



- [Home](#)
- [News](#)
- [Products](#)
- [Blogs](#)
- [Buyers Guide](#)
- [Whitepapers](#)
- [Job Search](#)
- [Events](#)
- [Subscribe](#)
- [Issue Archive](#)

Topic Center: [Email Security](#) [Compliance](#) [Patch Management](#) [Financial Services](#) [Health Care](#) [Retail](#) [RSS](#) | [Login](#) | [Register](#)

SPONSOR:

Alcatel-Lucent Alcatel-Lucent delivers always-on, user-centric security solutions that meet the needs of today's dynamic enterprises.

[Home](#) > [News](#) > [Features](#) > Friendly fire

FEATURES

Friendly fire

[Dan Kaplan](#) September 01, 2008

PRINT EMAIL REPRINT FONT SIZE: [A](#) | [A](#) | [A](#) BOOKMARK



Sam Peterson

Protecting users from internet-borne threats falls on trusted websites, says Overstock's Sam Peterson. Dan Kaplan reports.

When hobbyist Dan Thompson created a website in 2000 for music fans to discuss and trade lyrics of one-hit wonders – think “Come on Eileen” or “Ice, Ice Baby” – he never thought the site would become a cyber target.

But that's just what happened last month, when hackers launched injection attacks against the vulnerable site by inserting a simple, customized script into the URL string. This query manipulated the contents of the Structured Query Language (SQL) Server database – common on most dynamic websites – causing the comment sections below message board threads to disappear.

Luckily (and perhaps stupidly), the vandals failed to initiate their script tags, meaning the 5,000 daily visitors to Thompson's site were not silently redirected to a rogue China-based website that was included in the script. Had they been, there is a strong chance the machines of unpatched users would have been infected with a trojan.

“I wrote [the site] eight years ago when I was first learning programming,” he says. “People like it. It's kind of organically grown because of the users. I've never really checked it for vulnerabilities. I guess now I need to start working on it.”

It was a wake-up call for Thompson, who lives in Kansas City and works full-time as a systems analyst.

“I'm sure there's some amount of responsibility for me to give people a site that's not going to turn their computer into a zombie,” he says.

Thompson is far from alone in his predicament. Since last fall, when attackers began using tools to automatically search for and then compromise vulnerable websites, hundreds of thousands of pages – almost all of them as innocuous and legitimate as Thompson's website, [onehitwondercentral.com](#) – have been silently overtaken.

This is causing some of the largest websites to take action. Retail bellwether [Overstock.com](#), home to some one million unique visitors a day, is well aware that the internet is today's preferred attack surface.

Just last year, Overstock rebuilt its entire site in Java, partially out of security fears.

Most Popular	Most Emailed	Most Recent
<ul style="list-style-type: none"> ■ Palin's personal email account hacked, contents leaked ■ Hackers prevent research on malicious code ■ Hacker answered personal questions to steal Palin password ■ McAfee to purchase Secure Computing for \$465 million ■ Cybercrime bill passes House, awaits Bush signature ■ Google Docs flaw could allow others to see personal files ■ Report: 60 percent of businesses hit by cybercrime ■ BusinessWeek website compromised ■ Brad Pitt, Beyonce, most exploited stars in cyberspace ■ Apple fixes another DNS vulnerability 		

"The security concerns were the fact that it was more of the unknown [with the old site]," says Sam Peterson, 32, senior vice president of technology at Overstock and the company's first-ever software developer. "If we're changing something here, what else are we changing? What [other vulnerabilities] could I be introducing?"

Salt Lake City-based Overstock has made it a point to only hire senior software engineers, he says. The belief is that these 60 men and women have been in the business long enough to appreciate not only novel application features and quick turnaround times, but also the value of security.

"We now have a team dedicated to security," Peterson says. They are responsible for testing code before and during the production process and running regular tests once it has gone live.

"Since we know the code base and have access to the servers, we can run a much deeper scan than someone externally," he says. "The bar is even higher for us. We're making sure security is above and beyond what it needs to be. If your application is secured, no matter what they throw at you, you're not going to have a problem."

Increase in infected sites

Still, most websites seem slow to respond at best, or caught completely off-guard at worst.

According to San Diego-based Websense's "State of Internet Security," a report released in July, 75 percent of today's websites containing malicious code are legitimate sites. That marks a 50 percent increase over the previous six-month period.

Among the trusted web destinations that have been hit are MSNBC, Wired, the United Nations, the Association of Tennis Professionals and Sony PlayStation.

Websense says 60 percent of the 100 most heavily trafficked websites have fallen victim to similar malicious activity.

Jeremiah Grossman (*right*), founder and chief technology officer of Santa Clara, Calif.-based WhiteHat Security, which estimates that nine out of 10 websites contain a serious vulnerability, says URL filtering and corporate proxy servers dramatically have improved. This has forced cybercrooks to refine their strategies.



"The bad guys used to try to get you to come to their website," Grossman says. "Instead of putting their malware on an untrusted site, now they put them on a trusted site – the sites you can't block."

And how have cybercriminals been able to so easily overtake these highly visited sites? Grossman says insecure coding is almost entirely to blame.

"Most of them are riddled with vulnerabilities because those who coded them didn't know of particular issues, didn't care, or weren't educated in such things," he says.

Caleb Sima, chief technologist of application security for Palo Alto, Calif.-based Hewlett-Packard, says there is no patch for individuals wanting to protect their websites against common exploits, such as SQL injection and cross-site scripting. Instead, they must ensure their applications are designed in such a way that they recognize legitimate requests from the not-so-nice ones.

This is known as input validation, Sima says. Following this procedure would eliminate about 80 percent of vulnerabilities, he estimates. Attackers would still be able to inject SQL into a database, for example, but their commands would go unheeded.

"From a web development perspective, I tell people there's only one thing they need to do," he says. "Make that the number one priority."

Featured White Papers

[Database Auditing Tools and Strategies](#)

Learn about a new set of software tools that provide low overhead audit collection with storage, alerting and reporting...

[View Now](#)

[Effective Web Policies- Ensuring Staff Productivity and Legal Compliance](#)

Employees increasingly expect to use the internet at work for their own personal use in return for longer hours, working...

[View Now](#)

[Safeguarding Data Loss](#)

When large companies and organizations perform inventory control of their electronic devices, managers often end up...

[View Now](#)

[Appliance Update Management](#)

Appliances are complex combinations of hardware and software that enterprises put into production environments to meet...

[View Now](#)

[Malware Security: Taking the Botnet Threat Seriously](#)

How does malware continue to infiltrate networks? Primarily because traditional defenses only address the threat in...

[View Now](#)

[View More Research](#)

Popular Tags

[Access Control](#) [Analyst Reports & Industry Surveys](#) [Anti Spam](#) [Anti Spyware](#) [Anti Virus](#) [Apple Threats](#) [Authentication Breaches & Exposures](#) [Consumer Threats](#) [Email Security](#) [Emerging Threats](#) [Finance](#) [Government](#) [Healthcare](#) [Lawbreakers & Cybercrime](#) [Microsoft](#) [Non-Microsoft](#) [Patches](#) [Patch Management](#) [Phishing](#) [Privacy](#) [Regulation](#) [Security Management](#) [Security Policies](#) [Spam](#)

If done properly, input validation could prevent hackers from being able to add a few extra characters to a URL string or web form, which could allow them to extract database assets or insert IFRAME tags – HTML code inserted into a legitimate web page – to secretly reroute victims to malicious sites.

Traditional network defense solutions do not work when it comes to the web, Grossman adds.

“You can’t firewall off a website, so firewalls aren’t going to do anything good, and all the exploits are going to be unique because all the websites have custom code,” he says. “Standard intrusion detection signatures won’t catch these types of attacks.”

Many sites are forced to go offline as a result of attacks. As a short-term fix, Grossman suggests trying to fix the broken code. But if that fails, companies should consider investing in a web application firewall.

“You just can’t go magically back and fix every line of code that has a problem with it,” he says. “It would just take too much time.”

Cross-site scripting, or XSS – which involves malware writers running malicious scripts in an unknowing victim’s web browser to steal cookies or to launch a phishing attack – is the most common web vulnerability. XSS are attacks on the client, with a trusted website unintentionally acting as a conduit.

SQL injections, on the other hand, involve attacks on the server to gain access to the database. They are far and away the most exploited web vulnerability. If XSS flaws made news in 2007, then SQL injections clearly have the lockdown on 2008.

According to a July report from ScanSafe, a San Mateo, Calif.-based web security firm, SQL injection attacks have spiked 212 percent from January to June of this year. In June alone, SQL injection made up 76 percent of all compromised sites. For years, these attacks have been used to extract database contents – some of the biggest reported identity theft heists have been caused by SQL injection – but most recently they have been leveraged to insert malicious content into websites, with the hope of infecting users’ machines.

Modifying databases

Mary Landesman, senior security researcher at ScanSafe, says that since about October, attackers have leveraged publicly available tools to search Google for websites vulnerable to SQL injection and then launched attacks. Since then, estimates place the number of compromised pages at upward of two million.

These vulnerabilities commonly lie in sites that use Microsoft’s ASP (Active Server Pages) to display information stored in the SQL Server database, she says. Because attackers are able to modify the database, they are able to modify what appears on the web pages.

“The coding choices that the developer makes dictate how that SQL Server is going to handle queries,” Landesman says. “If they haven’t given context to the queries that the database is going to receive, the database could act on the query as if it’s a command.”

In most cases, the attackers place JavaScript code into the database, which creates an IFRAME to silently call in the actual malicious payload from another site, WhiteHat’s Grossman says. Machines that are vulnerable to a particular flaw, usually a browser vulnerability, can be infected with malware, such as a password-stealing trojan or botnet-building backdoor.

Web security experts stress that attackers also have dozens of other ways to infiltrate an internet site. For example, websites need to protect stolen File Transfer Protocol (FTP) credentials, which if exposed through a phishing attack or through some password-stealing trojan, could be used by an attacker to make changes to website files. In February, web security firm Finjan said it uncovered an illegal database containing more than 8,700 stolen FTP server credentials.

“You basically own their website,” Landesman says. “You can make any modification you want.



The last comments for [Record number of active viruses measured - SC Magazine US](#)

JASON

When the college kids are out of school there will always be a increase in the number of new viruses.....

» 21 hours ago

[Jump to →](#)

The last comments for [Protection program defeats keyloggers - SC Magazine US](#)

JASON

I am gonna look more into this application sounds cool for admins.

» 21 hours ago

[Jump to →](#)

The last comments for [Weaponization trumps skill](#)

Christopher Cashell

This is a wonderful article. I'd love to see more like this. Any chance of Mr. Little doing a...

» 21 hours ago

[Jump to →](#)

The last comments for [QuickTime exploit disclosed for 1-week-old version - SC Magazine US](#)

JASON

I wonder why a apple pr person was na?

» 3 days ago

[Jump to →](#)

The last comments for [Hacker answered personal questions to steal Palin password - SC Magazine US](#)

JASON

Companies should allow custom security questions!!

» 3 days ago

[Jump to →](#)

Comments by [Intense Debate](#)

The attacker can even change security settings to allow future attacks to take place.”

She also warned about sites using third-party offerings, such as a web server (open-source Apache is hugely popular) or blog software, to ensure those programs are updated with the latest patches and deployed with security settings turned on.

Other threats

Meanwhile, Grossman – who says he successfully predicted a few years ago the rise of SQL and XSS attacks – thinks another major wave of web-based ambushes are on the way.

Business logic flaws, as they are known, include insufficient authentication and information leakage. They are simple glitches that have the ability to financially cripple a company, Grossman says. Yet, unlike poorly written code, these design flaws cannot be scanned for.

One prominent example: a North Carolina woman was found guilty of wire fraud last October after discovering a way to order items on QVC.com, cancel them without being charged, yet still have the merchandise delivered. She then sold the items on eBay, profiting more than \$400,000.

“They are very easy to exploit and very hard to see,” says Grossman, who presented on the topic last month at the Black Hat conference in Las Vegas.

Of course, when discussing website security, it would be a vast oversight not to mention phishing – the age-old scheme in which cybercrooks trick users into giving up their personal information.



Phishing attacks are more sophisticated than ever, says Avivah Litan (*left*), vice president and distinguished analyst at Stamford, Conn.-based Gartner. A December study of 4,500 U.S. adults shows a 118 percent rise in the number of phishing emails received over the past three years (3.3 percent of respondents lost money as a result).

The seriousness of the phishing threat was underscored in July when researchers at Indiana University reported that of some 2.5 million pages they examined, 128,000 contained open redirects.

This meant phishers could add some quick code to a web address and redirect users to the website of their choice.

“The query string part of the URL allows you to provide parameters of where you want things to go,” says Craig Shue, a Ph.D. student and one of the lead researchers.

To the victim, he says, the URL for the phishing site would appear just like the legitimate domain name, just with some added characters that allowed the page to redirect somewhere else.

“It’s really just routing through the legitimate site to the bad site,” Shue says. “It’s taking advantage of the user’s familiarity with the brand and using it against them.”

As was the case with SQL or XSS, poor coding by developers is to blame, he says.

As a way to combat phishing, the CA/Browser Forum, a group of certification authorities and web browser software manufacturers, created an extended-validation SSL certificate, first released last year. The new certificates are different than their predecessors because they are represented by a green shade in the address bar, while the name of the site and its company location are displayed on the browser chrome, says Tim Callan, vice president of SSL marketing at VeriSign. So far, roughly 6,000 companies – which were vetted by a certificate provider – have deployed the new technology.

The goal is to increase consumer confidence by making website visitors more informed and more aware of what to look for in a trusted site – in this case, green, Callan says.

“The name of the site appears on the chrome of the browser,” he says. “It can’t be changed or

manipulated. A person who runs a false site can make their HTML look like Bank of America. What they can't do is put Bank of America in the green spot in the chrome of the browser to the right of the address bar in Internet Explorer 7." (In Firefox 3, the chrome appears to the right of the address bar).

But Litan questions the effectiveness of such seals of approval. "It will tell you if a company is registered with a legal authority, but that doesn't mean they're not a crook," she says.

Additional measures

Others have questioned whether users are smart enough to know to look – and where to look – for visual cues, such as a green address bar in the browser chrome. Still others think the problem is a fundamental one: If credentials, such as Social Security numbers, were not so valuable to criminals, why would anyone go after them?

Websites must take additional measures to stop phishing, Litan says. Gartner advises its clients to implement strong authentication; engage anti-phishing and brand monitoring services, such as those from RSA, MarkMonitor or Cyveillance; and protect accounts with fraud detection and transaction verification.

Peterson says Overstock – one of the first companies to deploy extended-validation certificates through VeriSign – does not tolerate phishing and relies on its partners to help wage the battle. "We want them to know we're going to come after them legally," he says. "We have a team of lawyers. That's all they want to do is shut these guys down."

But Peterson also understands that his \$1 billion-a-year company's obligation to protect against malicious code writers and phishing schemers extends well beyond its own borders. By taking action, Overstock is making a commitment to internet commerce as a whole.

"If the major guys can't fend off the bad guys, then no one is going to have trust in the internet," he says. "It's up to us, up to Amazon, up to eBay to make sure we have the top security."

[sidebars]

SQL INJECTION: The going rate

Gunter Ollmann, chief security strategist for Armonk, N.Y.-based IBM Internet Security Systems, says a well-oiled underground market has emerged to supply attackers of all skill levels (and wallets) with the three-step means to perpetrate the exploits.

\$40 to \$50: A toolkit that uses search engines to discover websites vulnerable to SQL injection, then tries the injection. The best toolkits can deface up to 1,500 websites per minute.

\$80 to \$100: An IFRAME hosting site. IFRAMES are the tags embedded on compromised sites which silently redirect victims to malicious sites.

\$100 to \$400: Malware generation kits that attempt to exploit a vulnerability on a victim's computer. The flaw is typically a browser bug. – *Dan Kaplan*

TO DO: A checklist for security

- Scan site regularly for common attacks.
- Audit web logs for suspicious activity.
- Harden the web server and monitor for changes in security settings.
- Investigate third-party apps before deployment.
- Filter user input for anomalies.
- Deploy free scanning tools from Microsoft and HP.
- Consult resources, such as the OWASP Top 10 list.
- Enter your site into free tools, such as Scandoo, to check for compromise.
- Provide an email address for users to notify you of live attacks.

Source: ScanSafe

From the September 2008 Issue of SCMagazine

Tags: [Vulnerabilities & Flaws](#) [Browser Flaws](#)

Ads by Google

[Vista Wallpaper](#)

Windows Vista offers great features for small businesses. Learn more.
www.Microsoft.com/Windows

[Best Desktop Computers](#)

Get the answer to your problems for free with the PC community.
www.pc.com

[HP m8100y Media Center PC](#)

Shop High-Performance Media Center PCs & More at the HP Official Store
www.hpshopping.com

Comments

 Login  Follow this discussion ▾

There are no comments posted yet. [Be the first one!](#)

Post a new comment

Enter text right here!

Name *

Email (track replies)

Blog URL

 Sign up for IntenseDebate [Why?](#) | [Login](#)

Or post using OpenID

Comments by [intense debate](#)

[Get better comments](#)

SPONSORED LINKS

Find the zombies and malware hiding on your network.

Domain Health Check™ is a free service that provides actionable information about your company's mail and Web traffic. This information is provided by Secure Computing TrustedSource™, a global reputation system that tracks messaging and Web activity for every domain on the Internet. Find the zombies and malware hiding on your network. [View Sample Report](#)

Alternative Thinking about Application Security:

Alternative thinking is harnessing the security power of HP Software to identify threats to your system and risks to your business. [Learn more at hp.com/go/securitysoftware](http://hp.com/go/securitysoftware)

WatchGuard delivers network security solutions to businesses worldwide.

Our award-winning products and services enable customers to securely conduct business. WatchGuard integrated security products allow customers to choose the best security solutions to fit their needs.

RedSeal Systems First to Automate PCI-DSS Assessment

The scale and complexity of today's networks makes it essentially impossible for a manual review of firewall rules and policies to be accurate. RedSeal SRM for PCI automatically conducts a network-wide analysis of your router and firewall configurations and policies. [Request a demo/download the datasheet.](#)

SC World Congress, December 9-10, 2008, New York City

Located in New York City the SC World Congress is the only dedicated IT security event in this extremely important location focused on providing the latest solutions and inside information to help IT & Data security professionals do their jobs better. Within a 300 mile radius of New York City is the largest concentration of corporate headquarters and federal / local government offices in the US. Where the need for the latest technologies and solutions to protect valuable data is at its highest and where the budgets supporting information security are the largest. www.scworldcongress.com

BigFix – Speed, Automation, Consolidation. You've got to put "BigFix" on your list.

SC MAGAZINE US SITEMAP

News

Latest News
Latest Features
Latest Opinions
Latest Company News

Products

Latest Products
Latest First Looks
Latest Reviews
Latest Group Tests

Blogs

The News Team Blog
The Data Breach Blog

Media

Podcasts
Editorial Webcasts
Vendor Webcasts

Whitepapers

Latest Whitepapers

Buyers Guide

Browse our Buyers Guide


Jobs

IT Security Jobs

Events

Awards

More

Newsletters
Subscribe
Contact Us
Advertising
Editorial
 RSS

Topics

Anti Spam
Anti Spyware
Anti Virus
Apple
Browser Flaws
Consumer Threats
Data Loss Prevention
Emerging Threats
Insider Threats
Lawbreakers & Cybercrime
Microsoft
Non Microsoft Patches
Patch Tuesday
Security Policies
Spam Techniques
Trojans
Phishing
Vulnerabilities & Flaws

Sectors

Email Security
Mobile Endpoint Security
Patch Management
IT Security Training
Compliance

Verticals

Finance
Government
Healthcare
Retail

Events

Awards

Media

Podcasts
Editorial Webcasts
Vendor Webcasts

This material may not be published, broadcast, rewritten or redistributed in any form without prior authorization.
Your use of this website constitutes acceptance of Haymarket Media's Privacy Policy and Terms & Conditions