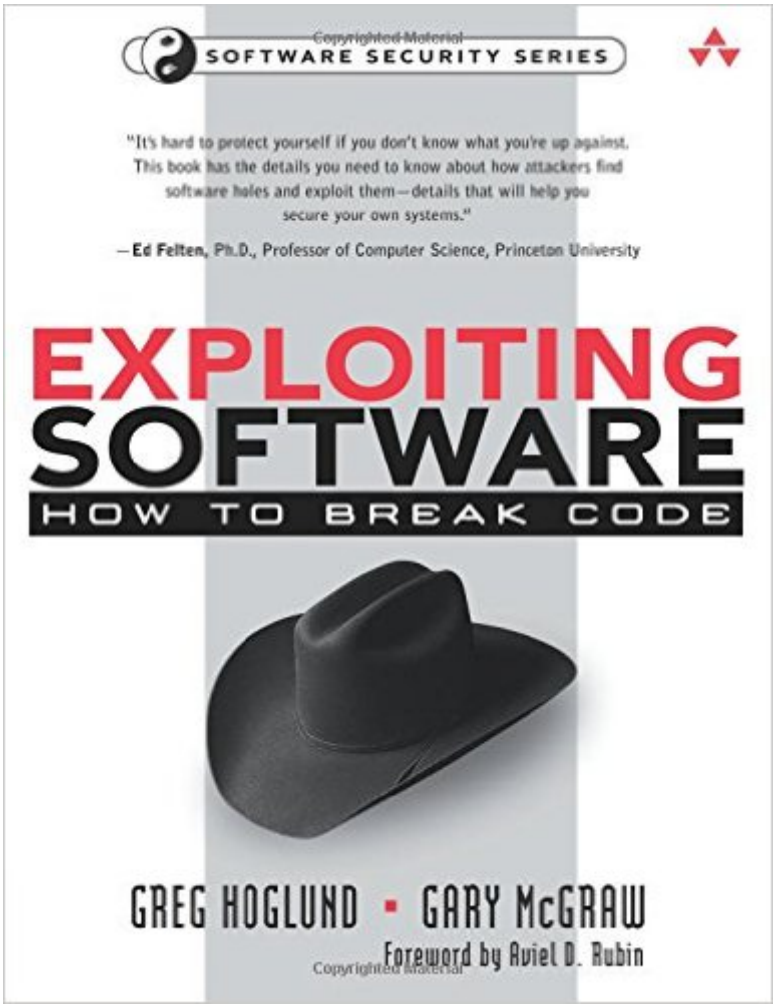
Exploiting Software: How To Break Code



Synopsis

Praise for Exploiting Software â œExploiting Software highlights the most critical part of the software quality problem. As it turns out, software quality problems are a major contributing factor to computer security problems. Increasingly, companies large and small depend on software to run their businesses every day. The current approach to software quality and security taken by software companies, system integrators, and internal development organizations is like driving a car on a rainy day with worn-out tires and no air bags. In both cases, the odds are that something bad is going to happen, and there is no protection for the occupant/owner. This book will help the reader understand how to make software quality part of the designâ ”a key change from where we are today!â • Â Â Â Â Â Â Â Â Â â ”Tony Scott Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Chief Technology Officer, IS&S Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â General Motors Corporation â œItâ ™s about time someone wrote a book to teach the good guys what the bad guys already know. As the computer security industry matures, books like Exploiting Software have a critical role to play.â • Â Â Â Â Â Â Â Â Â â ”Bruce Schneier Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Chief Technology Officer Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Counterpane Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Author of Beyond Fear and Secrets and Lies â œExploiting Software cuts to the heart of the computer security problem, showing why broken software presents a clear and present danger. Getting past the â ˆworm of the dayâ ™ phenomenon requires that someone other than the bad guys understands how software is attacked. This book is a wake-up call for computer security.â • Â Â Â Â Â Â Â Â Â â ”Elinor Mills Abreu Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Reutersâ ™ correspondent â œPolice investigators study how criminals think and act. Military strategists learn about the enemyâ ™s tactics, as well as their weapons and personnel capabilities. Similarly, information security professionals need to study their criminals and enemies, so we can tell the difference between popguns and weapons of mass destruction. This book is a significant advance in helping the â ˆwhite hatsâ ™ understand how the â ˆblack hatsâ ™ operate. Through extensive examples and â ˆattack patterns,â ™ this book helps the reader understand how attackers analyze software and use the results of the analysis to attack systems. Hoglund and McGraw explain not only how hackers attack servers, but also how malicious server operators can attack clients (and how each can protect themselves from the other). An excellent book for practicing security engineers, and an ideal book for an undergraduate class in software security.â • Â Â Â Â Â Â Â Â Â â ”Jeremy Epstein Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Director, Product Security & Performance Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â webMethods, Inc. â œA provocative and revealing book from two leading security experts and world class software exploiters, Exploiting Software enters the mind of the cleverest and wickedest crackers and shows you how they think. It

illustrates general principles for breaking software, and provides you a whirlwind tour of techniques for finding and exploiting software vulnerabilities, along with detailed examples from real software exploits. Exploiting Software is essential reading for anyone responsible for placing software in a hostile environmentâ ”that is, everyone who writes or installs programs that run on the Internet.â • Â Â Â Â Â Â Â Â Â â ”Dave Evans, Ph.D. Â Â Â Â Â Â Â Â Â Â Â Â Â Â Associate Professor of Computer Science Â Â Â Â Â Â Â Â Â Â Â Â Â Â University of Virginia â œThe root cause for most of todayâ ™s Internet hacker exploits and malicious software outbreaks are buggy software and faulty security software deployment. In Exploiting Software, Greg Hoglund and Gary McGraw help us in an interesting and provocative way to better defend ourselves against malicious hacker attacks on those software loopholes. The information in this book is an essential reference that needs to be understood, digested, and aggressively addressed by IT and information security professionals everywhere.â • Â Â Â Â Â Â Â Â Â â ”Ken Cutler, CISSP, CISA Â Â Â Â Â Â Â Â Â Â Â Â Â Â Vice President, Curriculum Development & Professional Services, Â Â Â Â Â Â Â Â Â Â Â Â Â Â MIS Training Institute â œThis book describes the threats to software in concrete, understandable, and frightening detail. It also discusses how to find these problems before the bad folks do. A valuable addition to every programmerâ ™s and security personâ ™s library!â • Â Â Â Â Â Â Â Â Â â ”Matt Bishop, Ph.D. Â Â Â Â Â Â Â Â Â Â Â Â Â Â Professor of Computer Science Â Â Â Â Â Â Â Â Â Â Â Â Â Â University of California at Davis Â Â Â Â Â Â Â Â Â Â Â Â Â Â Author of Computer Security: Art and Science â œWhether we slept through software engineering classes or paid attention, those of us who build things remain responsible for achieving meaningful and measurable vulnerability reductions. If you canâ ™t afford to stop all software manufacturing to teach your engineers how to build secure software from the ground up, you should at least increase awareness in your organization by demanding that they read Exploiting Software. This book clearly demonstrates what happens to broken software in the wild.â • Â Â Â Â Â Â Â Â Â â ”Ron Moritz, CISSP Â Â Â Â Â Â Â Â Â Â Â Â Â Â Senior Vice President, Chief Security Strategist Â Â Â Â Â Â Â Â Â Â Â Â Â Â Computer Associates â œExploiting Software is the most up-to-date technical treatment of software security I have seen. If you worry about software and application vulnerability, Exploiting Software is a must-read. This book gets at all the timely and important issues surrounding software security in a technical, but still highly readable and engaging, way. Hoglund and McGraw have done an excellent job of picking out the major ideas in software exploit and nicely organizing them to make sense of the software security jungle.â • Â Â Â Â Â Â Â Â Â â ”George Cybenko, Ph.D. Â Â Â Â Â Â Â Â Â Â Â Â Â Â Dorothy and Walter Gramm Professor of Engineering, Dartmouth Â Â Â Â Â Â Â Â Â Â Â Â Â Â Founding Editor-in-Chief,

IEEE Security and Privacy â œThis is a seductive book. It starts with a simple story, telling about hacks and cracks. It draws you in with anecdotes, but builds from there. In a few chapters you find yourself deep in the intimate details of software security. It is the rare technical book that is a readable and enjoyable primer but has the substance to remain on your shelf as a reference. Wonderful stuff.â • Â Â Â Â Â Â Â Â Â â ”Craig Miller, Ph.D. Â Â Â Â Â Â Â Â Â Â Â Â Â Â Chief Technology Officer for North America Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Dimension Data â œItâ ™s hard to protect yourself if you donâ ™t know what youâ ™re up against. This book has the details you need to know about how attackers find software holes and exploit themâ ”details that will help you secure your own systems.â • Â Â Â Â Â Â Â Â Â â ”Ed Felten, Ph.D.
Â Â Â Â Â Â Â Â Â Â Â Â Â Professor of Computer Science Â Â Â Â Â Â Â Â Â Â Â Â Â Princeton University â œIf you worry about software and application vulnerability, Exploiting Software is a must-read. This book gets at all the timely and important issues surrounding software security in a technical, but still highly readable and engaging way.â •Â Â Â Â Â Â Â Â Â â ”George Cybenko, Ph.D. Â Â Â Â Â Â Â Â Â Â Â Â Â Dorothy and Walter Gramm Professor of Engineering, DartmouthÂ Â Â Â Â Â Â Â Â Â Â Â Â Â Founding Editor-in-Chief, IEEE Security and Privacy Magazine â œExploiting Software is the best treatment of any kind that I have seen on the topic of software vulnerabilities.â •Â Â Â Â Â Â Â Â Â â ”From the Foreword by Aviel D. Rubin
Â Â Â Â Â Â Â Â Â Â Â Â Â Associate Professor, Computer ScienceÂ Â Â Â Â Â Â Â Â Â Â Â Â Â Technical Director, Information Security Institute, Johns Hopkins University How does software break? How do attackers make software break on purpose? Why are firewalls, intrusion detection systems, and antivirus software not keeping out the bad guys? What tools can be used to break software? This book provides the answers. Exploiting Software is loaded with examples of real attacks, attack patterns, tools, and techniques used by bad guys to break software. If you want to protect your software from attack, you must first learn how real attacks are really carried out. This must-have book may shock you--and it will certainly educate you.Getting beyond the script kiddie treatment found in many hacking books, you will learn about Why software exploit will continue to be a serious problem When network security mechanisms do not work Attack patterns Reverse engineering Classic attacks against server software Surprising attacks against client software Techniques for crafting malicious input The technical details of buffer overflows Rootkits Exploiting Software is filled with the tools, concepts, and knowledge necessary to break software.

Book Information

Paperback: 512 pages

Publisher: Addison-Wesley Professional; 1 edition (February 27, 2004)

Language: English

ISBN-10: 0201786958

ISBN-13: 978-0201786958

Product Dimensions: 6.9 x 1.1 x 9.2 inches

Shipping Weight: 2.1 pounds (View shipping rates and policies)

Average Customer Review: 4.3 out of 5 starsÂ Â See all reviewsÂ (29 customer reviews)

Best Sellers Rank: #795,645 in Books (See Top 100 in Books) #190 inÂ Books > Computers & Technology > Certification > CompTIA #305 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Testing #366 inÂ Books > Computers & Technology > Computer Science > Systems Analysis & Design

Customer Reviews

Anyone who’s been in network security long enough will tell you that the current state of products and `solutions’ to security problems are woefully inadequate.Firewalls, intrusion detection systems, content filters and anti-virus solutions are all reactive technologies, and as a result, they fail to address the primary cause of security vulnerabilities.This root cause is bad software. Viruses, worms and hackers exploit vulnerabilities in the design and logic of software applications to compromise, destroy and otherwise take control of important information. Once you accept this fact, you’ll realize that the only path to good security is to write better code.`Exploiting Software - How to Break Code’ is a book that fires up the hacker in me. It does not aim to teach you about the latest scanning tool, instead, it teaches you how to find and exploit vulnerabilities in systems. While many of the ideas in the book (such as the omnipresent buffer overflow) are not new, there is simply no literary comparison to the treatment given to them in this book.Application security is one of the highest regarded and specialized technical services in the security industry, and thus, finding people (let alone books) that delve in-depth into the topic is rare and refreshing. The first day I used this book, I was on an application security project. The target application was a distributed database application running on SQL server with a web front-end.I happened to have this book along with me, and while reading through it, the section on equivalent requests was something I hadn’t tried - sure enough, 20 minutes later I had full control of the application and a very good impression of this book.

Exploiting Software: How to Break Code 2012 International Plumbing Code (Includes International Private Sewage Disposal Code) (International Code Council Series) Rethinking Acrylic: Radical Solutions For Exploiting The World's Most Versatile Medium Charts Don't Lie: 10 Most Enigmatic Price Behaviors in Trading: How to Make Money Exploiting Price Actions (Price Action Mastery Book 2) Exploiting Earnings Volatility: An Innovative New Approach to Evaluating, Optimizing, and Trading Option Strategies to Profit from Earnings Announcements The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws Software Engineering Classics: Software Project Survival Guide/ Debugging the Development Process/ Dynamics of Software Development (Programming/General) Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection: Obfuscation, Watermarking, and Tamperproofing for Software Protection Break the Code: Cryptography for Beginners (Dover Children's Activity Books) The Code Book: How to Make It, Break It, Hack It, Crack It How to Code in 10 Easy Lessons: Learn how to design and code your very own computer game (Super Skills) Virtual Memory Source Code Secrets (Code Secrets V2) Swift: Programming, Master's Handbook; A TRUE Beginner's Guide! Problem Solving, Code, Data Science, Data Structures & Algorithms (Code like a PRO in ... engineering, r programming, iOS development) Ruby: Programming, Master's Handbook: A TRUE Beginner's Guide! Problem Solving, Code, Data Science, Data Structures & Algorithms (Code like a PRO in ... web design, tech, perl, ajax, swift, python,) Java Programming: Master's Handbook: A TRUE Beginner's Guide! Problem Solving, Code, Data Science, Data Structures & Algorithms (Code like a PRO in ... web design, tech, perl, ajax, swift, python) Php: Programming, Master's Handbook: A TRUE Beginner's Guide! Problem Solving, Code, Data Science, Data Structures & Algorithms (Code like a PRO in ... engineering, r programming, iOS development,) Python: Programming, Master's Handbook; A TRUE Beginner's Guide! Problem Solving, Code, Data Science, Data Structures & Algorithms (Code like a PRO ... engineering, r programming, iOS development) 2012 International Energy Conservation Code (International Code Council Series) 2009 International Energy Conservation Code: Softcover Version (International Code Council Series) DEWALT HVAC Code Reference:: Based on the 2015 International Mechanical Code (DEWALT Series)