Foreword

Ryan Barnett recently asked if I'd write the foreword to his book. I was delighted to even be considered because Ryan is an exceptional security professional and the honor could have easily gone to anyone in the industry. Ryan has a background as someone who actively defends government web sites. He's the person who led the effort to create the Apache Benchmark standard for the Center for Internet Security (CIS). He's a co-author of the Web Security Threat Classification for the Web Application Security Consortium (WASC), and has more certifications than I knew existed. Ryan is also a SANS Instructor for Apache Security. There's quite a bit more, but suffice it to say Ryan has to be one of the most-qualified experts to write *Preventing Web Attacks with Apache*.

A foreword is an opportunity to express why a particular topic is important and describe what role the information plays in a broader context. Even though I've been part of the web application security field for a really long time (back before there was a term to describe what we do), more research was in order. I fired up Firefox and headed on over to Google for some investigation. Netcraft, the WASC, the CIS, the Open Source Vulnerability Database (OSVDB), SecurityFocus, and Wikipedia are incredible resources for collecting security information. While I was taking notes and saving bookmarks, it suddenly occurred to me that during my research, I must have crossed paths with hundreds of Apache web servers without realizing it. What a perfect way to describe the importance of Apache security!

According to Netcraft's Web Server Survey (September 2005), Apache accounts for roughly 70 percent of the Internet's web servers. Through our tiny browser window, it's difficult to imagine the global hum of 72 million web servers, the keyboard chatter of over 800 million international netizens, wading through a sea of 8 billion web pages. Apache is a fundamental part of our daily online lives—so much so, it's become a transparent artifact in the architecture of the web. When we shop for books, reserve plane tickets, read the news, check our bank account, bid in an auction, or do anything else with a web browser, the odds are there's an Apache web server involved. How's that for important?

The web has become bigger and more powerful than we ever imagined. 24x7x365, web sites carry out mission-critical business processes, exchanging even the most sensitive forms of information including names, addresses, phone numbers, social security numbers, financial records, medical history, birth dates, business contacts, and more. Web sites may also supply access to source code, intellectual property, customer lists, payroll data, HR data, routers, and servers. If a particular computer system or business process isn't web-enabled today, bet that it will be tomorrow. Anything a cyber-criminal would ever want is available somewhere on a web site. With all the great things we can do on the web, one must temper the benefits with the risk that any information available on or behind a web site is also a target for identify theft, industrial espionage, extortion, and fraud. It should come as no surprise that the attack trends we're witnessing are migrating from the network layer up to the web application layer.

Here's where things get interesting and scary at the same time. Firewalls, anti-virus scanners, and Secure Sockets Layer (SSL) do not help secure a web site. Let me say that again. Firewalls, anti-virus scanners, and SSL *do not help secure a web site*. When you visit any web site, we don't see any of these things because they functionally don't exist at the web layer. On the web, there's nothing standing between a hacker, your web server, your web applications, and your database. With something as pervasive as Apache, the knowledge of how to prevent web attacks is vital.

A martial arts black belt is a suitable analogy. It might take someone years to acquire the knowledge required to proficiently react to a given security scenario. Both Ryan and myself have experience defending extremely large and public web-enabled systems. We've witnessed the sophisticated and voluminous attacks that inundate our web servers. From Brute-Force or Cross-Site Scripting to Denial of Service or SQL Injection and Worms, the attacks are varied and pervasive. A single day of monitoring web server log files is enough to appreciate how much skill is required to thwart the ever-growing security threats.

Ryan has done a remarkable job combining his years of personal experience with the collective knowledge of a community of experts. Readers will be well served by this material for as long as there are web servers. I'll finish up with a famous quote I feel captures the essence of *Preventing Web Attacks with Apache*.

> *"The significant problems we face cannot be solved at the same level of thinking we were at when we created them."*
>
> *—Albert Einstein (1879-1955)*

We must be diligent, we must keep learning, we will prevail.

Jeremiah Grossman
Founder and CTO of WhiteHat Security
Cofounder of the Web Application Security Consortium (WASC)
September, 2005