

Securing Your Web Applications

Why It Can Be the Most Important Thing You Do

I, like many other people, receive a newsletter from the SANS Institute that lists recently discovered vulnerabilities. This newsletter not only gives details about vulnerabilities but it also provides a summary that gives the number of vulnerabilities in each category (OS, Web Apps, 3rd Party Apps, etc.). Well, over the past couple of years or so I have been seeing those numbers shift. At one time operating systems had most of the vulnerabilities and Web Apps had very few. This has now completely shifted 180 degrees. With operating systems becoming more and more difficult to crack, web applications have become the hot target for hackers.

If it happened to them, it can happen to you!

If you haven't been living in a cave, you must have heard about TJX, the owner of clothing retailers TJ Max and Marshalls Inc., who had the largest known data theft to date. Over a period of 18 months, hackers invaded TJX computer systems and took at least 45.7 million credit and debit card numbers. Let's not forget about ChoicePoint, Inc. who lost the personal financial records of 163,000 consumers. There is also the University of Southern California, Natwest, Tower Records, and PetCo. You may ask why I am giving you this list of shame. It's because they all got into trouble through their web apps.

How to stay out of trouble

The best way to stay out of trouble is to find out where you stand with your web apps. Let's face it, most web developers are usually not all that security conscious (though I have seen some improvement). With the advent of programs that write the HTML code for you, anyone can produce a web page with interactive content. It may not be a good web page but a web page any way, and here is where we have some trouble. I have been to companies where I have found some very old and poor code buried in some very nice looking web pages. What I usually hear is "Yea, Ted built that page back in 97 when we first put up a web site. We just update the look and it just keeps on running." Unfortunately, Ted's contribution is full of security holes and no one but the hackers know it. What this company needed (of course that's why I was there) was a good audit. I learned early on in my auditing career that the mantra of auditors everywhere is "How do you know?" You know by testing.

Testing

Many large organizations have full time security teams dedicated to keeping their web pages safe. If you work for one them, you can stop reading - call a meeting and have the security team test your web apps, the rest of you may want to take a different approach. There are several possibilities here depending on how much time, training, and expense you want to devote to this process. If you want someone else to handle it, I would suggest a consultant. There are many advantages to using a consultant - no training, no company resources are used, and you don't even have to bind your own reports. If you do a lot of in house web development, you really should develop a testing process so that you can be assured that your web apps are securely coded during the development cycle. If you decide to go this on your own, there is a lot of good commercial testing software out there. SpyDynamics (now part of HP) makes some of the best, especially for development cycle testing. If you would really like to go it on your own, there are always plenty of free "Hacker" tools on the Internet. I use many of these types of tools to investigate possible false positives generated from the commercial tools or just to dig deeper. There can often be a great advantage to being able to see and manipulate the code yourself.

Tools

Below you will find some of the free tools that I work with. I most often scan first with a general commercial vulnerability scanner, to gather a baseline of the basic security of the web server. I then scan with a commercial web vulnerability scanner to dig deeper into the web apps. This looks for CGI vulnerabilities, SQL Injection, Cross-site scripting and a long list of other flaws. When these are done and I have had a good look at the data, I usually use a few of my favorite “hacker” tools. These tools are great for looking deeper at a flaw, because they are so specialized. One of the first that I use in this phase of the audit is Nikto. Nikto is an excellent little CGI scanner and while it is usually not as current as the commercial tools, it typically catches most of the issues. Two of the other free tools that I like are Brutus and WebScarab. Brutus is a nice authentication tester. WebScarab is an excellent tool that acts as a local proxy allowing you to collect and manipulate traffic flowing to and from a web page. Of course, there are many other excellent tools available on the Internet. They are well worth downloading. If nothing else, they can provide you a better understanding of what you face.

Conclusion

I hope this article has given a little insight to a growing security threat. No matter how you decide to approach this issue, it is important that it be approached. If you have interactive web pages with forms or any type of data entry point, those pages should be tested.

#

#

#

David B. Wean, Senior Security Analyst
(937) 384-0444 ext 2399
Email: dave.wean@digitalcontrols.com

David Wean has been a member of Digital Controls service team for 9 years. As a Senior Security Analyst, David is responsible for various security disciplines including Network Audits for Regulatory Compliance, Network Audits for Policy Compliance, Penetration Testing of Hardened Networks and Network Security Devices, Pre-deployment Device and Server Security Certification, Creation of Network Security and Physical Security Policy Sets, Secure Network Design, Security Forensics Investigation, Installation of Security Software and Hardware, Secure Wireless Design and Installation, WAN and LAN Hardware Installation, Hardware and Software Phone Support, and WAN/LAN Design.

Digital Controls Corporation is a local IT services and software company. Digital Controls Technology Services Group provides services to IT in the key areas of security, data storage management, networking, Microsoft infrastructure, and product sourcing. These services are delivered through consulting, professional services, on-site and remote managed services.

Digital Controls Corporation. All Rights Reserved. Published March 2008.