Cross-Site Scripting

Description: In this second installment of their three-part coverage of web-based remote code injection, Steve and Leo discuss cross-site scripting vulnerabilities and exploits. Steve quickly reads through the 28 vulnerabilities discovered in popular software just during the previous month and discusses the nature of the threat and challenge facing authors of modern 'dynamic' web sites and services.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-086.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-086-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 86 for April 5, 2007: Cross-Site Scripting, Part 2.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Nerds On Site. Looking to grow your IT service business? Find out how Nerds On Site can help. Visit Iwanttobeanerd.com.

It's time for Security Now!, our second episode of the week because we had a special on the problem with the animated cursor vulnerability: [64 kbps: http://media.grc.com/sn/SN-085a.mp3; 16 kbps: http://media.grc.com/sn/SN-085a-lq.mp3]. That was on Monday. Trust you've solved your problems with that. Steve Gibson's back now to resume our conversation about cross-site scripting. Hey, Steve.

Steve Gibson: Hey, Leo, great to be back with you.

Leo: What's the update on the animated cursor, by the way?

Steve: Exactly. I was just going to say it's worth making sure that everyone has run Windows Update. Microsoft did, as we expected and as they had stated, push out an out-of-cycle, single-vulnerability fix just for this problem on Tuesday, which would have been the 3rd. And so that's a week earlier than their normal second Tuesday of the month patch cycle, which apparently they're still going to have a bunch of other stuff that they're going to be doing next Tuesday on April 10th. But I want to make sure that everyone's got that.

So, you know, it turns out that it's being widely exploited. There's now a lot of use of it on the 'Net, hoping to find users who are not updating, who don't have Windows Update turned on, who haven't visited Windows Update and in one way or another gotten themselves patched. So I imagine there's going to be, for a month or so, a strong effort to continue to install malware into unsuspecting users' machines through this vector. And it may never go away completely, as these things tend not to.

Leo: You have to think that there was this window of vulnerability. The vulnerability's been out there for three months. Microsoft patched it April 3rd. And there were exploits happening as early as March 30 or even earlier. I mean, that's the first we heard it. That must mean that some, many, maybe millions of computers were bit.

Steve: And actually I got email specifically from people after our special podcast saying they knew of, I mean, personal knowledge of specific instances where people got malware through this vector. So we called it a zero-day exploit, as we do when it's discovered – when the first discovery of it publicly is its exploitation. What's annoying, as I mentioned a couple days ago, is that Microsoft was sitting on this thing. Now they say they were planning to patch it on the 10th, which I assume they were because they knew it was a bad problem. But they were not in any real big hurry for the last three months or four months. So it's like, okay. You know, this is the frustration that I hear from many security researchers, like the guys at eEye. At one point they were showing a calendar of how long things they had informed Microsoft of had just been ignored by Microsoft. And known vulnerabilities remaining unpatched for, like, six, nine months even.

Leo: I've been hearing this from security experts for a long time. This is a very common complaint about Microsoft. And I understand that Microsoft doesn't want to push patches it hasn't tested because, especially now that people have automatic patching turned on, there's a risk in that.

Steve: Well, and in fact I got a wacky error message about a conflict of address space on a DLL. I think it was the htmlhelp.dll, but I'm not sure. But it was after the system rebooted on an XP machine where I had applied the patch. And I know I'm not alone because I saw some other reports, actually I received some other reports of the same thing. So there was some sort of a little oopsie, you know, interaction that got away from them. And you can see Microsoft really pushing for what they call "responsible disclosure." They're big into responsible disclosure now to remind everyone that they don't want irresponsible disclosure, which is to say they don't want to be pushed or hurried.

Leo: And that some might characterize as irresponsible, to be honest with you. eEye, as long as we're mentioning them, I'd love to get your opinion at some point down the road, does offer a free, I guess it's a firewall. It's called Blink.

Steve: Yes. Blink is a very well-known and reputable tool which is sort of their prophylactic around Windows which they maintain. And it's like their main deal is this really nice – well, they also have something called Retina, which everything of course is in the eye, e-y-e, theme.

Leo: Oh, I get it, all right, yeah.

Steve: So you've got Blink and Retina and so forth. And I guess it deals with Windows

cataracts, I'm not sure.

Leo: Security blindness on the part of Microsoft. So it's hard to exactly figure out what it is. It sounds like it's an antivirus. It sounds like it's antispyware. It also sounds like it does some Internet security. It sounds like it would be a very good choice for a lot of people.

Steve: Well, consider this. It has the same sort of auto-updating features. And they inform Blink, that is, eEye informs Blink of the stuff they find when they find it. So during this somewhat frightening – I can't think of the word, the word I'm looking for – this sort of refractory period during which Microsoft knows about a problem but hasn't yet fixed it. Well, the eEye guys that know about the problem, they have fixed it in Blink. So Blink users were protected during this whole period of time from December 20th of '06 when they informed Microsoft, all the way through now. So that's a very cool thing. I mean, you'd like to have that kind of preemptive protection.

And then, of course, once Microsoft fixes it, I'm not sure whether the eEye guys remove that rule from Blink or leave it around. I would imagine they'd leave it around because it's, you know, it's a good thing to protect yourself from. So it's like, whereas the AV people are often always playing catch-up, you could argue that eEye with their Blink tool is really leading the pack. Of course there are other vulnerabilities that they don't know about that other security researchers are reporting to Microsoft. And it's not clear to me how active they are in trying to reverse engineer those things and put that protection into Blink as well. One would certainly think that it makes sense for them to do so.

Leo: So you would recommend Blink. Of course, if you're running another antivirus or security software you probably shouldn't mix. And so that's the question, is Blink a full-service antivirus or just a purpose-built antivirus to...

Steve: And I haven't looked at it that closely. But these guys are down in Southern California, not far from me. We might consider getting them on the show and talking about their stuff.

Leo: They're good. I trust them.

Steve: They are. And I've also met them at a couple of user group meetings. And they've really got the technology.

Leo: So that's the good news, it's [audio glitch] XP, Windows 2000, Tablet PC and Media Center. The bad news is it doesn't come on Vista. And the really bad thing is it's the first serious Vista vulnerability. Here we are, not two months into the Vista era, and already a serious unpatched exploit that's been there since the beginning, since Vista shipped, that doesn't bode well, frankly. I mean, to me the sole recommendation for Vista is improved security. And if it can't do that, well, I don't know.

Steve: Well, it's certainly the case that this is old code. This has been around for a long time for it to affect all versions of Windows, including Windows 2000. I did note something interesting, and that is that apparently it's XP Service Pack 2 that is affected, but not presumably original XP and Service Pack 1. So it sounds like something that got introduced somewhere along the way. And it's worth mentioning also that this ANI, this animated cursor issue, if that sounds familiar to people it's because there have been security problems there in the past that Microsoft – so Microsoft in fixing those may have created this or didn't find this

one when they were in the code fixing other ones. But this has been a vector for trouble that we've seen before.

Leo: Good to know, and we'll keep an eye on it. Of course that's one of the reasons we do these special updates. It's kind of our commitment to you, when we see an issue like this, we will push out a special edition of Security Now!. That's a good reason to subscribe to the podcast, not rely on manual downloads or listening on the website.

Steve: It is – yeah. I'm sorry. I didn't mean to interrupt you.

Leo: You can do that through iTunes, of course, and we have a podcast feed of this is I guess what I'm saying. Subscribe to it.

Steve: I did want to remind people, though, that IE7 with its enhanced protection turned on was not vulnerable to this. So that is an aspect of Vista's enhanced security which does bear against this kind of problem. Whatever it was in detail that was causing the trouble, turning on the IE7 extra protection that is available in Vista did prevent this.

Leo: Is that on by default?

Steve: I don't remember whether it's on. It's in the standard security settings, and it's sort of innocuous looking. I sort of think it's not on by default actually because, again...

Leo: It breaks a lot of sites.

Steve: That's the problem is that you start getting – in fact, someone sent me just recently a DEP error that IE was kicking up. And I think it was under XP, I'm sure it was under XP because he sent me a screen shot of the dialogue box. And so but that was IE causing some sort of trouble. Which is, again, which is why we're moving very slightly toward tightening things up. But I'm glad to see Microsoft really is putting pressure on the world to make the stuff more secure.

Leo: Let's see. Any other addenda or additions before we address cross-site scripting?

Steve: Well, yeah, I did want to talk about, follow up a little bit on last week's discussion of eBook stuff. I know that there's a strong interest in it. The thing that brought me into the topic, as you'll remember, last week was that I've had a lot of feedback from people saying, hey, you know, what other authors do you like? I loved your last recommendation of Peter Hamilton. Who else? And so of course I talked about Michael McCollum at scifi-az.com, SciFi Arizona, as another one of my favorite authors. He and I have had some email back and forth because I've been interested in figuring out basically what it would take to move his electronically downloadable books over to the Sony.

And in fact you'll remember, Leo, that when we talked you had had the Sony for a while, that is, the new Sony eBook reader, they call it the Sony Reader, it's the PRS-500. And I was expecting mine to arrive the following day. It did, and I'm now converted. I like this experience. I've picked up my Palm that I was using for years, various Palms, but the one I was most recently using, and just sort of looked at the screen again and then looked back at the Sony.

And I've got to say, I mean, it would be nice if the Sony had an optionally turn-on-able backlight of some sort that was available – or maybe like edge lighting or something so that you didn't have to bring your own lighting. I know that you bought the booklight, I also did, from Sony's site, that clips on the top and sort of reaches around. And it's got just two very bright white LEDs that do a great job of illuminating this thing. But overall I really like this.

Now, I mean, I've got a bunch of complaints with it. But I'm also an early adopter, as I know you are. And I remember Sony's journey through the MiniDisc. Their very first MiniDisc recorder that I owned was sort of a big black portable blob with a big battery pack that connected to the outside. And it worked, but it was first-generation. It had that feeling. And then a year later they had one with three times the battery life and smaller batteries and more features, and it was smaller. And then another year later even better, and another year later even better. And, I mean, to the point now where their current MiniDisc recorders are just these gorgeous little things, I mean, really refined.

And so I think that this first reader has the same sort of feeling. I mean, it is new technology. It's using this eInk technology, so-called "electrophoretic display." And the way it works, I've learned a lot about it since because I've been curious, is I described it incorrectly last week as spheres that rotated either their white hemisphere or their back hemisphere forward, which is actually one of the eInk technologies, but it's not the one this one uses. And have you noticed ghosting from, like, the prior page?

Leo: Yeah. There are couple of complaints that we all have. I talked to Patrick Norton about this because he was really high on this as well. And we all agree, the controls aren't great, and this little flicker you get when you turn a page is slightly annoying.

Steve: Yes. It turns out that Sony – there are different ways to refresh this technology. What's actually happening is that the pixel resolution, that is, the pixels we're used to thinking of in terms of what's on screen, is 800x600, so it's sort of the original, what, SVGA resolution. Although of course it's in portrait orientation as opposed to the 4x3 original VGA landscape orientation.

Leo: And for the size of that screen, that's a pretty high resolution. That's a decent...

Steve: Oh, and Leo, I've been very critical of the, I mean, I've stared at the screen with a very critical eye, looking closely, as closely as my eyes will focus on the characters. And they're beautiful because they are anti-aliased characters. So what's actually happening here is that this screen has an ultra-high particulate resolution. I mean, down in the something-or-other microns. And there are tiny, tiny little particles of titanium, I think it's titanium dioxide, which is a white particle. And it's embedded in a dark hydrocarbon-like oil, essentially, emulsion. And so what happens is, when these particles are pushed to the back, you see darkness there. And when they're pulled to the front, you see their whiteness there. But the idea is so there's this super-high resolution surface, I mean, really high resolution. And then there are charging pads on the front and back, transparent of course on the front and not necessarily so on the back, which put an electrostatic field across a square region of all of these particles. So the point is that the ghosting is when not all of them move all the way back or all the way front when you've switched one of these pixels, rectangular regions, from black to white or white to black.

So it turns out that there are – there's like a quick change that Sony can do or a more extensive change where it's sort of like, you know, how hard do you shake the Etch-a-Sketch. It's sort of, you know, that's sort of an analogy for it. Do you want to really shake it hard and get it all the way erased, or are you kind of, for reasons of UI, would you rather just do it more quickly because a little bit of the past won't really annoy you. And so Sony has different strategies for this that they've been evolving. I'm not minding that screen change. It does...

Leo: You get used to it.

Steve: ...take a little, yes, it takes a little getting used to. And in fact because there's a little bit of delay, I'll now hit the next page button while I'm reading the last line of the screen, knowing that it's going to take a while for it to catch up with me.

Leo: You're a smart monkey. You've learned. You've adapted.

Steve: So there are a number of things...

Leo: Why is it not paper white? That's my biggest complaint is that it's not as high contrast as it could be.

Steve: I completely agree. And I think it's just that the nature of the particles, the particle density, the particle color, and probably the fact that it's basically very white things suspended in a dark medium, even when you pull them all to the front, you're still going to have some of the dark goo that's around them, it's going to be lowering their overall reflectivity. One of the things that I have noticed is that, unlike a book, like regular book paper, like especially paperback paper that sort of tends to be a little bit yellow, this is almost metallically reflective. In other words, it tends to reflect the color of the light on it. So that, for example, when I'm under incandescent light, it has sort of a yellower feel than when I'm outside it has a much bluer sort of look. And when I'm under white LEDs that sort of have that real sort of blue crispness, it looks just fantastic.

So I'm pleased with it. There are a whole bunch of UI things. You talked last week about not being really happy about the page turning. I completely agree with you. I'm still having to kind of figure out how to hold it so that my thumb or a finger can rest on the buttons. Also it's wrong that paging forward is given no more preference over paging backward.

Leo: Right, because that's what you do mostly, yeah.

Steve: Exactly.

Leo: How often do you turn a page back?

Steve: Exactly. Sometimes if the paragraph on the page you're reading, wait a minute, doesn't make sense, or you got interrupted while you were reading, you'll have to go back to...

Leo: But that's probably one time in ten.

Steve: Oh, if that. I would say more like one in a hundred.

Leo: A big button that says Next Page.

Steve: Yes. And sure, you definitely want to be able to go back. But you don't have to go back equally to going forward, which is what they offer you right now. So again, I want to remind people, I mean, this thing is, what is it, $349?

Leo: Right, it's cheap.

Steve: So, well, okay, except – you and I each have one. There are people who have said, and I completely understand...

Leo: That's ten hardcover books, and you can put a hundred on there.

Steve: Okay, from that standpoint, yes, it's cheap.

Leo: Of course, the books aren't cheap. The books are only slightly cheaper than the hardcovers.

Steve: What I am absolutely sure will happen, and this is always what Sony does, I mean, the first Walkman to the Walkman now, the first MiniDisc player to the MiniDisc player now, anything they do, it starts out big and bulky, sort of almost proof-of-concept. It's like the engineers say, we can do this, let us try, let us try. And so they're going to prove themselves. And so I would say to anybody who's annoyed by Apple with the iPod phenomenon, where you buy one and then next week they come out with the one you wish you'd waited for, but you didn't know they were going to come out with one a week later, certainly we are going to see the price of this thing fall. It is Linux-based. There's a bunch of stuff that they've left in there that they didn't need to leave in there. It's running MontaVista, I think it is, MontaVista Linux.

Leo: Must be an embedded Linux. My only question would be if it's selling well enough for Sony to pursue it. It may be, I mean, do you get the sense that it's taking the world by storm? I don't.

Steve: I have no sense for that yet either way.

Leo: Yeah. And so that could be a bad sign. We know Sony is unusually defensive of their products. Look how long they've kept MiniDisc alive. But at the same time, if it's not doing well, I don't know if they would...

Steve: Well, and it is DRM'd again. That's the other real annoyance. Although I have to say that I think, and you would know this better than I because I just read this once, that when you purchase a book from the Sony CONNECT store, you have five or six devices that you're able to install it on.

Leo: Now, remember the computer is one.

Steve: Yes, the computer counts as one. But still that seems very liberal to me.

Leo: It's much like the iTunes store. I wouldn't say, I mean, how many devices are you going to put that thing on?

Steve: Right. Right. I like the Palm model, actually, the Palm Reader, when you download from them you need to unlock it using the credit card number you used to purchase. And their theory, of course, is you're going to be reluctant to give your credit card number to anybody else in order to unlock the book you bought on their reader. So I think that's sort of a nice, clever inhibition for piracy. But and I will say that, Leo, I have never ever seen the battery charge indicator come off of full.

Leo: I know. Neither have I. It goes a long time.

Steve: And also the books tend to be 350, 360K, like an average-sized book. Which means that the 100 megs which is free in this thing will, I mean, it's all the books you will ever need to carry at one time. So the only reason I can see for using the SD card and the Memory Stick, again, another Sony proprietary technology, would be for music. And as an experiment a couple mornings ago I did put a bunch of music on it. And it's the only thing – playing music was the only way I was ever able to get the battery full meter off of high.

Leo: How did the music sound? Because I haven't listened to music on it.

Steve: Sounded absolutely fine. And in fact, if I didn't already own every iPod and a Shuffle and all these things...

Leo: Can you read a book and listen to music at the same time?

Steve: Well, my music, I've got this weird sort of spacey stuff.

Leo: But, I mean, will that technology allow you to play a song while you're reading?

Steve: Oh, it's designed for that.

Leo: Oh, see, that's not so bad. Oh, that would be nice. I could put some classical music on there and read.

Steve: That's exactly right. There's an artist called Liquid Mind that I really like. And it's just, it's very, you know, ethereal, interesting sort of ambient in the background...

Leo: Perfect for a plane, perfect for a plane.

Steve: Yes. And so this works perfectly. You stick your headphones in, you go and choose what music you want. Now, they don't currently, at least I don't think they currently have any sort of playlist facility, and they sort the music based on the name in the ID3 tag.

Leo: It's kind of an afterthought, in other words.

Steve: Yeah. No, again, everything about this is first-generation. You are able to create book collections, as they call them, in order to provide some organization of authors and books by collection. There's no facility for that over on the audio side. So what I did is because they don't even sort based on filename, they sort based on ID3 tagging, I went in and edited my tags in order to force the sort order that I wanted because it always plays...

Leo: The same.

Steve: ...in the order, yeah, exactly, in the same order. But, I mean, it really works. You plug your headphones into the bottom. You turn on music. And then you go right back to reading, and everything works great.

Leo: What kind of life do you get with the music?

Steve: I don't have any sense for it because I had never charged it. And I've been using it extensively now for nearly a week. And when I plugged the headphones in and started playing music, not long after I first saw the highest charge bar disappear. But I'd already been using it for days without even a thought for charging. That I really like. And I have to say, I mean, the text is so large, it's very readable. I'm not trying to promote our listeners to go purchase this the way I really wanted to recommend Michael's books. And by the way, he will before long have his books also offered in Sony Reader format.

Leo: Thanks to you. You've figured out the way to do it.

Steve: Yes. The industry is a mess at the moment. And I could do it now with a lot of jockeying around. But I'd rather work out the way for him to be able to convert his books over. And he's absolutely demonstrated an interest in doing so. For example, he made "Gibraltar Earth" available to me in a format, basically he exported what he had in HTML, and I found some really wacky tools, I mean, Python and Java and all this junk mixed together. But I'm reading "Gibraltar Earth" now on the Sony Reader. And so it's completely workable, and I'm really pleased. And of course I'm rereading it because I'm excited to go to the sequel, which is "Gibraltar Sun." But there was some confusion. I wanted to make sure people knew that, if I were to recommend a first series to read of his, I think the Antares Trilogy, which I first recommended to you, Leo, it's just fantastic.

Leo: Well, I have both. And I was a little disappointed because they're unprotected PDFs, which in theory you can play on the Sony Reader, but it turns out you can't just put any old PDF on there. And so with your help I hope he'll re-encode them so I can read them. I'm looking forward to bringing it to Vancouver with me. That's the main reason I bought this. I found myself carrying a giant "Judas Unchained," the giant Peter Hamilton book, on the plane, weighs about eight pounds. And I thought, you know, I need something lighter for this stuff.

Let's, before we get to cross-site scripting, I just want to mention once again our great friends at Nerds On Site, at Iwanttobeanerd.com. They are sponsors of this podcast. And they are looking for more nerds. It's kind of a neat idea. These guys aren't – they're not

the company. They're a guild, really, of independent contractors. So you're still in business for yourself, but not by yourself. So you focus on your passion and not the burdens of running a business. This sounds like a great idea. I wish there were something like this for podcasting. There are Nerds On Site in seven, I think eight countries now – Canada, USA, Mexico, England, Australia, South Africa, and Bolivia, all over the world. If you are an expert, PC to Mac, Cisco to Oracle, fixit technicians, website designers, programmers, project managers, even sales, trainers, security experts, antivirus gurus – they particularly like those folks who like to tear apart, build, and troubleshoot their own systems – visit Iwanttobeanerd.com and register for a Nerds Only meeting in your area today. Nerds On Site, Iwanttobeanerd.com.

Steve: And Leo, that's sort of a perfect segué for a fun mention of SpinRite, too. I didn't understand until I read this that this was one of the Nerds who had sent me a note. And so you'll see as I read this from the context that that must be who he is. He says, "I would just like to share an experience I had using SpinRite last week. I had a PC in my office" – and this is a different sort of SpinRite testimonial, too, so as you'll see it's a different aspect of SpinRite. "I had a PC in my office that I suspected had a hard drive going bad. I ran chkdsk on it several times, and it found nothing. The PC kept blue-screening and freezing up at the worst possible times." Like there's a good time to get a blue screen.

"So I decided it was a good time to try out SpinRite. I started to do a scan and was ready to let it run as I have heard other Nerds say it takes a while to do its thing. Within a minute or two a screen popped up from SpinRite saying that this drive was in danger of complete failure, cancel the tests and back up any data as the drive may not survive the testing process." And that's something that's cool, that's something cool that I built into SpinRite 6 is while it's doing its stuff, it's constantly polling the drive's SMART subsystem. And as we know from a podcast we did on this, SMART is not as smart as we would like it to be. But it has the ability of really raising a red flag and saying, okay, we are in serious trouble here. So that will never false-positive. It generally doesn't save you the way it would be nice if it did. But since SpinRite is monitoring it all the time, if SpinRite sees that its own use of the drive is causing the drive to panic, it'll stop and say to the user, look, there may not be enough of your drive left here to save.

So continuing with his note, he says, "I was a little skeptical, to say the least. But to save time I put in a new drive and started reloading Windows. Just for kicks, I put the 'bad' drive in another PC and started SpinRite again to see what it would do. About five minutes into the test I heard a very familiar clunking sound coming from the definitely bad hard drive." And he says, "You don't need to be a nerd to know that's not good."

Leo: Now we know. He's come out of the closet. All right.

Steve: He said, "The drive crashed hard." And then he says, "It's great to know we have access to a product" – meaning the Nerds because I've done a deal with the Nerds guys to make SpinRite available to them, a site license, essentially, which is one of the things we offer – "that we can rely on to give us accurate results and thus make us better techs. My thanks to Steve Gibson and the folks at SpinRite for saving me a bunch of time." Dave Everett in Michigan.

Leo: That's great. You should add that, you know, "Nerd Certified" or "Tested by Nerds."

Steve: It's all over the country.

Leo: Inspected by Nerd No. 5. All right. Let's get to cross-site scripting, shall we? This is something we talked a little bit about last week. We kind of got our start, but now we're going to go into some greater detail, as you are wont to do. You like to set us up, then knock it down.

Steve: Well, and so last week we sort of talked about the generic problem of what I would call, stepping back a little bit, sort of overall website or web code injection, where through various mistakes made in servers and in the sort of next-generation web code that is now becoming so popular, in other words to say scripting, all kinds...

Leo: Folks, just in case you didn't know, Steve doesn't like scripting.

Steve: Well, all kinds of problems are being created. Now, rather than just saying that and making a blanket statement, I thought I would start out by giving people a sense for recently discovered problems with prominent and less prominent web-based software. So I started enumerating them. I thought, okay, we'll just go for 2007. What's been found in 2007? Well, there was so much trouble that I said, okay, forget this, let's just do March. Let's just do March because March had 28 problems that were identified...

Leo: Wow. Where do you go to find this stuff?

Steve: Well, the really terrific resource I continually use is the SANS Institute. You know, the SANS security guys, I'm on their mailing list; I get notices of this. And it's one of the things that has always had the issue of cross-site scripting on my mind as something I wanted to talk about in this podcast is because I scan it every week, and I see what's going on. And sure enough, every single week there's six or seven or eight or nine new cross-site scripting vulnerabilities that they're reporting. And so it's like a constant annoyance that I'm seeing this going on. And I wanted to, again, we've never talked about this before, so I thought it was a topic really worth mentioning. So I'm going to very quickly, as quickly as I can, zip through just in March what was found. And to give people – it'll give you a sense for obscure companies and some well-known companies like IBM and Oracle are mentioned in here as having vulnerabilities, and also sort of a sense for the nature of the problem. So the first one here is:

"Built2Go News Manager Blog is a blog application. The application is exposed to multiple cross-site scripting issues because it fails to sanitize user-supplied input." We'll be hearing that phrase a lot. "Built2Go News Manager version 1.0 is affected."

Then we have "OrangeHRM is a human resource management application. The application is prone to multiple unspecified vulnerabilities on the login page of the application. OrangeHRM versions prior to 2.1 alpha 5 are affected." So it sounds like they found out about that, and they fixed it.

"Webmin is a web-based Unix system administration interface..."

Leo: Oh, yeah, everybody uses this. I use this.

Steve: Uh-huh, "...implemented in Perl. The application is exposed to multiple cross-site scripting issues because it fails to sanitize user-supplied input to multiple unspecified parameters of the 'chooser.cgi' script. Webmin versions prior to 1.330 are affected." Wordpress. Ever heard of that?

Leo: Yeah.

Steve: Uh-huh. "Wordpress allows users to generate news pages and web logs dynamically. It is exposed to a cross-site scripting issue because it fails to properly sanitize user-supplied input to the 'post' parameter of the 'wpadmin/post.php' script. Wordpress version 2.1.1 is affected."

"Webpress is a web-based publishing application. The application is exposed to multiple cross-site scripting issues because it fails to sanitize user-supplied input. Version 2.1.1 is affected."

This looks like "Docebo" – D-o-c-e-b-o – "is a content management system (CMS) application. The application is exposed to multiple cross-site scripting issues because it fails to sanitize user-supplied input of 'index.php' and '/modules/htmlframechat/index.php' parameters. Versions 3.0.5 and earlier are affected."

"PhotoStand is a photo blog application. The application is exposed to a cross-site scripting issue because it fails to properly sanitize user-supplied input to the 'a' parameter of the 'index.php' script. PhotoStand version 1.2 is affected."

"PhpWebGallery is an image gallery application. The application is exposed to multiple cross-site scripting issues because it fails to sanitize user input. PhpWebGallery version 1.4.1 is affected."

Active Calendar, now, I'm going to stop going through this. But I'm going to say Active Calendar, web-based calendar creation; Trac is a wiki and issue tracking system; the dynaliens program is a guestbook application that's got problems. Lazarus Guestbook is a web-based guestbook application; it's got problems. vCard Pro is a virtual greeting card application – oh, goodness. That's got problems.

"VirtueMart is an ecommerce application. The application is prone to multiple cross-site scripting issues because it fails to sanitize user-supplied input. Unspecified parameters to the 'ps_cart.php' and 'virtuemart_parser.php' scripts are vulnerable."

"DirectAdmin is a web site administration panel." "Oracle Portal is a portal application integrated into Oracle's application server software. The application is exposed to..." blah blah blah, blah blah blah. "IBM Rational ClearQuest is a software development management application...is exposed to cross-site scripting..." blah blah blah. "Multiple Cisco products are exposed to cross-site scripting issues because they fail to properly sanitize user-supplied input."

"Horde Framework is a web log application. The application is exposed to..." multiple HTTP cross-site scripting, blah blah blah. "PHProjekt is a modular web-based application to share information and documents." I think it probably shares a little more information and a little more documents than it was intended to. "MindTouch DekiWiki is a file server and intranet tool." Oh, again, Oracle Application Server has a problem. Here's another WordPress "PHP_SELF" problem. Interstage Application Server has a problem. "Overlay Weaver is a web-based search engine..." that's not happy. eBitWhizzy, I'm not kidding – oh, no, I'm sorry.

Leo: This is all in the month of March, by the way.

Steve: This is just March. I was going to do the '07.

Leo: I'm glad you didn't. I don't think we have a long enough podcast.

Steve: I think everybody's glad. They don't have enough time to download this. aBitWhizzy, I've got three left, is "aBitWhizzy is a PHP script that uses whizzywig.js to create and edit web pages through a WYSIWYG interface. The application is exposed to multiple cross-site scripting and directory traversal issues because it fails to sufficiently sanitize user-supplied input to the 'd' parameter."

"Mephisto Blog is a web log application, implemented in Ruby. The application is exposed to..." blah blah blah, multiple cross-site scripting blah blah. CoCounter, I'm sorry, "CcCounter is a web site hit counter application. It is exposed to a cross-site scripting issues." Aagh.

[Full text for above:

http://www.GRC.com/sn/files/Cross_Site_Scripting_March_2007.txt]

Leo: Well, one thing that becomes obvious is that most of these are web-based tools. That's of course why they're at risk, because anybody can use these tools and enter in data, and then the data can be overflowed.

Steve: Well, that's exactly right. So there's a couple things this means. Essentially, you know, look how long it took us to get Microsoft up to speed on security. Now what's happened is, essentially, because of Web 2.0 and PHP and Ruby and JavaScript and all these other tools that are allowing and empowering, in all fairness, empowering web guys, webmasters, and administrators to create really amazing active websites, suddenly now they're all having to be security experts, and they're not.

So the problem is that any situation where it's possible for user-supplied input to contain scripting itself, that is, that's the whole injection deal, the whole cross-site scripting problem is that users are able to provide stuff which the application will then digest and perhaps show to them or to other users. And in the process their browsers, which are running scripting as part of what they do to offer these features, their browsers will run code that malicious creators have written and, bang, you're in trouble. You don't need buffer overflows. DEP won't protect you. SSL won't protect you.

Basically the fundamental problem is that the way web page scripting has been designed from the start is you could argue it's too powerful because there's a free mixture of web visual content and interpreted content mixed right in. That is, right in the middle, for example, of a web page, you could say [script], and then you could say document.cookie and then [\script] in order to close the script. What would happen is, when your browser is showing you this page, it encounters that script tag and immediately, without any requirement, switches on the script interpreter which reads "document.cookie." Well, that's a variable which the interpreter replaces with your cookie for that site, and then it continues. So what the user will see is blah blah blah, they're reading along, and then they will see the cookie, which is supposed to be and up to now has been secret between them and the remote server. Their browser understands that it's okay to show this cookie because after all it's a page coming from this remote server. Well, that power, the power of being able to embed script anywhere, and you can even embed it in the arguments of queries, you know, the famous "get" query which search engines use, for example, in order to send information back, you're able to put script tags even there. And the browser will dutifully interpret whatever the script is and run it on the spot, replacing whatever you've got with current variables.

So it turns out that there's a way, and it's well documented, all the hackers know about how to do this, where if you provide the URL for a malicious server as part of that little script, you can have the malicious server receive the cookie for whatever server has served the page. Which means it completely breaks this notion of cookies being safe for authentication and for session tracking. I mean, for example, when I'm using eBay, I choose the little checkmark of leave me logged in for some length of time until I explicitly log out. The same thing with Amazon. I

mean, Amazon is smart in, for example, if I try to add a new mailing address for books, it makes me type my password in again, which is a good thing because what cross-site scripting does is it absolutely allows session hijacking where, because of the fact that cookies are what's used to maintain state as we move from page to page on a site, anybody else returning my cookie will be believed to be me.

So you can easily see a scenario where, for example, if Amazon were to have a cross-site scripting flaw, it would be possible for third parties to capture Amazon user cookies on the fly while they were logged in, immediately open a session using their cookie, thus completely impersonating them to Amazon, and then buy a whole bunch of stuff using their credit card because that's all stored by Amazon and you're never required to enter that again, and then add a mailing address other than where you want, you know, other than your default or any that you've used in the past, and basically buy anything they want and have it sent to them, and the user would know nothing about it until their credit card bill comes at the end of the month and they go, wait a minute, I didn't spend $5,000 on Amazon.com. But by that time the damage is done and the goods have been shipped.

And so this is the power of this kind of exploit. Now, it's true that the only credentials which will leak through this are those of the site which has the problem. So, for example, as far as we know, and certainly in March, Amazon.com had no trouble, nor did eBay. But they have – eBay has notoriously historically had cross-site scripting problems and was abused like this. So what happens is you definitely need to hope that your bank doesn't have cross-site scripting vulnerabilities because this is the kind of exploit that would really concern people who were doing electronic banking. And of course the double whammy is you typically have to have scripting enabled in your browser in order to use the banking site.

So the beauty of all of this is, if you had no scripting in your browser, your browser would ignore that start script/end script tag. It would skip right over it, and you'd see something missing on the page, but there's no vulnerability. The vulnerability comes from the client browser which is being tricked because of this leakage of unintended text from a trusted website like Amazon or eBay or your favorite blogging site or whatever you're using, where a hacker has been able to inject their own text into that flow. When that happens, you can get into trouble.

And so this is not a problem like, well, for example, like three days ago we had the huge problem with Windows animated cursor exploit that was going to be immediately exploited and was immediately exploited essentially worldwide. Instead, these kinds of vulnerabilities, because they are specific to applications, you know, specific vulnerabilities in specific applications, they tend to be more targeted attacks. That is, it doesn't make sense to try to send everybody a link to a known problematic blog and have them go there because they may never have been there before, they haven't established an identity, they don't have any log-on credentials to be stolen, so that doesn't make any sense.

But you can merge these with social engineering attacks. For example, knowing that a site is vulnerable and wanting to be up to some mischief, you could, for example, if it was a blogging site or an online forum site, you could start chatting with people, find out a little bit about who they are, and then send them a link saying, hey, you know, check this out. And when they click on the link, essentially that goes to one of the forum pages where there's a known scripting vulnerability that will cause their browser to divulge their credentials to this third party, which allows them to then log on as that first-party user and essentially pretend to be them on the blogging site and cause all kinds of mischief.

Leo: That's an interesting combination of social engineering and hacking. Which more and more that's what you're seeing. I mean, that's – you want to get the job done, that's how to do it.

Steve: Well, exactly. And so for the targeted kinds of attacks, and for example I think we mentioned a couple weeks ago when we were talking about China deliberately attacking the Defense Department, those are targeted attacks where they will take known cross-site scripting vulnerabilities. And remember that one of the real gotchas with this is it is a firewall-penetrating attack, meaning that if somebody from outside, for example outside the United States – I don't mean to pick on China by any means, but that does seem to be where the bandwidth of these attacks is emanating largely...

Leo: Important, by the way, you point out the bandwidth but not necessarily the attackers, since they can spoof any location, obviously.

Steve: Exactly. Or bounce through proxies in China and actually be located anywhere else.

Leo: It may just mean that's where the most unprotected machines are. We don't know what it means really.

Steve: Well, and historically when we look at the demographics of the machines that have been infected by worms, China has been a large infection target, meaning that, if nothing else, their Windows machines were not being kept currently patched. So whether they were legitimate or not is impossible to guess. But so an email from, like, scattered across the Defense Department, containing a URL to an Intranet server inside of the security perimeter of the Defense Department, would then have preferred access to whatever was going on. And even there, by allowing the browser to trust the Intranet server, the cross-site scripting vulnerability is able to use those enhanced power credentials in order to get up to much more mischief internally and essentially establish a stronghold inside of the external security perimeter.

So these are real problems. They're not like, oh my god, the sky is falling, Windows has a zero-day exploit scale problem. But in terms of how they affect individual users, everybody who is using a certain vulnerable blogging site or people who are being socially engineered where there's someone trying to get you and these sorts of problems, if they find out what sites you visit and then cross-reference that versus known vulnerabilities, they have a way of targeting people. And it's also worth mentioning that you notice that we were seeing, okay, those 28 problems I read just from last month and didn't go back any further, I mean, this is always happening. So one of the problems is that many sites that will be using these web packages are not updating them at the same rate or level of frequency, if ever, that Microsoft is updating Windows. So the other thing that is helping Windows is that we are all now slaved to this second Tuesday of the month, if not sooner...

Leo: Or first Tuesday if it needs to be.

Steve: Yes, exactly, update paradigm. Whereas many of these shopping cart and blogging and Web 2.0 tools, they install them, they get them running, and then the developer's contract runs out or he's off to do something else; they're not being maintained at the same level that Windows is. So many sites that will talk about diversions of their PHP whatever it is they're running, the hackers look at that, and they go, okay, cool, we can hack this anytime we want. And they just sort of leave it there. These problems tend not to get found because they're not huge world-shaking problems. They're little, specific, sort of like vertical problems that can be exploited whenever a hacker has an opportunity or for whatever reason needs to. But they exist all over the Internet right now.

Leo: Well, I was going to say it's a PHP problem, but then you have some Perl scripts in there, too, which run out of cgi-bin. So it's not purely that it's running on a – it's just, you know, a lot of programmers are not used to looking at the inputs and making sure that it's valid and protected.

Steve: And again, Leo, as I've said before, as a developer myself, the psychology of the developer is, oh, can I just get this thing working? I just want to be done with this. I want to get this working because my boss is breathing down my neck, and I'm already three weeks late. And so there isn't that awareness. And again, as a developer, I really respect how clever many of these hacks are. For example, there are filters which will attempt to look for [script]. I mean, that's the most obvious thing you would filter out. But it turns out that there are very clever ways to obscure even that token. You can use all kinds of weird Unicode escape. You can even use – there's even some ways of using some permissible script to expand to non-permissible scripting. I mean, so again, the hackers are sitting here pounding on this, trying to figure out how they can break in. Whereas the developers are just happy that the thing seems to work and not crash the server anymore. So it's two very different mindsets with radically different goals. And the big problem is that the people who are developing these are not security experts. They're generally, I mean, I talk to people all the time who are barely coders. They go, well, you know, I learned PHP in order to implement my own blog.

Leo: Well, that's how PHP was written. It was a Personal Home Page program designed to do exactly that, to enhance a blog.

Steve: And it's an easy-to-learn language, so it's made for amateurs. So almost by definition, amateurs are not going to know about this, about all the problems that they're opening themselves and, more importantly, their users of their insecure sites to, due to the nature of this kind of problem.

Leo: Well, I'm glad that we can clarify this. And I hope that anybody who's thinking about doing some programming will think about validating user input. Because clearly that's where the problem lies.

Steve: Yes, that is the nature of it. I've got three really good links on our show notes for this week – a couple white papers that talk about this in more detail, show code samples so people can actually see how this works in real life, and the third link is to a really nice consortium. I think they're about, boy, I don't know, 80-some members. It's OWASP, the Open Web Application Security Project. This is an organization clearly formed because of the recognition of this kind of real pervasive problem. There's a bunch of utilities there. They've got some scanners and some tools and guidelines. And so if we do have – I'm sure we do have, I know we have, in fact, because I know some of them, they've written to me – web designers who are listening to Security Now!, and this episode has really caught your attention, I highly recommend – it's the third link on the Security Now! notes for this Episode 86, or just put in OWASP into Google and you'll get there. And they've got a whole bunch of great resources.

Leo: Excellent. GRC.com. That's the place to go. As long as I'm pointing you to places to go, I might remind you that this podcast is sponsored by our good friends at Astaro, the ultimate security folks. They really are good. The Astaro Security Gateway is used by many businesses to protect themselves. And now Version 7 just came out, and it has so many nice new features. The usual, of course, antivirus, antispyware, content filtering, IM and P2P control, network firewall, remote access and VPN, intrusion protection. But they've now

added encryption and decryption at the server side so that no additional software is required by your users. There you have now secure remote access via SSL VPN, the easiest to implement. And of course they scale very well. You can cluster up to ten different Astaro Security Gateways together, eliminating the need to install additional load balancing. It's patent-pending technology, actually. It increases the speed and reliability of your network. As your network grows, so does Astaro. Don't forget you can get a free trial by calling 877-4AS-TARO in your business.

And if you're a home non-commercial user, those home licenses now have been extended in the v7 package. You get everything, the base license plus all subscriptions and Astaro Up2Date. That used to be 79 euros per year. Now it's free for up to ten IPs, ten users, and a thousand current connections. So Astaro Security Gateway for the home user is an incredible deal. If you've got an old PC lying around, highly recommended. Astaro.com. We thank them so much for their support.

So we've wrapped another sucker up here. And well done, I must say, Steve. I am fascinated by the subject. Are we done with cross-server-side scripting, or is there going to be...

Steve: Well, we're done with this. But next week I want to talk about another equally troublesome remote injection. This is not the same sort, though. This is called SQL Injection, or Sequel Injection.

Leo: Oh, yeah.

Steve: A big problem.

Leo: I've been subject to that myself. A lot of forums had problems with SQL injections. Okay. That'll be next week on Security Now!. For transcripts of this edition and 16KB versions for the bandwidth-impaired, go to Steve's site, GRC.com. That's where you'll find his show notes, those links he mentioned, and of course his great program, SpinRite, which is really the disk maintenance and recovery utility. Just ask the Nerds On Site. They know. SpinRite.info for testimonials or GRC.com to buy yourself a copy. Steve, we'll wrap this thing up.