

# Things you should know about Web 2.0 security

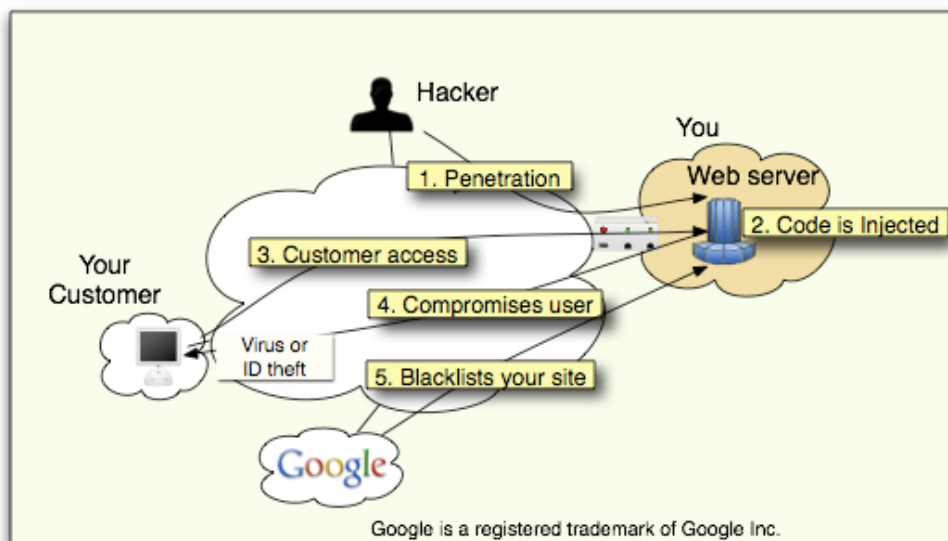
Don't let web-security stand in the way of your business

## BREAKING NEWS

**Why antivirus software and firewalls are not enough.**

**The Code Injection attack and how it can kill an e-business.**

**75% of bank web-sites have basic security flaws, and more ...**



### How Code Injection works?

**Step 1:** The hacker breaks into your system through vulnerabilities in your web site.

**Step 2:** The hacker injects malicious code into your website.

**Step 3:** Your customer visits your website trusting your reputation.

**Step 4:** The injected code in your site compromises his machine: a virus is downloaded and his machine turns into a bot (the hacker controls his computer).

**Step 5:** Search Engines visit and blacklist your website as malicious.

Web security is an arms race between good and evil. If a service is networked and interactive, it is most likely not 100% secure. It can be only made less vulnerable. Proof: Security giant Symantec and Kaspersky's websites were cracked by hackers in 2009. If security companies can't keep their website safe, who can claim they are secure?

**1. Why antivirus software and a firewall are not enough.** Unless you are willing to give up on Web 2.0 functionality, web-site owners need to go beyond antivirus software and firewalls. There are ever evolving vulnerabilities and mechanisms for gaining access to a website. A major factor is vulnerabilities through one's website. In addition there is the human factor; the careless employee who visits a malicious website, fails to protect their password, or brings an infected laptop inside the firewall. As a result, expecting you will never be broken into is like hoping that your home will never be burglarized.

**2. The Code Injection attack and how it can kill an e-business.** Code injection (see Figure and explanation) turns your website into a beacon of malware dissemination without your knowledge. Its typical goals are to: (a) disseminate viruses and compromise your customers' computer, and (b) perform identity theft on your customer. The problem is real: BusinessWeek was hacked (Nov 2008), 70,000 pages were hacked in June 2008.

*Code Injection can ruin an e-business:* Once blacklisted by the major search engines, the reputation of one's website plummets (reportedly from top 10 to bottom 10,000). In addition, currently there are no good tools to help you recover from a code injection. The stopbadware.org is filled with people unable to get off the blacklists.

CONT.

**I BET YOU DIDN'T KNOW:**

**a. Viruses started to masquerade as anti-virus software to fool people into downloading them.**

**b. Cyber-crime as a Service: (CaaS):** Providing a rogue spam campaign or launching a DoS to a target of choice has its own market:

“Malware writers that sell toolkits online for as little as \$400 will now configure and host the attacks as a service for another \$50, a security expert has said.” ITNews 3/2009.

*What can you do:* (a) *Prevent:* stress test the security of your site frequently, (b) *Detect:* monitor your site at least daily, and (c) *Recover:* be ready to react to a break in.

**3. Website vulnerabilities are rampant: 75% of bank web-sites have basic security flaws.** Major banks and prominent security companies fall victims to web-based intrusions. According to InformationWeek (7/2008): “Security risks caused by basic flaws in Web site design are widespread, according to computer scientists”. A U. of Michigan study found that more than three-quarters of bank websites have design flaws that could expose bank customers to financial loss or identity theft. In addition, an FDIC Technology Incident Report on suspicious activity at banks found 536 computer intrusion incidents with an average loss of \$30,000 and a total loss of \$16 million in the second quarter of 2007.

**4. The XSS vulnerability: how your website vulnerabilities can hurt your customers.** Using spam, XSS allows hackers to point careless users to your site and execute malicious code attached to the hyperlink the user clicks on. As of 2007, cross-site scripting carried out on websites were roughly 80% of all documented security vulnerabilities.

**5. Most web-user are “idiots”,** according to a research study. In fact, several studies quantify the carelessness of web-users, which include both one’s employees and one’s customers: users click before thinking, they don’t read warning messages, and they don’t update their software:

“Researchers find that, in their haste to get rid of annoying popup alerts, most users don’t bother to examine popups for the telltale signs of browser-based malware.” - *Ars Technica* 8/08.

“40% of surfers don’t bother with browser security updates” - *Ars Technica* 7/08.

This could partially explain why identity theft has reached 10 million victims until 2007. On average, each identify theft recovery costs \$1,500 and 175h per person for a total \$50 billion in 2007.

**6. The intertwined world of cyber-crime:** Interestingly, many malicious activities are interconnected and supportive of each other: viruses, bots, website intrusion, code injection, and spam are tightly related. For example, consider the following cycle of crime: (a) a hacker uses code injection to create a malicious website, (b) the hacker uses a botnet to launch a spamming campaign attracting users to a malicious website, (c) careless users visit the website, are compromised and turned into bots, (d) the newly created bots are used to do more spamming.

Security is a community concern and a weakest-link game. We all need to do our part.



**stopthehacker.com**

© Jaal LLC

Making the Internet safer  
one website at a time™

We are committed to fighting cyber-crime focusing on web-site security. We provide products and services to web-site owners for safeguarding the security and, consequently, the reputation of their site. The comprehensive services are critical for before, during and after an intrusion and include: (a) assessing the vulnerability of a customer's site, (b) monitoring the site to detect security breaches, such as code injection, and (c) facilitating the recovery of a compromised site, which is a surprisingly involved, tedious and time-consuming process.