The New Wild West

Presented by: WIU's Chief Technology Security Officer

It used to be that if you only surfed large well know websites and stayed away from certain categories of websites (such as adult websites) you could surf the web reasonably secure. However, the number of compromised websites hosting malicious code has skyrocketed in recent months. Based on some estimates 70% of the most popular websites have hosted malicious code (http://www.securecomputing.net.au/News/135019,websense-number-of-compromised-websites-at-alltime-high.aspx) resulting in an explosion in the number of drive-by downloads.

Drive-by downloads occur when malicious code is downloaded to your computer after visiting a compromised website. You don't necessarily have to click on anything on the site. Malicious code can be as simple as a hidden form field redirecting you to a known malicious website. It is more commonly malicious code (typically JavaScript) hidden in everything from advertisement banners to graphics, pictures or stored as user input in databases.

How are websites compromised?

Malware writers often create entire sites to infect users. In addition, websites with user generated content, typical of Web 2.0 sites, have created a huge opportunity for the introduction of malicious code into otherwise legitimate websites as user-submitted malware. This code is hidden from both end users and website operators.

Summarized below is a list of the top ten vulnerabilities found in web applications as defined by the Open Web Application Security Project (www.owasp.org) an industry think-tank providing application security thought leadership. Another valuable resource is the SANS Institute's Top 25 Most Dangerous Programming Errors list (http://www.sans.org/top25errors).

A1 - Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
A2 - Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3 - Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
A4 - Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5 - Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
A6 - Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.

A7 - Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
A8 - Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9 - Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
A10 - Failure to Restrict URL Access	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

Source: OWASP Top 10 List

Coming to a website near you

WIU has experienced three known cases of malicious code being hosted on personal or organizational websites at the University since the beginning of the Fall Semester. Couple that with approximately 8,200 active websites hosted on behalf of individuals or organizations at the University and you have an atmosphere that is conducive for the mass hosting of malicious code.

Protecting yourself

Haute Secure (hautesecure.com) provides Internet Explorer and Firefox toolbars that protect your web surfing in two ways. If a URL is on their suspicious or banned lists, Haute Secure intercepts possible threats before they happen  allowing you to decide what to do.

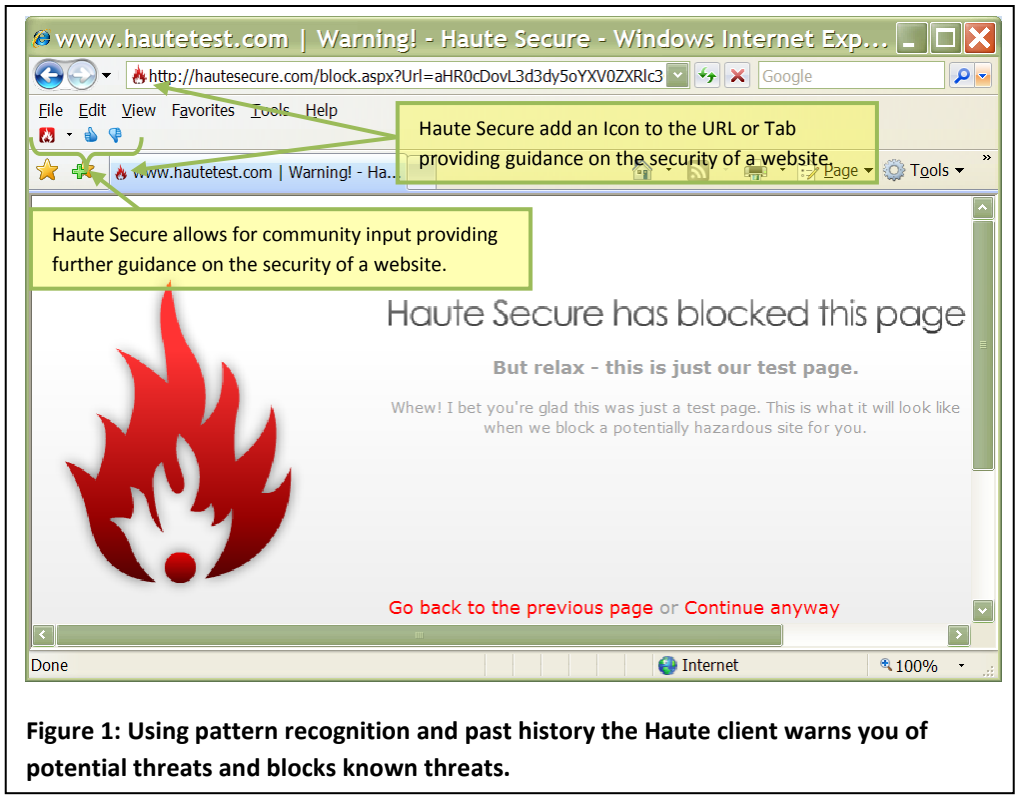
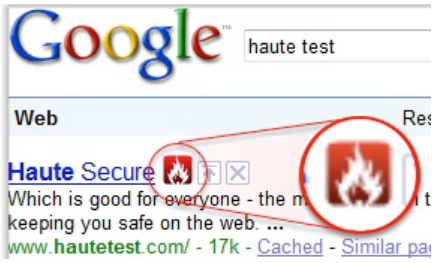


Figure 1: Using pattern recognition and past history the Haute client warns you of potential threats and blocks known threats.

Secondly, keeping in mind that most web surfing begins on a search engine. Haute secure allows you to find out more about possible threats before viewing with integrated search engine results.



Protecting your web site

Whether you are a faculty member managing your personal website or a student managing your clubs website there are things you can do to protect visitors to your website. The following is a sample of resources that will help you analyze your web site:

- http://unmaskparasites.com/security-report/
- http://www.google.com/safebrowsing/diagnostic?site=www.wiu.edu
- http://www.siteadvisor.com

Tools that you can use to help analyze your own website
(**INTENDED ONLY FOR MORE ADVANCED WEBSITE OWNERS**):

- Finding SQL Injection with SQL Injector and Crawler (Scrawlr) from HP Web Security Research Group https://download.spidynamics.com/products/scrawlr/

- The Microsoft Source Code Analyzer for SQL Injection tool is available to find SQL injection vulnerabilities in ASP code: http://support.microsoft.com/kb/954476

Contact the support center (309.298.2704 or SupportCenter@wiu.edu) or your college technology representative if you suspect your website has been compromised or is hosting malware.

As responsible website owners and concerned website surfers we need to do what we can to ensure the relative security of our piece of the World Wide Web. I strongly advocate learning from each other. If you know of additional resources to protect websites or website users drop me a note. I will update this article as appropriate.

Regards,

Michael Rodriguez
CTSO @ Western Illinois University
ma-rodriguez2@wiu.edu

"We only need to be lucky once. You need to be lucky every time." — The IRA to former British Prime Minister Margaret Thatcher