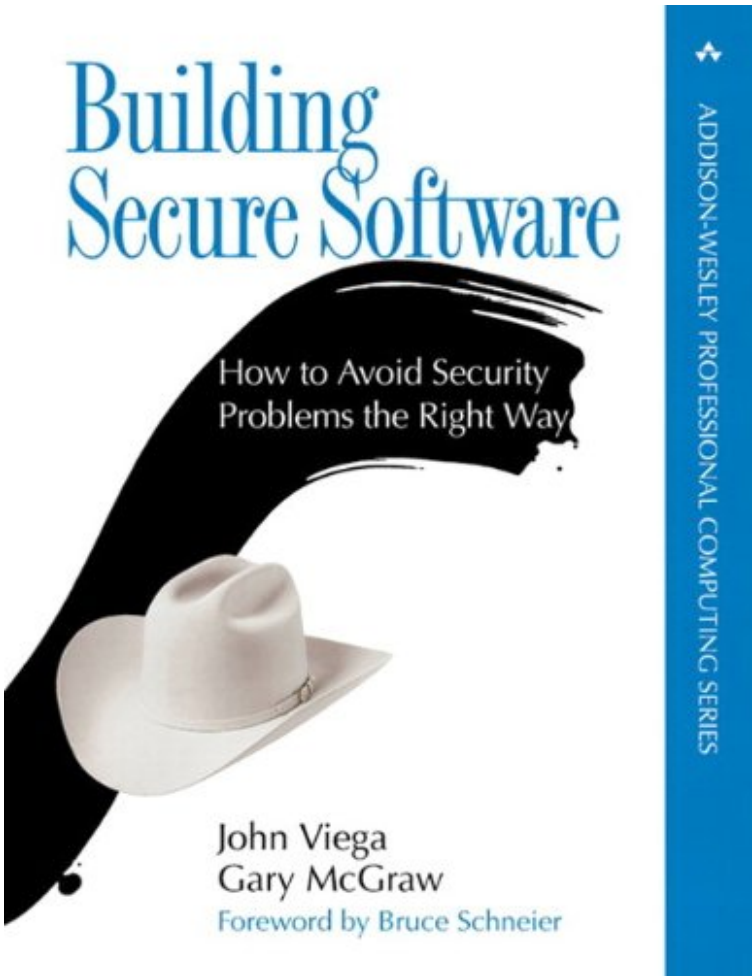
Building Secure Software: How to Avoid Security Problems the Right Way

Von John Viega, Gary R. McGraw
*ePub | *DOC | audiobook | ebooks | Download PDF*



Produktinformation -Verkaufsrang: #675954 in eBooksVerffentlicht am: 2001-09-24Erscheinungsdatum: 2001-09-24File Name: B003CW67YQ | File size: 29.Mb

Von John Viega, Gary R. McGraw : Building Secure Software: How to Avoid Security Problems the Right Way before purchasing it in order to gage whether or not it would be worth my time, and all praised Building Secure Software: How to Avoid Security Problems the Right Way:

KundenrezensionenHilfreichste Kundenrezensionen3 von 4 Kunden fanden die folgende Rezension hilfreich. Starting slow - Gaining speedVon Oliver KlingThe book starts with several chapters meant as an introduction and providing base knowledge for non-programmers. This introduction is too lenghty at least in my opinion (over 100 pages) and would have not really convinced me (if I have not been before) that the topic 'secure programming' is so important as it really is.If one have managed this slow start - the technical part (3/4 of the complete book) dives really into technical details. For C programmers very helpful (examples of other programming languages are rather rare to find). If you feel not that comfortable with C the book is probably harder to read and one have to dig out the essences of this book.The

content is well structered and most readers will not miss important chapters.Some statements are obviously discussible but the authors marked their personal opinion properly.Overall a good - very good book written by authors with indepth knowledge.0 von 0 Kunden fanden die folgende Rezension hilfreich. Guter berblick ber Sicherheitsaspekte in der SEVon amazinguserDas Buch bietet einen sehr guten berblick ber die Sicherheitsaspekte in und um Software. Speziell das leidige Thema der buffer overflows wird im Detail behandelt. Obwohl die Autoren versuchen das Buch sprachenbergreifend zu machen ist der Groteil der Beispiele an C geknpft - was aber weiter nicht stren sollte weil sich die meisten Beispiele leicht umzulegen sind.

KurzbeschreibungMost organizations have a firewall, antivirus software, and intrusion detection systems, all of which are intended to keep attackers out. So why is computer security a bigger problem today than ever before? The answer is simple--bad software lies at the heart of all computer security problems. Traditional solutions simply treat the symptoms, not the problem, and usually do so in a reactive way. This book teaches you how to take a proactive approach to computer security. Building Secure Software cuts to the heart of computer security to help you get security right the first time. If you are serious about computer security, you need to read this book, which includes essential lessons for both security professionals who have come to realize that software is the problem, and software developers who intend to make their code behave. Written for anyone involved in software development and usefrom managers to codersthis book is your first step toward building more secure software. Building Secure Software provides expert perspectives and techniques to help you ensure the security of essential software. If you consider threats and vulnerabilities early in the devel-opment cycle you can build security into your system. With this book you will learn how to determine an acceptable level of risk, develop security tests, and plug security holes before software is even shipped. Inside you'll find the ten guiding principles for software security, as well as detailed coverage of: Software risk management for security Selecting technologies to make your code more secure Security implications of open source and proprietary software How to audit software The dreaded buffer overflow Access control and password authentication Random number generation Applying cryptography Trust management and input Client-side security Dealing with firewalls Only by building secure software can you defend yourself against security breaches and gain the confidence that comes with knowing you won't have to play the "penetrate and patch" game anymore. Get it right the first time. Let these expert authors show you how to properly design your system; save time, money, and credibility; and preserve your customers' trust.KurzbeschreibungMost organizations have a firewall, antivirus software, and intrusion detection systems, all of which are intended to keep attackers out. So why is computer security a bigger problem today than ever before? The answer is simple--bad software lies at the heart of all computer security problems. Traditional solutions simply treat the symptoms, not the problem, and usually do so in a reactive way. This book teaches you how to take a proactive approach to computer security. Building Secure Software cuts to the heart of computer security to help you get security right the first time. If you are serious about computer security, you need to read this book, which includes essential lessons for both security professionals who have come to realize that software is the problem, and software developers who intend to make their code behave. Written for anyone involved in software development and usefrom managers to codersthis book is your first step toward building more secure software. Building Secure Software provides expert perspectives and techniques to help you ensure the security of essential software. If you consider threats and vulnerabilities early in the devel-opment cycle you can build security into your system. With this book you will learn how to determine an acceptable level of risk, develop security tests, and plug security holes before software is even shipped. Inside you'll find the ten guiding principles for software security, as well as detailed coverage of: Software risk management for security Selecting technologies to make your code more secure Security implications of open source and proprietary software How to audit software The dreaded buffer overflow Access control and password authentication Random number generation Applying cryptography Trust management and input Client-side security Dealing with firewalls Only by building secure software can you defend yourself against security breaches and gain the confidence that comes with knowing you won't have to play the "penetrate and patch" game anymore. Get it right the first time. Let these expert authors show you how to properly design your system; save time, money, and credibility; and preserve your customers' trust.Synopsis In the age of e-Business, information security is no longer a minor detail: it's at the heart of every business process and relationship. And software -- not firewalls, intrusion detection systems, or anything else -- is at the heart of most security problems. In Building Secure Software, two of the field's leading experts present a start-to-finish methodology for developing secure systems. They cover the entire software lifecycle, showing how to identify and respond to vulnerabilities as early in the process as possible, when security enhancements cost less -- and are more effective. In Part I, the authors focus on the security issues developers should face before writing any code, demonstrating how to integrate security into your entire software engineering practice. Part II focuses on implementation, showing developers how to avoid a wide range of common security problems. Viega and McGraw show how to determine acceptable levels of risk, develop effective security testing processes, and understand in advance how applications would behave in response to

an attack. The book contains extensive C-based source code examples.