

book reviews



ELIZABETH ZWICKY, WITH
RIK FARROW, SAM F. STOVER,
AND KIM GRILLO

WICKED COOL PHP: REAL-WORLD SCRIPTS THAT SOLVE DIFFICULT PROBLEMS

William Steinmetz with Brian Ward

No Starch Press, 2008. 181 pp.
ISBN 978-1-59327-173-2

Wicked Cool PHP is aimed at an audience that can write PHP—possibly because they learned how to code “Hello World!” somewhere else, possibly just because it’s not that hard if you already know other programming languages—but want to know how to do interesting things. In another context, it might be called a PHP pattern book. It gives frameworks for accomplishing common tasks, along with information about common mistakes people make when trying to do these things.

It comes from a sensible but relatively naive security perspective. For instance, it tells you to use MD5 hashes instead of shuttling passwords around, but does not have any information about salts. It gives information about letting Web site users send mail, but doesn’t suggest that you need controls to keep from becoming a spam engine. It doesn’t give you any information about avoiding cross-site request forgery (where a user who has a valid cookie is tricked into sending a request). Nonetheless, it does give appropriate warnings about PHP configuration, sanitizing user input, and avoiding SQL injection and cross-site scripting. It’s not suitable as your only resource for building a complex site, but it’s a good starting point.

ESSENTIAL PHP SECURITY: A GUIDE TO BUILDING SECURE WEB APPLICATIONS

Chris Shiflett

O’Reilly, 2006. 103 pp.
ISBN 0-596-00656-X

As you might expect, this does a much better job of covering security than *Wicked Cool PHP*. It goes much deeper into threats, covers general security techniques and attitudes (never trust the user! defense in depth!), and provides convincing examples of attacks. (A surprising number of people have difficulty getting their heads around the idea that people might not access your Web server from your forms.)

Unfortunately, it’s not an easy read. For a motivated reader, a PHP programmer who wants the essentials from a PHP perspective, it’s probably still a good choice. It’s probably your only choice for some specialist topics; it covers securing your part of a shared Web server, when other books are likely to leave you frustrated and despairing.

YES: 50 SCIENTIFICALLY PROVEN WAYS TO BE PERSUASIVE

Noah J. Goldstein, Steve J. Martin, and Robert B. Cialdini

Free Press, 2008. 272 pp.
ISBN 978-1-4165-7096-7

You may be sure that you are too smart to fall for silly tricks like having a sales pitch come from somebody “like you.” Don’t be so sure. In one study, nearly twice as many people were willing to fill out a survey form when it came from somebody with a name like theirs. And not one of them believed the name had anything to do with it.

This is the latest summary of research on influence, which Robert Cialdini is the grand master of. It’s easy to read, convincing, and reassuringly convinced of the importance of actually being a reasonable person. It’s also a little scary as you see just how effective some of these techniques can be.

Aside from being a fascinating read, this book is a useful tool for anybody who’s trying to get people to do something (upgrade their software, clean out their over-full mailboxes, use approved channels to report problems, report the problems in the first place).

DON'T MAKE ME THINK: A COMMON SENSE APPROACH TO WEB USABILITY, SECOND EDITION

Steve Krug

New Riders, 2006. 197 pp.
ISBN 0-321-34475-8

To finish up, we neatly combine the themes of Web development and persuasion with the second edition of a classic book about Web design. Well, actually, about Web usability, which is to say, it's not about whether or not you should paint it blue and make the corners rounded, it's about building something that people will actually enjoy using. Not because you should panic now—on the Web people have no attention span and will flee to a competitor—but because, get this, people don't like it when things are hard to use, and torturing your customers is never good.

OK, so that doesn't sound like a deep insight, and without some advice on how to make things easy to use, it wouldn't be all that useful. But it's more of an insight than you might think, and it's a pleasant antidote to the people who wish to assure us that it is all different on the Web. This book will not only convince you that it's more important to have a usable Web site than to have a beautiful one, it will also provide you with a handy form letter to pass on to the boss who thinks that a Flash intro page is the best idea ever.

Along the way, you get a brief introduction to usability testing and how to do it cheaply and effectively, some amusing cartoons, and a number of straightforward instructions. It truly is both fun and educational.

CONFESSIONS OF A PUBLIC SPEAKER

Scott Berkun

O'Reilly, 2009. 220 pp.
ISBN 978-0-596-80199-1

REVIEWED BY RIK FARROW

This is a book of advice for potential and current public speakers. Berkun points out that everyone is a public speaker, even if this speaking only occurs over beers. But he also writes that most people who read his book won't be good public speakers (p. 140). He then repeats the single bit of advice he's been harping on: practice. Berkun goes beyond suggesting the practice is important, or even a virtue—it is the essential ingredient for good presentations.

If that was all he had to say, this book would be quite short. But Berkun has a conversational writing style that's easy to read, and he peppers his writing with storytelling, making this truly a book about confessions. Some of the confessions, such as that all speakers have some level of fear before a presentation, are very comforting. Berkun's story about being part of the B-roll footage for a CNBC five-hour primetime TV series was one of being panicked, and later, humbled: "First, I have no idea what is going on, yet I am the center of attention, much like how it would feel to be invited over for dinner by a family of cannibals" (p. 97).

Berkun offers lots of advice, much more than you can take in with one reading. Although I have presented routinely since 1986, I found lots of ideas I hadn't thought of myself, or things that I had done sometimes without making it part of my bag of tricks. For example, Berkun covers audience issues—like the giant, mostly empty room, or the frequent questioner who wants to take over your talk—by providing useful advice for dealing with these very real issues. Of all the suggestions offered, I want to repeat one that Berkun also repeats: the audience is there for you. Even if they want to attack you later, they want you to present your points first. And most of the time the audience is there because you are going to give them something useful, and so it has a vested interest in your success.

Even though most people will never become professional public speakers, we are, as Berkun says, all public speakers at some level. I found his book easy to read, enjoyable as well as useful, and a book I can recommend.

HACKING: THE NEXT GENERATION

Nitesh Dhanjani, Billy Rios, and Brett Hardin

O'Reilly, 2009. 296 pp.
ISBN 978-0596154578

REVIEWED BY SAM STOVER

This book is fantastic! Everyone on the planet should read it. Here are the goods:

Chapter 1 introduces the more obvious intel-gathering techniques such as dumpster diving and social engineering, but also logical techniques such as automated Google hacking, file metadata gathering, social network analysis, and email harvesting.

Chapter 2 dives into a fair bit of detail concerning JavaScript methods for turning browsers into access points into an organization. Lots of good reading on XSS, CSRF, attack automation, content ownership,

and even using the browser to steal files off of local file systems.

Chapter 3 might seem disappointing to the technically savvy, as it deals with protocols like FTP, Telnet, ARP, and SMTP. The authors justify the chapter, saying that these are long-standing issues with older protocols, and I have to agree. This might be old hat to most of us, but it's still a problem in the real world.

Chapter 4 explains blended threats, starting with application protocol handlers, which I found interesting. Not only are protocol handlers explained and used in blended threats, but methods are given to enumerate protocol handlers in Windows, OS X, and Linux. Good stuff.

Chapter 5 addresses cloud computing, with a focus on Amazon (EC2) and Google (AppEngine). Some basic attacks are presented, like poisoned virtual machines, and management console targeting. In some cases, XSS/CSRF come into play, connecting back to Chapter 2.

Chapter 6 leaves the world of Web technology to look at how mobile devices are being used and abused in the mobile workforce. Most of the chapter deals with stealing information from hotel networks and hotspots, and there are some tidbits concerning cell phone voice-mail and physical attacks against cell phones.

Chapter 7 is one of the best phishing primers that I've ever seen. Example sites (that worked) are dissected in a way that makes it easy to see what was happening. An interesting take-away from this chapter is that successful phishers don't have to be techno-wizards; lame phishing pages still produce results. A decent intro into the e-crime underground is also provided, which provides a nice backdrop.

Chapter 8, an offshoot of Chapter 1, focuses on social engineering, showing how attackers use a small bit of information as a foundation to a profile. Things like calendars and social network sites can yield all that's needed to "buddy up," and several examples are discussed. Not being a fan of social sites, I feel vindicated after reading this book, although I'm not sure I buy into the viability of "sentiment analysis."

Chapter 9 provides a profile of steps for building a targeted attack. The chapter starts with an overview of motives, moves into information gathering methods, and finishes with attack options. Techniques such as penetrating

the inner circle and "targeting the assistant" are discussed.

Chapter 10 gives two case studies that build from the previous chapters. Not very technical and pretty brief, but still realistic and representative.

Overall, this book is a triumph. Well written, solid material, and fun. Just what you'd expect from an O'Reilly book.

SCENE OF THE CYBERCRIME, SECOND EDITION

Debra Littlejohn Shinder and Michael Cross

Syngress, 2008. 744 pp.
ISBN 978-1597492768

REVIEWED BY KIM GRILLO

When I first read the title of this book I figured that after investigating cybercrime for the past five years as part of my job, this book would be too entry-level for me. However, the author introduces many tools and forensics techniques that were not covered either in my formal education or as part of my on-the-job training. The authors have a very good understanding of the issues that law enforcement and security professionals face when investigating cybercrime. These issues are introduced at the beginning of the book to lay the groundwork for the subsequent chapters. The book covers a wide range of information, including investigation of cybercrimes and security basics, best practices for preventing threats and implementing security, and collection of information for prosecution that would be of interest to law enforcement and IT professionals as well as those just entering the world of cyber investigations.

For example, Chapters 15, 16, and 17 spend a lot of time discussing the cybercrime legal process, which is a great introduction to the topic for someone who has never encountered it before or for the techie who needs to work closely with law enforcement. These chapters provide a good background on some of the obstacles law enforcement faces when working cybercrime, such as jurisdictional issues, and also provides an in-depth look into what to expect if testifying as an expert witness. There is also enough technical discussion of tools and tips to keep the technical crowd interested. Chapter 6 deals with Computer Forensic Software and Hardware, which provides a fair amount of information on disk imaging, file recovery, and Linux/UNIX tools. The chapter even includes a forensic software reference, over 30 pages of programs and utilities with brief descriptions of their uses.

I think this book is targeted at law enforcement officers assigned to cybercrime cases with no formal background in information technology. The book probably covers more information than they would need to perform their job and at times might be a bit too technical for someone without an IT background. But this makes it very well suited to the technical individual who has responsibilities or an interest in cyber investigation, providing a good mix of the “known” (tools and tricks introduced in the Computer Forensics Software and Hardware chapter) and the unknown (learning about cybercrime legal process). Overall, this is a great book for anyone already working in the field of cybercrime as well as those just entering it.

Why the Semicolon in ;login:?

The answer, as told to Peter Salus by Dennis Ritchie:

“The ; was utilitarian. During most of the early '70s the most popular terminal was the Teletype model 37. The sequence <esc>; put it into full-duplex mode so the terminal didn't print characters locally, but let the system echo them. So this sequence was put into the greeting message. Of course it didn't print when you used that terminal, but other terminals that appeared later didn't understand the message and so printed the ;.”

—Peter H. Salus, *A Quarter Century of UNIX*, p. 69.

