huge fines, but you're right, people got to be aware of that, and if they know it, it's even that much more important to be compliant. I like how you also brought in the fact that yeah, we're talking money, fines, but also the brand and reputation you have, which can be as much or even more disastrous.

Dre Armeda: Absolutely, absolutely.

Bob Dunn: Yeah. Well, if our listeners didn't know about PCI, they do now, that's for sure. I love it.

Dre Armeda: Hey, I hope it was useful. I think it's an important part. You know, we're so stuck on what's right in front of us, right? Like, "Hey, I need to update WordPress, that's awesome. Hey, I need to add this next SKU," but you're accepting some credit card transactional information, what are you doing to safeguard that and protect your client base? What are you

doing to show that your business is a responsible party in selling, and should be, and could be trusted to safeguard this information online?

It behooves you to check out PCIDSS, check out PCISecurityStandards.org. Go to our blog, search for PCI. You're going to see a bunch of cool articles, from steps on how to start ... PCI requirement, one. Install and maintain the firewall. Holy cow, that's literally step 1 of the standard. From there, don't use defaults. What are you doing to make sure that you're hardening your environment and protecting against these attacks?

Bob Dunn: Yeah. Running an e-commerce site is obviously different than running that site for your business, so you're just putting up a few things, there's all these other variables including everything you just talked about, and I'm glad we're able to bring in people like you that can bring those to light and help people build, grow their online stores.

Again, thanks so much for sharing your expertise and knowledge with us, Dre.

Dre Armeda: My pleasure, my pleasure. Thanks for having me, Bob.

Bob Dunn: You bet. Now, speaking of the last show of this series, that I introduced this of at the beginning, in the final episode, we are going to be talking payment gateways, probably one of the largest challenges for many people who are starting or even running an online store. I know from experience, having talked to so many who are planning their stores, or even current store owners, understanding and choosing a payment gateway or gateways really can sometimes bog down your progress, and often, you may hit a brick wall with that one, as far as that being one of the aspects of your store, and a very important one. Dre will be returning, as I mentioned, but we will also be joined by Lee Blue of Cart66, to bring in even more tips, insights, and experience around payment gateways, so make sure you tune in.

Lastly, do check out our sponsor, **Sucuri.net**. Their **blog** has an amazing archive of posts, as Dre referred to, on just about every aspect of online security that you can imagine. They also have a free scanner on their site where you can check your own site at no cost, and of course some very cool plans to keep your site secure, as well as services to help you if you've been hacked, and some of those services include, like Dre said, firewall.

Getting your site compromised is no fun at all, and trying to fix it yourself, well, a search on Google and following someone's instructions can often make the matters worse, or you think you fixed it, and heck, the hack raises its ugly head again. That's why I always recommend calling in a pro like Sucuri. Check them out today at **Sucuri.net**. That's Sucuri ... Dre has a little hard time with spelling, so it's S-U-C-U-R-I.net. I'm just giving him a little bad time, last seconds of the show. Sorry about that, Dre.

Dre Armeda: I love it, I love it. If I may add, Bob ... Look, folks, if you're interested in learning a little bit more about how to account for security in all of your customer projects, I'm actually doing a Webinar as well here, the first week of November. I'd love to have you join us, and I'd love to have you ask questions that we can help you with. You can find that over at sucuri.net/webinars, or hit me on Twitter @dremeda. We'll get you signed up.

Bob Dunn: Very cool. I will also put a link to that in the notes. Until we meet again, everyone, stay safe. Tune in to our next WPE Commerce Show.

BobWP
The WP eCommerce Show

Thanks to our Sponsor!