PREFACE

THE TANGLED WEB WE'VE WOVEN

Over three years ago, *Hacking Exposed, First Edition* introduced many people to the ease with which computer networks and systems are broken into. Although there are still many today who are not enlightened to this reality, large numbers are beginning to understand the necessity for firewalls, secure operating system configuration, vendor patch maintenance, and many other previously arcane fundamentals of information system security.

Unfortunately, the rapid evolution brought about by the Internet has already pushed the goalposts far upfield. Firewalls, operating system security, and the latest patches can all be bypassed with a simple attack against a Web application. Although these elements are still critical components of any security infrastructure, they are clearly powerless to stop a new generation of attacks that are increasing in frequency every day now.

We cannot put the horse of Internet commerce back in the barn and shut the door. There is no other choice left but to draw a line in the sand and defend the positions staked out in cyberspace by countless organizations and individuals.

For anyone who has assembled even the most rudimentary Web site, you know this is a daunting task. Faced with the security limitations of existing protocols like HTTP, as well as the ever-accelerating onslaught of new technologies like WebDAV and XML Web Services, the act of designing and implementing a secure Web application can present a challenge of Gordian complexity.

Meeting the Web App Security Challenge

We show you how to meet this challenge with the two-pronged approach adapted from the original *Hacking Exposed*, now in its third edition.

First, we catalog the greatest threats your Web application will face and explain how they work in excruciating detail. How do we know these are the greatest threats? Because we are hired by the world's largest companies to break into their Web applications, and we use them on a daily basis to do our jobs. And we've been doing it for over three years, researching the most recently publicized hacks, developing our own tools and techniques, and combining them into what we think is the most effective methodology for penetrating Web application (in)security in existence.

Once we have your attention by showing you the damage that can be done, we tell you how to prevent each and every attack. Deploying a Web application without understanding the information in this book is roughly equivalent to driving a car without seatbelts—down a slippery road, over a monstrous chasm, with no brakes, and the throttle jammed on full.

HOW THIS BOOK IS ORGANIZED

This book is the sum of parts, each of which is described here from largest organizational level to smallest.

Parts

This book is divided into three parts:

I: Reconnaissance

Casing the establishment in preparation for the big heist, and how to deny your adversaries useful information at every turn.

II: The Attack

Leveraging the information gathered so far, we will orchestrate a carefully calculated fusillade of attempts to gain unauthorized access to Web applications.

III: Appendixes

A collection of references, including a Web application security checklist (Appendix A); a cribsheet of Web hacking tools and techniques (Appendix B); a tutorial and sample scripts describing the use of the HTTP-hacking tool libwhisker (Appendix C); step-by-step instructions on how to deploy the robust IIS security filter UrlScan (Appendix D); and a brief word about the companion Web site to this book, www.webhackingexposed.com (Appendix E).

Chapters: The Web Hacking Exposed Methodology

Chapters make up each part, and the chapters in this book follow a definite plan of attack. That plan is the methodology of the malicious hacker, adapted from *Hacking Exposed*:

- ▼ Profiling
- ■ Web server hacking
- ■ Surveying the application
- ■ Attacking authentication
- ■ Attacking authorization
- ■ Attacking session state management
- ■ Input validation attacks
- ■ Attacking Web datastores
- ■ Attacking XML Web Services
- ■ Attacking Web application management
- ■ Hacking Web clients
- ▲ Case studies

This structure forms the backbone of this book, for without a methodology, this would be nothing but a heap of information without context or meaning. It is the map by which we will chart our progress throughout the book.

Modularity, Organization, and Accessibility

Clearly, this book could be read from start to finish to achieve a soup-to-nuts portrayal of Web application penetration testing. However, as with *Hacking Exposed*, we have attempted to make each section of each chapter stand on its own, so the book can be digested in modular chunks, suitable to the frantic schedules of our target audience.

Moreover, we have strictly adhered to the clear, readable, and concise writing style that readers overwhelmingly responded to in *Hacking Exposed*. We know you're busy, and you need the straight dirt without a lot of doubletalk and needless jargon. As a reader of *Hacking Exposed* once commented, "Reads like fiction, scares like hell!"

We think you will be just as satisfied reading from beginning to end as you would piece by piece, but it's built to withstand either treatment.

Chapter Summaries and References and Further Reading

In an effort to improve the organization of this book, we have included two features at the end of each chapter: a "Summary" and "References and Further Reading" section.

The "Summary" is exactly what it sounds like—a brief synopsis of the major concepts covered in the chapter, with an emphasis on countermeasures. We would expect that if

you read each "Summary" from each chapter, you would know how to harden a Web application to just about any form of attack.

"References and Further Reading" includes hyperlinks, ISBN numbers, and any other bit of information necessary to locate each and every item referenced in the chapter, including vendor security bulletins and patches, third-party advisories, commercial and freeware tools, Web hacking incidents in the news, and general background reading that amplifies or expands on the information presented in the chapter. You will thus find few hyperlinks within the body text of the chapters themselves—if you need to find something, turn to the end of the chapter, and it will be there. We hope this consolidation of external references into one container improves your overall enjoyment of the book.

THE BASIC BUILDING BLOCKS: ATTACKS AND COUNTERMEASURES

As with *Hacking Exposed*, the basic building blocks of this book are the attacks and countermeasures discussed in each chapter.

The attacks are highlighted here as they are throughout the *Hacking Exposed* series.

This Is an Attack Icon

Highlighting attacks like this makes it easy to identify specific penetration-testing tools and methodologies and points you right to the information you need to convince management to fund your new security initiative.

Each attack is also accompanied by a Risk Rating, scored exactly as in *Hacking Exposed*:

Popularity:	The frequency of use in the wild against live targets, 1 being most rare, 10 being widely used
Simplicity:	The degree of skill necessary to execute the attack, 10 being little or no skill, 1 being seasoned security programmer
Impact:	The potential damage caused by successful execution of the attack, 1 being revelation of trivial information about the target, 10 being superuser account compromise or equivalent
Risk Rating:	The preceding three values are averaged to give the overall risk rating and rounded to the next highest whole number

We have also followed the *Hacking Exposed* line when it comes to countermeasures, which follow each attack or series of related attacks. The countermeasure icon remains the same:

This Is a Countermeasure Icon

This should be a flag to draw your attention to critical fix information.

Other Visual Aids

We've also made prolific use of visually enhanced

icons to highlight those nagging little details that often get overlooked.

ONLINE RESOURCES AND TOOLS

Web app security is a rapidly changing discipline, and we recognize that the printed word is often not the most adequate medium to keep current with all of the new happenings in this vibrant area of research.

Thus, we have implemented a World Wide Web site that tracks new information relevant to topics discussed in this book, errata, and a compilation of the public-domain tools, scripts, and dictionaries we have covered throughout the book. That site address is:

```
http://www.webhackingexposed.com
```

It also provides a forum to talk directly with the authors via e-mail:

```
joel@webhackingexposed.com
mike@webhackingexposed.com
```

We hope that you return to the site frequently as you read through these chapters to view any updated materials, gain easy access to the tools that we mentioned, and otherwise keep up with the ever-changing face of Web security. Otherwise, you never know what new developments may jeopardize your applications before you can defend yourself against them.

A FINAL WORD TO OUR READERS

There are a lot of late nights and worn-out mouse pads that went into this book, and we sincerely hope that all of our research and writing translates to tremendous time savings for those of you responsible for securing Web applications. We think you've made a courageous and forward-thinking decision to stake your claim on a piece of the Internet—but as you will find in these pages, your work only begins the moment the site goes live. Don't panic—start turning the pages and take great solace that when the next big Web security calamity hits the front page, you won't even bat an eye.

—Joel & Mike