SANS SOFTWARE SECURITY with Frank Kim

Secure Coding.
Practical steps to defend your web apps.

Copyright SANS Institute

Author Retains Full Rights

This paper is from the SANS Software Security site. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Secure Coding: Developing Defensible Applications (DEV536)"
at http://software-security.sans.orghttp://software-security.sans.org/events/

Web Browser Insecurity

Introduction

There has been much debate lately between two different browsers, namely Microsoft's Internet Explorer and the Mozilla Project's Firefox web browser. Security is in the center of this debate, accompanied by features and usability. This article will focus on the security aspects, particularly the risks involved with running any web browser and how to overcome some of these security shortcomings. I will use Internet Explorer and Firefox as examples, as these are the most commonly used, and therefore the most commonly exploited. That's good news for all you Safari and Opera users. Congratulations to the Safari and Opera development teams, because according to Secunia you have zero unpatched vulnerabilities (See Opera Vulnerability Report http://secunia.com/product/1543/ and Safari Vulnerability Report http://secunia.com/product/761/).

I imagine that the browser debate going on today will continue throughout the year, and we may even be at a full-blown "Browser War" status in the near future. Regardless of the outcome, and regardless of who wins, the bottom line is that you will need to secure your web browser. This may not always translate into actual browser or operating system configuration, but may mean being aware of your web browsing behavior. There are certainly some good tips to securing your web browser that you can configure (I will cover some in this article), however I believe that you will find less malware (spyware, adware, and viruses) on your computer by changing your browsing habits and being more aware of your clicking. Almost all the browser exploits require that you click on something. Now lets come back to reality and realize that people are going to click stuff, children especially, that could trigger malicious software to run on your computer. So our strategy is two fold, maintain a secure environment and be an educated user. The goal of this article is to help you in both of these areas. First, I will show examples of the more common threats, then move on to the defensive measures. The weaknesses shown here are not the most critical, but they will help you to understand the basics of how web browser exploits work and how they are used in attacks.

Browser Weaknesses

Internet Explorer

Internet Explorer has had its share of problems. This year alone MS has already released numerous updates that fix various security problems. These are the vulnerabilities that have been recognized by Microsoft. Vulnerabilities that have not yet been fixed by Microsoft also exist and pose an even greater threat, because there is no patch for them, yet. I have chosen an example of an

© SANS Institute 2000 - 2005 Author retains full rights.

unpatched Internet Explorer vulnerability that I will explain in detail. The vulnerability deals with the status bar, which is the space in Internet Explorer (and all other browsers) in the lower left hand corner that displays, among other things, the destination of the hyperlink that you currently have your curser positioned over. Due to a bug in Internet Explorer it is possible to construct a link that will display one web site link in the status bar, but really take you to a different web site. I have posted an example of this at:

http://www.defensiveintuition.com/ieexploit.html

Going to this site presents you with a page that links to http://www.defensiveintuition.com. When you move your mouse over this link you will see "http://www.brown.edu" appear in the status bar. However, if you are using MS Internet Explorer, clicking this link takes you to a different site (in this example, and all others in this article, it should take you to http://www.google.com). Now try going to this website in Firefox and notice that you will be taken to the correct web site.

This vulnerability poses a threat because you may think that you are being taken to your bank's web site, but in reality you are going to a web site created by an attacker attempting to gather your personal information through a phishing attack. It is important to note that this vulnerability also exists in MS Outlook Express.

Mozilla Firefox

Firefox has gained popularity as a web browser very quickly. It is a trimmed down version of the Mozilla web browser. It does have some security advantages, however it does not include support for technologies such as MS ActiveX, which coincidentally has posed many security issues for Internet Explorer. Not all web sites/applications will work the Firefox, but most agree is works well for general web browsing. Of course, just as any software, Firefox has its share of security problems too. It contains a similar bug that you saw above with Internet Explorer, using a slightly different exploit. It too will allow a malicious user to "spoof" the real destination of a link in a web site. This time it only works when hovering over the link, right clicking, and choosing "Save Link As…". Using Firefox version 1.0.1 you can see the exploit in action at the following web site:

http://www.defensiveintuition.com/firefox_exploit.html

This exploit only works with Firefox version 1.0.1 and appears to have been fixed in later versions. When I tried it with 1.0.3 and 1.0.4 I could see the "hidden" link to "http://www.google.com" if I clicked and held the mouse button down on the link or right clicked and chose "Save Link As…". For fun, go to the link above using Internet Explorer and notice that it spoofs the status bar successfully. I

© SANS Institute 2000 - 2005 Author retains full rights.

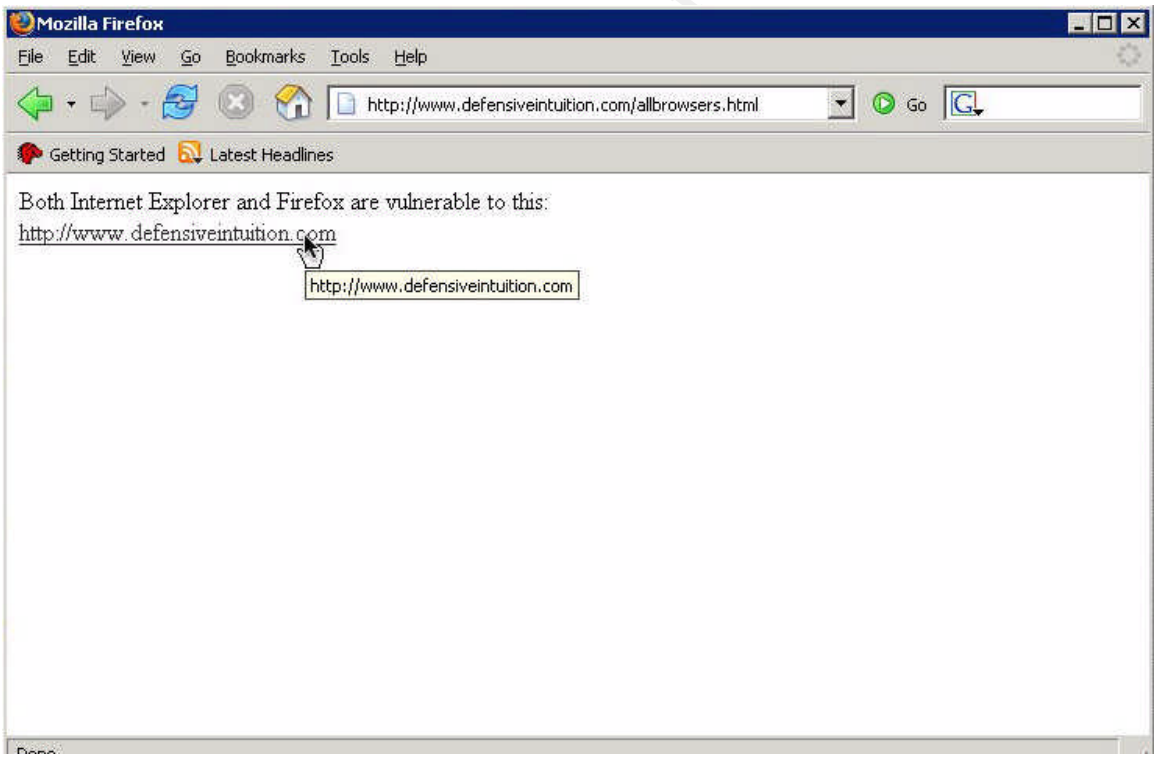
found it interesting that a vulnerability originally released for Firefox seems to work better in Internet Explorer. Even so, we still do not have an exploit that works well with both.

Universal Status Bar Spoofing?

The above examples use two different ways to implement the URL status bar spoofing in pure HTML. Using JavaScript we can construct an exploit that works equally well with the latest versions of Internet Explorer and Firefox. Remember, clicking the link in either example does not take you to http://www.defensiveintuition.com, but to http://www.google.com. Go to the following link to try it with your favorite web browser:

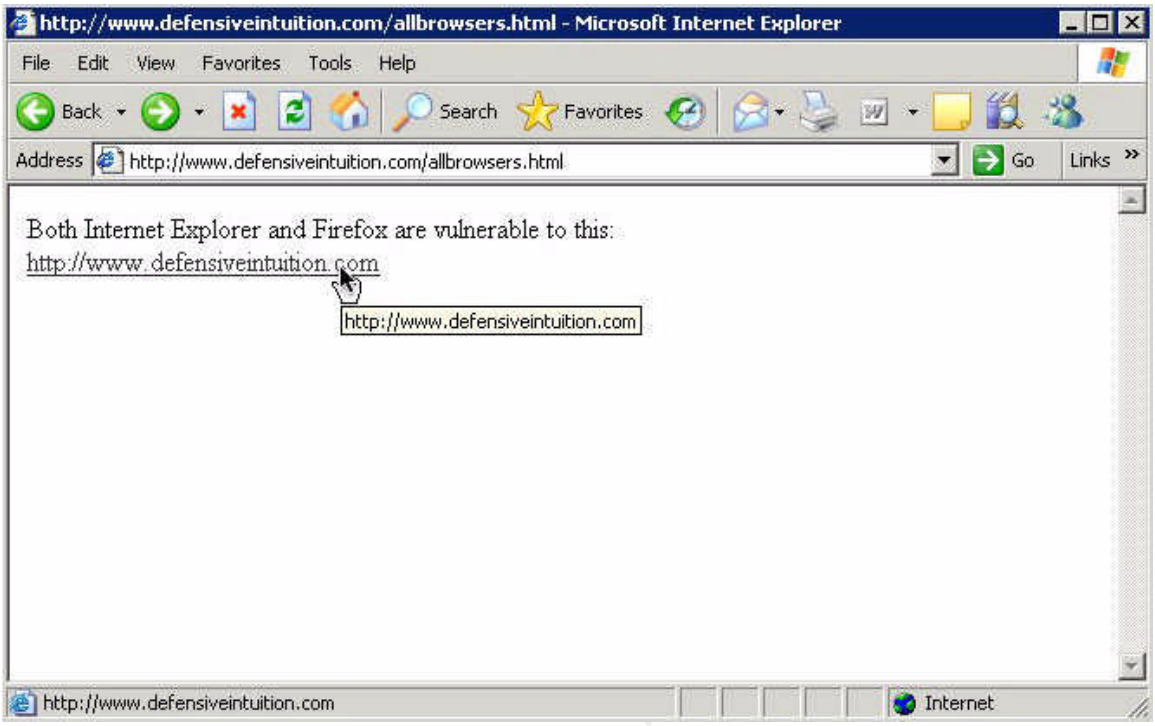
http://www.defensiveintuition.com/allbrowsers.html

The exploit in the above link works differently depending on which browser you are using. Below is an example of how it works in Firefox:



In Firefox it will display the spoofed site in the text bubble when you hover over the link. Firefox does not display the spoofed link the status bar because it will not allow the contents to be modified by JavaScript. Internet Explorer appears to be completely fooled, as shown below:

© SANS Institute 2000 - 2005 Author retains full rights.



Notice the spoofed site appears in both the text bubble and the status bar. An interesting note, visit this link with Opera 8.0 or Safari 1.3 and see that they are not fooled.

URL status bar spoofing is not as critical a vulnerability as some other web browser vulnerabilities. It allows an attacker to trick users into going to a web site to perform a phishing attack. However, it shows that browsers contain vulnerabilities that may go unpatched, and how the exploits for these vulnerabilities are morphed to maintain effectiveness. There are many other exploits for both browsers, some patched and some not. All software will contain vulnerabilities sooner or later; it is the responsiveness of the vendor/author of the software that matters. I use Firefox for general web browsing and only use Internet Explorer for sites that don't work in Firefox. Firefox seems to have less security problems. It is better at handling all those web-browsing annoyances, like pop-ups and banner ads. Regardless of your web browser choice you should implement the tips in the remainder of this article to help protect you from being vulnerable, whether they are patched vulnerabilities, unpatched vulnerabilities, or behavior-based vulnerabilities.

Keep Your System Updated

This is the most fundamental step to securing your computing environment. You should run windows update automatically and have it check for updates daily. Remember, be certain to reboot after you have run Windows updates. In Firefox you will need to look for an arrow-type icon in the upper right hand corner and click on it when it appears. This will guide you through installing the latest

© SANS Institute 2000 - 2005 Author retains full rights.

version of the web browser.

Configure Security In Your Web Browser

There are many steps you can take to tighten the security of your web browser. Some of these may cause web sites and applications not function. Disclaimer: Use these tips at your own risk:

- Disable JavaScript – This can be done in most browsers and will prevent certain attacks, such as the universal URL status bar spoofing.

- Disable Java – This falls in the same category as JavaScript.

- Use a pop-up blocker – Sometimes sites will use pop-ups to execute malicious code, plus they are pretty annoying.

- Don't cache your passwords or saved form information – Caching means that this information can be stored on your computer where other people could collect it.
-

Keep Your Browser In Check

A step often left out in the patching process is testing the system to see if the patches actually applied. This is difficult for the average user, as the best way to do this is to actually attempt to exploit the vulnerability after each patch. An easier way to test is to visit either of these two great web sites that will check your web browser software and configuration for vulnerabilities. You should visit them each time you apply a patch:

- http://bcheck.scanit.be/bcheck/

- http://browsercheck.qualys.com/index.php

Principal Of Least Privilege

Many users ignore this rule when setting up their personal PC. If it can be helped you should be logged in as a user that does not have administrative rights. Mac OS X is a good example of this model, when you need to do something that requires administrative privileges you are prompted for the administrative password. To translate this to Windows you should use the "Run As…" feature. The excuse I hear all the time by users for running as administrator is they need to install software. The solution is to download the software you wish to install, right click on the icon, choose "Run As…" from the menu, and enter the administrative credentials. It requires a little more extra effort than OS X, but will help prevent malicious web site from installing

© SANS Institute 2000 - 2005 Author retains full rights.

software without your knowledge on your computer. This tactic is especially useful for children.

Anti-Spyware

Every system should have at least one Anti-Spyware package installed. It should be run on a regular basis to remove unwanted spyware and adware. It is best to do this while running in Windows Safe Mode (While booting windows press the F8 key when the Windows XP splash screen appears), as Anti-Spyware software will be able to remove spyware more easily. Here are some of my favorite Anti-Spyware packages:

MS Anti-Spyware – This is still in beta at the time of this writing, but generally works really well. It constantly monitors your system for spyware, automatically updates its definitions, and even allows you to easily secure your web browser using its advanced features. This is, so far, a free product from Microsoft.

Ad-Aware – This is a commercial product that in generally well known and good at removing spyware.

Spybot – This is a free Anti-Spyware product that is also well known and good at removing Spyware.

HiJackThis - A very advanced spyware removal tool that gives you more control, but uses less discretion than the above tools.

Anti-Virus

No computer system should be without anti-virus software. It helps to protect your system against malware, and newer versions even detect spyware and adware. Here are two that I use with much success:

- Clamwin – This is a free anti-virus program that features auto-updating and a large support based. It was the February 2005 project of the month and seems to be gaining wider support.

- Symantec Anti-Virus – With each version this software package seems to get smarter. Newer versions contain more protection from spyware, adware, and browser injected malware than ever before. It features automatic updates and numerous other features.

Think before you click…

As I stated previously, you can prevent malware from being installed on your computer and phishers from getting your personal information be changing your habits. Here are some general guidelines to follow:

© SANS Institute 2000 - 2005 Author retains full rights.

- Do not follow links sent to you via email
- View email in plain text, not HTML
- Use a separate credit card for Internet purchases (with a low limit)
- If it sounds too good to be true, it probably is
- If you do your banking online, only do it from one computer you trust
- Open attachments only if you are expecting them
- Always type in the web site manually if you are going to enter personal information
- Never trust the status bar!

References

McGranaghan, Peter, SANS Reading Room, A Spyware Survival Toolkit March 15, 2005 http://www.sans.org/rr/whitepapers/threats/1625.php

Secunia Advisories, Secunia, Internet Explorer/Outlook Express Status Bar Spoofing February 17, 2005, http://secunia.com/advisories/14304/

Secunia Advisories, Secunia, Firefox "Save Link As..." Status Bar Spoofing Weakness, March 14, 2005, http://secunia.com/advisories/14565/

Author: Paul Asadoorian, GCIA, GCIH
Defensive Intuition (http://www.defensiveintuition.com)

Date: May 25, 2005

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS App Sec Training

SANS vLive - DEV544: Secure Coding in .NET: Developing Defensible Applications	**DEV544 - 201307,**	**Jul 15, 2013 - Aug 07, 2013**	**vLive**
Community SANS Halifax	**Halifax, NS**	**Jul 22, 2013 - Jul 27, 2013**	**Community SANS**
Network Security 2013	**Las Vegas, NV**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS vLive - DEV541: Secure Coding in Java/JEE: Developing Defensible Applications	**DEV541 - 201310,**	**Oct 08, 2013 - Oct 31, 2013**	**vLive**
Community SANS Paris @ HSC - DEV522	**Paris, France**	**Oct 14, 2013 - Oct 18, 2013**	**Community SANS**
SANS Dubai 2013	**Dubai, United Arab Emirates**	**Oct 26, 2013 - Nov 07, 2013**	**Live Event**
SANS South Florida 2013	**Fort Lauderdale, FL**	**Nov 04, 2013 - Nov 09, 2013**	**Live Event**
SANS vLive - DEV544: Secure Coding in .NET: Developing Defensible Applications	**DEV544 - 201311,**	**Nov 04, 2013 - Nov 27, 2013**	**vLive**
South Florida 2013 - DEV522: Defending Web Applications Security Essentials	**Fort Lauderdale, FL**	**Nov 04, 2013 - Nov 09, 2013**	**vLive**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**