

"Both novice and seasoned readers will come away with an increased understanding of how Web hacking occurs and enhanced skill at developing defenses against such Web attacks.

Technologies covered include Web languages and protocols, Web and database servers, payment systems and shopping carts, and critical vulnerabilities associated with URLs. This book is a virtual battle plan that will help you identify and eliminate threats that could take your Web site off line..."

-From the Foreword by William C. Boni, Chief Information Security Officer, Motorola

"Just because you have a firewall and IDS sensor does not mean you are secure; this book shows you why."

-Lance Spitzner, Founder, The Honeynet Project

Whether it's petty defacing or full-scale cyber robbery, hackers are moving to the Web along with everyone else. Organizations using Web-based business applications are increasingly at risk. *Web Hacking: Attacks and Defense* is a powerful guide to the latest information on Web attacks and defense. Security experts Stuart McClure (lead author of *Hacking Exposed*), Saumil Shah, and Shreeraj Shah present a broad range of Web attacks and defense.

Features include:

- Overview of the Web and what hackers go after
- Complete Web application security methodologies
- Detailed analysis of hack techniques
- Countermeasures

What to do at development time to eliminate vulnerabilities New case studies and eye-opening attack scenarios Advanced Web hacking concepts, methodologies, and tools "How Do They Do It?" sections show how and why different attacks succeed, including:

- Cyber graffiti and Web site defacements
- e-Shoplifting
- Database access and Web applications
- Java(TM) application servers; how to harden your Java(TM) Web Server
- Impersonation and session hijacking
- Buffer overflows, the most wicked of attacks
- Automated attack tools and worms

Appendices include a listing of Web and database ports, cheat sheets for remote command execution, and source code disclosure techniques.

Web Hacking informs from the trenches. Experts show you how to connect the dots--how to put

the stages of a Web hack together so you can best defend against them. Written for maximum brain absorption with unparalleled technical content and battle-tested analysis, Web Hacking will help you combat potentially costly security threats and attacks.

Foreword

In your hands is a book that is an essential companion safeguarding the increasingly critical Web sites and e-commerce systems that are the cornerstone of global e-businesses. Web Hacking: Attacks and Defense offers the distilled experience of leading security consultants that will help level the playing field for the beleaguered security and IT staff challenged with fending off the hacker onslaught—those who see the Internet as a faster and more efficient mechanism for stealing from and abusing others. If you read and apply the lessons offered here, some of the most disreputable people on the Internet are going to be severely disappointed, as some of their most effective tricks will be useless against your sites. They will have to be much more creative and work a lot harder to compromise the security of your applications. These pages are filled with the knowledge and distilled experience of some of the world's best white-hat hackers, the stalwart consultants of Foundstone.

The authors have delivered eye-opening and dazzling insights into the world of Web site and application hacking. Some of the most devastating tools and techniques that have been used by cyber criminals and hackers to lay waste to Web sites around the planet are discussed in this book. The part opener case studies and chapter examples lay out in stunning detail the consequences of failing to understand and anticipate the many methods that are available and in use by the "dark side." The countermeasures necessary to combat these depredations are detailed with clinical efficiency. To defeat thieves, it helps to know where, how, and why they strike and the weak points they favor. Web Hacking is your guidebook to these techniques.

The book is a technical tour de force chock full of valuable descriptions of how, when, where, and why elements of the Web site will be attacked. It balances accurate and complete technical exposition with explanations that help less technically knowledgeable readers grasp the essential elements of the attacks and essential defenses.

Shocking in some places, it describes how even well-trained Web site designers and operators often make crucial mistakes in implementing sites. By the time you have read this book, you will have learned dozens of ways that Web sites can be attacked and manipulated. The first and most important step is to accept the fact that the threat to Web sites is real and ever increasing. Given that, the Internet provides the perfect environment for hacking, and this book helps e-commerce and online businesses to understand and guard against these global risks.

The chapters are replete with examples that drive home the lesson that the Internet really is a dangerous place to operate a business. When virtual storefronts meet real criminals operating in cyberspace even seemingly minor errors (the way sites are coded and how components are linked) can create huge vulnerabilities. Recent research by the Honeynet (www.honeynet.org) project has proven that an inadequately secured site will be attacked within minutes after it

becomes visible on the Internet. What is worse, commercial Web sites with high-risk vulnerabilities will be exploited by criminals who may never be identified, and even if they are found, could well be out of reach of traditional law enforcement agencies. Even nonprofit sites may be defaced or abused to provide online storage for illegal transactions such as cracked software.

We live in an age reminiscent of the American Old West, and it's too often a case of survival of the fittest. When classic law enforcement methods do little to prevent attacks, IT managers and Web site designers and operators cannot rely on luck alone to defend their vital e-business environments. Knowledge truly is power, so equip yourself and your organization with the insights of some of the best ethical hackers to be found anywhere. This book is a virtual battle plan that will help you identify and eliminate threats that could take your Web site off line due to cyber fraud, defacement, unauthorized access, modification, or destruction. Let the insights of these expert security consultants work for you and sleep better knowing that you and your organization are doing your part to reduce the potential for cyber crime.

William C. Boni
Chief Information Security Officer, Motorola
July 2002

Introduction

Truth is one, but error proliferates. Man tracks it down and cuts it up into little pieces hoping to turn it into grains of truth. But the ultimate atom will always essentially be an error, a miscalculation.

—René Daumal (1908–1944), French poet, critic.

"We're Secure, We Have a Firewall"

If only we had a nickel for every time we've heard a client utter these words. We'd probably not be writing this book; rather, we'd be sipping Piña Coladas on some white sand beach by now and... .

If you're skeptical, all warm and cozy next to your firewall, just remember this: Over 65% of reported attacks occur via TCP port 80, the traditional Web port (<http://www.incidents.org>). Is the threat to the Web real? You bet—it's all too real.

To Err Is Human

In the course of performing hundreds of security reviews over the decades, we learned what you are about to learn (if you don't already know it): Nothing can be truly secure. Error is at the heart of every security breach and, as the saying goes: To err is human. No level of firewall, intrusion detection system (IDS), or anti-virus software will make you secure. Are you surprised that this type of comment introduces a security book? Don't be. It is the harsh reality that must be accepted before the race to security can be started.

So what should you do, just throw up your hands, turn off the power to your computer and ignore the Internet, the modem, and the computer? Sure, you can do that but you would be alone in your efforts. The Internet and all it has to offer is undeniable: increased communication and information sharing, connecting with people of all races, creeds, colors, sexes, and intelligence without boundaries or limits. And those are just the home users' benefits. Businesses use the Internet 24 hours a day, 7 days a week, making money and transmitting funds around the world at the blink of an eye. Anyone who denies the ubiquity and staying power of the Internet is just kidding themselves.

Writing on the Wall

More than three years ago, one of the authors of this book wrote a foreboding article that was indicative of things to come. Printed on August 9, 1999, it was titled "Bane of e-commerce: We're secure: We allow only Web traffic through our firewall" (<http://www.infoworld.com/articles/op/xml/99/08/09/990809opsecwatch.xml>). The article warned of flaws in the security wall at that time, but no one wanted to believe it, much less talk about it. Everyone seemingly was too caught up in either hyped technologies, such as Firewalls, IDS, and virtual private networks (VPN), or peripheral technologies that never hit mainstream, such as Public Key Infrastructure (PKI), Distributed Computing Environment (DCE), and single signon.

So why the tremendous interest in the Web and its security now? Because hacking events occur frequently in today's connected world. And people are beginning to understand how a single vulnerability in a Web application can expose an entire company's information system to an attacker (a.k.a. Code Red and Nimda worms).

Book Organization

We wrote this book for maximum absorption and comprehension—that is, moving from introductory to intermediate to advanced techniques and concepts. To accomplish this goal, we organized this book into four parts, containing seventeen chapters, and appendices.

Parts

- [Part One](#)—The E-Commerce Playground
- [Part Two](#)—URLs Unraveled
- [Part Three](#)—How Do They Do It?
- [Part Four](#)—Advanced Web Kung Fu

Each Part gets progressively more advanced in content and delivery, going from a brief Web languages introduction ([Chapter 1](#)) to finding and exploiting your own buffer overflows ([Chapter 14](#)). But don't let the increasing pace derail your learning. If you missed something, you can go back to it or, in some cases, you may be able to pick it up as you go along.

[Parts One](#) and [Two](#) give you a preliminary and then an intermediate introduction to the World Wide Web. In E-Commerce Playground we show you how the Web works—its languages, applications, databases, protocols, and syntax. In URLs Unraveled, we delve into the meaning of the URL, what is important to an attacker, and how visible code can be helpful to an attacker; we also show you how mapping Web sites can be crucial to an attacker's repertoire.

In [Part Three](#) we demystify the art of Web hacking, how it is pulled off, and how simple steps at development time can eliminate a large portion of the threat. This part is by far the meatier of the parts in terms of the information presented and often provides the best clues about how hackers do what they do. Each chapter provides both a detailed analysis of the hack as well as a countermeasure section at the end to help prevent the hack.

In [Part Four](#) we discuss some advanced Web hacking concepts, methodologies, and tools that you simply can't afford to miss.

Finally, at the end of the book, you will find Appendices that include a list of common Web ports on the Internet, cheat sheets for remote command execution, and source code disclosure techniques, among other useful information.

Chapters

[Part One](#), The E-Commerce Playground, contains five chapters.

- [Chapter 1](#), Web Languages: The Babylon of the 21st Century—discusses all the major Web languages used on the Internet today.
- [Chapter 2](#), Web and Database Servers—discusses the technologies behind the Web and how they introduce vulnerabilities.
- [Chapter 3](#), Shopping Carts and Payment Gateways—discusses the technologies behind online shopping carts and E-commerce sites on the Web.
- [Chapter 4](#), HTTP and HTTPS: The Hacking Protocols—discusses the two main protocols used to direct Web and E-commerce traffic on the Internet.

- [Chapter 5](#), URL: The Web Hacker's Sword—discusses understanding everything about a Web site just from reading the URL.

[Part Two](#), URLs Unraveled, contains three chapters.

- [Chapter 6](#), Web: Under(the)Cover—discusses the details of a complete Web application, including all its components and dependencies.
- [Chapter 7](#), Reading Between the Lines—discusses the fine art of disclosing source in a Web browser or alternative interface.
- [Chapter 8](#), Site Linkage Analysis—discusses how attackers inventory a Web site to understand the application as a whole and how to attack it.

[Part Three](#), How Do They Do It?, contains six chapters.

- [Chapter 9](#), Cyber Grafitti—discusses how attackers deface Web sites, their techniques, and their tricks.
- [Chapter 10](#), E-Shoplifting—discusses how attackers commit online shoplifting by tricking an application to give them merchandise at a lower price.
- [Chapter 11](#), Database Access—discusses how attackers break into Web applications through the database.
- [Chapter 12](#), Java: Remote Command Execution—discusses how attackers use Java as a mechanism for breaking into a system.
- [Chapter 13](#), Impersonation—discusses how an attacker can take on another user's identity.
- [Chapter 14](#), Buffer Overflows: On-the-Fly—discusses how an attacker can identify and create overflows in an application.

[Part Four](#), Advanced Web Kung Fu, contains the final three chapters.

- [Chapter 15](#), Web Hacking: Automated Tools—discusses the tools and techniques that hackers use to perform many of their tricks in an automated fashion.
- [Chapter 16](#), Worms—discusses the deadly worm and how it is created, propagated, and removed.
- [Chapter 17](#), Beating the IDS—discusses how IDS can help and hurt a hunt for an attacker.

A Final Word

This book offers both an introduction to hacking and a detailed look into the world of the Web hacker. At the same time it is intended to be an easy read—one that you won't be tempted to add to your list of insomnia cures. The ideal way to approach the book is from front to back. However, if you begin with a basic knowledge of security and Web technologies, you should have no problem jumping right into [Part Two](#) (URLs Unraveled) and [Part Three](#) (How Do They Do It?).

Vulnerabilities will always be present in any environment, but we hope that people using the Web and Internet will wake up and smell the coffee and correct their misconceptions and mistakes. Because if they don't, a hacker most certainly will.

Acknowledgments

Many elements contributed to the work that we all put into this book. First and foremost, we would like to thank the editorial staff at Addison-Wesley. Their guidance and patience throughout the process is laudable. Sincere respect and gratitude must go out to the dedicated professionals at Foundstone. The combined brainpower found at the company continues to impress and amaze.

We applaud the work of the security researchers in the industry, whom we have had the privilege of rubbing shoulders with (you all know who you are). Our gratitude also goes to our friends at Net-Square in India, for helping us research and collaborate on many topics in the book.

Finally, we would especially like to thank Barnaby Jack for his contributions to this book.

Contributor

Barnaby Jack is a Research and Development Engineer with Foundstone where he specializes in vulnerability research and exploit development. Prior to joining Foundstone he was an engineer with the COVERT research team at Network Associates.

He has been deeply involved with operating system internals for a number of years, primarily concentrating on Windows NT and its derivatives. He has performed considerable research in the field of Windows exploitation methods, and his work and articles have subsequently been referenced in a number of major security publications.