
Hacking The Code Asp Net Web Application Security

Hacking the Code

A Programmer's Introduction to Visual Basic .NET

Programmer's Ultimate Security DeskRef

Professional DotNetNuke Module Programming

Microsoft Log Parser Toolkit

Building a VoIP Network with Nortel's Multimedia Communication Server 5100

Perfect Password

CD and DVD Forensics

Hacks, Leaks, and Revelations

How to Cheat at Securing SQL Server 2005

Pro ASP.NET Web API Security

Hacking Web Apps

The Basics of Web Hacking

Web Application Security

Hacking- The art Of Exploitation

Hacking the Code: ASP .NET Web Application Security

XSS Attacks

PHP Hacks

Asp.net Core 2.0 Mvc & Razor Pages for Beginners

Learning ASP.NET Core 2.0

ASP.NET Dynamic Data Unleashed

The Web Application Hacker's Handbook

InfoSecurity 2008 Threat Analysis

Software Piracy Exposed

ASP.NET Website Programming

Real World .NET, C#, and Silverlight

Sockets, Shellcode, Porting, and Coding: Reverse Engineering Exploits and Tool Coding for Security Professionals

Cryptography for Developers

Hacking Exposed Web Applications, Second Edition

Beginning Cryptography with Java

Advanced ASP.NET Core 3 Security

Network Security Assessment: From Vulnerability to Patch

ASP.NET Core Application Development

Hack the Stack

Hacking the Code

ASP.NET 2.0 MVP Hacks and Tips

Beginning DotNetNuke 4.0 Website Creation in VB 2005 with Visual Web Developer 2005 Express

Snort 2.1 Intrusion Detection, Second Edition

Visual Studio Hacks

Hacking Exposed: Malware and Rootkits

*Hacking The Code Asp Net Web
Application Security*

Downloaded from archive.imba.com by
guest

COOK ANDREWS

Hacking the Code Syngress

While many resources for network and IT security are available, detailed knowledge regarding modern web application security has been lacking—until now. This practical guide provides both offensive and defensive security concepts that software engineers can easily learn and apply. Andrew Hoffman, a senior security engineer at Salesforce, introduces three pillars of web application security: recon, offense, and defense. You'll learn methods for effectively researching and analyzing modern web applications—including those you don't have direct access to. You'll also learn how to break into web applications using the latest hacking techniques. Finally, you'll learn how to develop mitigations for use in your own web applications to protect against hackers. Explore common vulnerabilities plaguing today's web applications Learn essential hacking techniques attackers use to exploit applications Map and document web applications for which you don't have direct access Develop and deploy

customized exploits that can bypass common defenses Develop and deploy mitigations to protect your applications against hackers Integrate secure coding best practices into your development lifecycle Get practical tips to help you improve the overall security of your web applications

A Programmer's Introduction to Visual Basic .NET McGraw-Hill Osborne Media

This unique book offers readers invaluable information from the cream of the crop-Microsoft MVPs—who are now sharing undocumented hacks for the first time Packed with superlative advice on ASP, Microsoft's popular technology for Web sites, this book will help readers become more productive developers, find solutions to problems they thought unsolvable, and develop better applications During their many years of working with ASP.NET, Microsoft MVPs have answered thousands of questions, putting them in the distinctive position of knowing exactly what readers need to know Many of the hacks will apply to multiple versions of ASP.NET, not just 2.0 but 1.0 and 1.1 as well This book is also available as part of the 5-book ASP.NET 2.0 Wrox Box (ISBN: 0-470-11757-5). This 5-book set includes: Professional ASP.NET 2.0 Special Edition (ISBN: 0-470-04178-1) ASP.NET 2.0

Website Programming: Problem - Design - Solution (ISBN: 0764584642) Professional ASP.NET 2.0 Security, Membership, and Role Management (ISBN: 0764596985) Professional ASP.NET 2.0 Server Control and Component Development (ISBN: 0471793507) ASP.NET 2.0 MVP Hacks and Tips (ISBN: 0764597663) CD-ROM with more than 1000 pages of bonus chapters from 15 other .NET 2.0 and SQL Server(TM) 2005 Wrox books DVD with 180-day trial version of Microsoft(r) Visual Studio(r) 2005 Professional Edition

Programmer's Ultimate Security DeskRef Elsevier

This book details the development techniques needed to work within the DotNetNuke framework. It discusses the available methods to extend the framework, as well as the situations and rules governing when each respective extension model should be used. Additionally, the book stresses leveraging the framework in as many areas as possible, and ultimately using the framework to the advantage of the developer. Samples in the book are provided in both C# and Visual Basic (VB), and provides some excellent new features that are supported, starting with DotNetNuke 5.0.

Professional DotNetNuke Module Programming John Wiley & Sons

This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications. The topics covered include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under the alias "PortSwigger", Dafydd developed the popular Burp Suite of web application hack tools.

Microsoft Log Parser Toolkit John Wiley & Sons

User passwords are the keys to the network kingdom, yet most users choose overly simplistic passwords (like password) that anyone could guess, while system administrators demand impossible to remember passwords littered with obscure characters and random numerals. Every computer user must face the problems of password security. According to a recent British study, passwords are usually obvious: around 50 percent of computer users select passwords based on names of a family member, spouse, partner, or a pet. Many users face the problem of selecting strong passwords that meet corporate security requirements. Too often, systems reject user-selected passwords because they are not long enough or otherwise do not meet complexity requirements. This book teaches users how to select passwords that always meet complexity requirements. A typical computer user must remember dozens of passwords and they are told to make them all unique and never write them down. For most users, the solution is easy passwords that follow simple patterns. This book teaches users how to select strong passwords they can easily remember.* Examines the password problem from the perspective of the administrator trying to secure their network* Author Mark Burnett has accumulated and analyzed

over 1,000,000 user passwords and through his research has discovered what works, what doesn't work, and how many people probably have dogs named Spot* Throughout the book, Burnett sprinkles interesting and humorous password ranging from the Top 20 dog names to the number of references to the King James Bible in passwords

Building a VoIP Network with Nortel's Multimedia Communication Server 5100 Sams Publishing

Implement bulletproof e-business security the proven Hacking Exposed way Defend against the latest Web-based attacks by looking at your Web applications through the eyes of a malicious intruder. Fully revised and updated to cover the latest Web exploitation techniques, Hacking Exposed Web Applications, Second Edition shows you, step-by-step, how cyber-criminals target vulnerable sites, gain access, steal critical data, and execute devastating attacks. All of the cutting-edge threats and vulnerabilities are covered in full detail alongside real-world examples, case studies, and battle-tested countermeasures from the authors' experiences as gray hat security professionals. Find out how hackers use infrastructure and application profiling to perform reconnaissance and enter vulnerable systems Get details on exploits, evasion techniques, and countermeasures for the most popular Web platforms, including IIS, Apache, PHP, and ASP.NET Learn the strengths and weaknesses of common Web authentication mechanisms, including password-based, multifactor, and single sign-on mechanisms like Passport See how to excise the heart of any Web application's access controls through advanced session analysis, hijacking, and fixation techniques Find and fix input validation flaws, including cross-site scripting (XSS), SQL injection, HTTP response splitting, encoding, and special character abuse Get an in-depth presentation of the newest SQL injection techniques, including blind attacks, advanced exploitation through subqueries, Oracle exploits, and improved countermeasures Learn about the latest XML Web Services hacks, Web management attacks, and DDoS attacks, including click fraud Tour Firefox and IE exploits, as well as the newest socially-driven client attacks like phishing and adware *Perfect Password* Createspace Independent Publishing Platform Using Dynamic Data, ASP.NET developers can create powerful, datadriven sites with amazing speed and efficiency, eliminating massive amounts of manual coding. ASP.NET Dynamic Data Unleashed is the first complete, practical guide to Dynamic Data for every experienced ASP.NET developer. The author thoroughly demystifies Dynamic Data, helping developers understand exactly what they can do with the framework and make it more accessible than ever before. He provides tested code to solve a wide variety of problems, explains how and why that code works, and identifies key tradeoffs and alternatives. Packed with breakthrough techniques for improving developer productivity, this book combines a hands-on tutorial, "drill-down" explanations of advanced techniques, and real-world development scenarios. Detailed information on how to... Use Dynamic Data components to overcome common real-world user interface development challenges Understand how ASP.NET Dynamic Data builds on strengths of WebForms, Entity Framework, and LINQ Develop simple custom templates to dramatically reduce code duplication Generalize templates to leverage metadata and generate user interfaces dynamically Create web pages for data entry, data filtering, and diverse views of data Use Data Annotations to implement powerful validation logic Write simple, yet effective automated tests to systematically verify the business logic Create complex interaction rules that aren't limited by single entity objects or types Optimize I/O-bound business logic by implementing it with T-SQL constraints, stored procedures, and triggers Implement role-based security with dynamic UI trimming

Generate entire data-driven web applications, complete with CRUD pages, complex business rules, integrated navigation, and security Extend Dynamic Data to support advanced scenarios Decide when Dynamic Data should be used instead of or together with ASP.NET MVC

CD and DVD Forensics Elsevier

Incorporate best practices with ASP.NET Core security. This book includes security-related features available in the framework, and security topics rarely covered elsewhere. It digs deep into the ASP.NET Core 3.1 source code, explaining how something works (or how to fix a problem). The ASP.NET Core framework does a good job in preventing certain types of attacks from happening, but there are many more non-trivial projects that invariably require developers to think outside the box. For that, there is very little guidance on how to safely venture beyond the simple use cases. And worse, there is a lot of bad advice online on how to implement functionality, be it encrypting unsafely hard-code parameters that need to be generated at runtime, to articles that advocate for certain solutions that are vulnerable to obvious injection attacks. This book aims to train developers to avoid these problems. Unlike the vast majority of security books that are targeted to network administrators, system administrators, or managers, this book is targeted specifically to ASP.NET developers. The book begins by teaching developers how ASP.NET Core works behind the scenes, then talks about how various attacks are performed and how to prevent them. Finally, it dives into the concepts a developer needs to know to do some testing on their own without the help of a security professional. What You Will Learn Discern which attacks are easy to prevent in the framework and which are challenging Dig into ASP.NET Core 3.1 source code to understand how the security services work Establish a baseline for understanding how to design more secure software Properly apply cryptography in software development Take a deep dive into web security concepts Validate input in a way that allows legitimate traffic but blocks malicious traffic Understand parameterized queries and why they are so important to ASP.NET Core Fix issues in a well-implemented solution Know how logging works and its weaknesses in ASP.NET Core Incorporate security in every phase of the software development process Who This Book Is For Software developers who have experience creating websites in ASP.NET and want to know how to make their websites secure from hackers and security professionals who work with a development team that uses ASP.NET Core. A basic understanding of web technologies such as HTML, JavaScript, and CSS is assumed, as is knowledge of how to create a website, and how to read and write C#. You do not need knowledge of security concepts, even those that are often covered in ASP.NET Core documentation.

Hacks, Leaks, and Revelations Elsevier

Topics in this comprehensive guide include: why should users move to Visual Basic.NET; major VB.NET changes; building classes and assemblies with VB.NET; building Windows services with VB.NET; and upgrading VB6 Projects to VB.NET .

How to Cheat at Securing SQL Server 2005 O'Reilly Media

The Programmer's Ultimate Security DeskRef is the only complete desk reference covering multiple languages and their inherent security issues. It will serve as the programming encyclopedia for almost every major language in use. While there are many books starting to address the broad subject of security best practices within the software development lifecycle, none has yet to address the overarching technical problems of incorrect function usage. Most books fail to draw the line from covering best practices security principles to actual code implementation. This book bridges that gap and covers the most popular programming languages such as Java, Perl, C++, C#, and Visual Basic. *

Defines the programming flaws within the top 15 programming languages. * Comprehensive approach means you only need this book to ensure an application's overall security. * One book geared toward many languages.

Pro ASP.NET Web API Security No Starch Press

The first book published on deploying Voice Over IP (VoIP) products from Nortel Networks, the largest supplier of voice products in the world. This book begins with a discussion of the current protocols used for transmitting converged data over IP as well as an overview of Nortel's hardware and software solutions for converged networks. In this section, readers will learn how H.323 allows dissimilar communication devices to communicate with each other, and how SIP (Session Initiation Protocol) is used to establish, modify, and terminate multimedia sessions including VOIP telephone calls. This section next introduces the reader to the Multimedia Concentration Server 5100, and Nortel's entire suite of Multimedia Communications Portfolio (MCP) products. The remaining chapters of the book teach the reader how to design, install, configure, and troubleshoot the entire Nortel product line. If you are tasked with designing, installing, configuring, and troubleshooting a converged network built with Nortel's Multimedia Concentration Server 5100, and Multimedia Communications Portfolio (MCP) products, then this is the only book you need. It shows how you'll be able to design, build, secure, and maintaining a cutting-edge converged network to satisfy all of your business requirements. Also covers how to secure your entire multimedia network from malicious attacks

Hacking Web Apps Elsevier

HTML5 -- HTML injection & cross-site scripting (XSS) -- Cross-site request forgery (CSRF) -- SQL injection & data store manipulation -- Breaking authentication schemes -- Abusing design deficiencies -- Leveraging platform weaknesses -- Browser & privacy attacks.

The Basics of Web Hacking Elsevier

Learn how web applications can be built efficiently using ASP.NET Core 2.0 and related frameworks About This Book Get to grips with the new features and APIs introduced in ASP.NET Core 2.0 Leverage the MVC framework and Entity Framework Core 2 to build efficient applications Learn to deploy your web applications in new environments such as the cloud and Docker Who This Book Is For This book is for developers who would like to build modern web applications with ASP.NET Core 2.0. No prior knowledge of ASP.NET or .NET Core is required. However, basic programming knowledge is assumed. Additionally, previous Visual Studio experience will be helpful but is not required, since detailed instructions will guide through the samples of the book. This book can also help people, who work in infrastructure engineering and operations, to monitor and diagnose problems during the runtime of ASP.NET Core 2.0 web applications. What You Will Learn Set up your development environment using Visual Studio 2017 and Visual Studio Code Create a fully automated continuous delivery pipeline using Visual Studio Team Services Get to know the basic and advanced concepts of ASP.NET Core 2.0 with detailed examples Build an MVC web application and use Entity Framework Core 2 to access data Add Web APIs to your web applications using RPC, REST, and HATEOAS Authenticate and authorize users with built-in ASP.NET Core 2.0 features Use Azure, Amazon Web Services, and Docker to deploy and monitor your applications In Detail The ability to develop web applications that are highly efficient but also easy to maintain has become imperative to many businesses. ASP.NET Core 2.0 is an open source framework from Microsoft, which makes it easy to build cross-platform web applications that are modern and dynamic. This book will take you through all of the essential concepts in ASP.NET Core 2.0, so you can learn how to build powerful web applications. The book starts with a brief introduction to the

ASP.NET Core framework and the improvements made in the latest release, ASP.NET Core 2.0. You will then build, test, and debug your first web application very quickly. Once you understand the basic structure of ASP.NET Core 2.0 web applications, you'll dive deeper into more complex concepts and scenarios. Moving on, we'll explain how to take advantage of widely used frameworks such as Model View Controller and Entity Framework Core 2 and you'll learn how to secure your applications. Finally, we'll show you how to deploy and monitor your applications using Azure, AWS, and Docker. After reading the book, you'll be able to develop efficient and robust web applications in ASP.NET Core 2.0 that have high levels of customer satisfaction and adoption. Style and approach Start an exciting journey to building high performance web applications using ASP.NET Core 2.0 and MVC

Web Application Security Elsevier

A team of MVP authors guides you through the .NET 4 Framework. Written by a group of experienced MVPs, this unparalleled book delves into the intricate—and often daunting—world of .NET 4. Each author draws from a particular area of expertise to provide invaluable information on using the various .NET 4, C# 4, Silverlight 4, and Visual Studio tools in the real world. The authors break down the vast .NET 4 Framework into easily digestible portions to offer you a strong foundation on what makes .NET such a popular and successful framework for building a wide range of solutions. Breaks down the .NET 4 Framework into easily understandable sections. Features more than a dozen MVPs serving as authors, each of whom focuses on a particular area of expertise. Covers such topics as Windows Presentation Foundation, Silverlight 4, Windows Communication Foundation, ASP.NET performance, the entity framework, and more. Shares C# tips and tricks and .NET architecture best practices from a team of Microsoft MVPs. Real World .NET 4 and C# is the ultimate resource for discovering and understanding the .NET 4 Framework.

Hacking- The art Of Exploitation McGraw Hill Professional

An all-star cast of authors analyze the top IT security threats for 2008 as selected by the editors and readers of Infosecurity Magazine. This book, compiled from the Syngress Security Library, is an essential reference for any IT professional managing enterprise security. It serves as an early warning system, allowing readers to assess vulnerabilities, design protection schemes and plan for disaster recovery should an attack occur. Topics include Botnets, Cross Site Scripting Attacks, Social Engineering, Physical and Logical Convergence, Payment Card Industry (PCI) Data Security Standards (DSS), Voice over IP (VoIP), and Asterisk Hacking. Each threat is fully defined, likely vulnerabilities are identified, and detection and prevention strategies are considered. Wherever possible, real-world examples are used to illustrate the threats and tools for specific solutions.* Provides IT Security Professionals with a first look at likely new threats to their enterprise * Includes real-world examples of system intrusions and compromised data * Provides techniques and strategies to detect, prevent, and recover * Includes coverage of PCI, VoIP, XSS, Asterisk, Social Engineering, Botnets, and Convergence

Hacking the Code: ASP .NET Web Application Security John Wiley & Sons

The book is logically divided into 5 main categories with each category representing a major skill set required by most security professionals: 1. Coding - The ability to program and script is quickly becoming a mainstream requirement for just about everyone in the security industry. This section covers the basics in coding complemented with a slue of programming tips and tricks in C/C++, Java, Perl and NASL. 2. Sockets - The technology

that allows programs and scripts to communicate over a network is sockets. Even though the theory remains the same - communication over TCP and UDP, sockets are implemented differently in nearly ever language. 3. Shellcode - Shellcode, commonly defined as bytecode converted from Assembly, is utilized to execute commands on remote systems via direct memory access. 4. Porting - Due to the differences between operating platforms and language implementations on those platforms, it is a common practice to modify an original body of code to work on a different platforms. This technique is known as porting and is incredible useful in the real world environments since it allows you to not "recreate the wheel. 5. Coding Tools - The culmination of the previous four sections, coding tools brings all of the techniques that you have learned to the forefront. With the background technologies and techniques you will now be able to code quick utilities that will not only make you more productive, they will arm you with an extremely valuable skill that will remain with you as long as you make the proper time and effort dedications.*Contains never before seen chapters on writing and automating exploits on windows systems with all-new exploits. *Perform zero-day exploit forensics by reverse engineering malicious code. *Provides working code and scripts in all of the most common programming languages for readers to use TODAY to defend their networks.

XSS Attacks Elsevier

CD and DVD Forensics will take the reader through all facets of handling, examining, and processing CD and DVD evidence for computer forensics. At a time where data forensics is becoming a major part of law enforcement and prosecution in the public sector, and corporate and system security in the private sector, the interest in this subject has just begun to blossom. CD and DVD Forensics is a how to book that will give the reader tools to be able to open CDs and DVDs in an effort to identify evidence of a crime. These tools can be applied in both the public and private sectors. Armed with this information, law enforcement, corporate security, and private investigators will be able to be more effective in their evidence related tasks. To accomplish this the book is divided into four basic parts: (a) CD and DVD physics dealing with the history, construction and technology of CD and DVD media, (b) file systems present on CDs and DVDs and how these are different from that which is found on hard disks, floppy disks and other media, (c) considerations for handling CD and DVD evidence to both recover the maximum amount of information present on a disc and to do so without destroying or altering the disc in any way, and (d) using the InfinaDyne product CD/DVD Inspector to examine discs in detail and collect evidence.

- This is the first book addressing using the CD/DVD Inspector product in a hands-on manner with a complete step-by-step guide for examining evidence discs - See how to open CD's and DVD'd and extract all the crucial evidence they may contain
PHP Hacks Elsevier

Written by Microsoft's Log Parser developer, this is the first book available on Microsoft's popular yet undocumented log parser tool. The book and accompanying Web site contain hundreds of customized, working scripts and templates that system administrators will find invaluable for analyzing the log files from Windows Server, Snort IDS, ISA Server, IIS Server, Exchange Server, and other products. System administrators running Windows, Unix, and Linux networks manage anywhere from 1 to thousands of operating systems (Windows, Unix, etc.), Applications (Exchange, Snort, IIS, etc.), and hardware devices (firewalls, routers, etc.) that generate incredibly long and detailed log files of all activity on the particular application or device. This book will teach administrators how to use Microsoft's Log Parser to data mine all of the information available within these

countless logs. The book teaches readers how all queries within Log Parser work (for example: a Log Parser query to an Exchange log may provide information on the origin of spam, viruses, etc.). Also, Log Parser is completely scriptable and customizable so the book will provide the reader with hundreds of original, working scripts that will automate these tasks and provide formatted charts and reports detailing the results of the queries. - Written by Microsoft's sole developer of Log Parser, this is the first book available on the powerful yet completely undocumented product that ships with Microsoft's IIS, Windows Advanced Server 2003, and is available as a free download from the Microsoft Web site - This book and accompanying scripts will save system administrators countless hours by scripting and automating the most common to the most complex log analysis tasks

Asp.net Core 2.0 Mvc & Razor Pages for Beginners Apress
 Want to learn how to build ASP.NET Core 2.0 MVC and Razor Page Web Applications? Prerequisites: C# (Intermediate level; including Generics, Reflection and Object-Oriented Programming (OOP)) HTML5/CSS3 (Basic knowledge) This book is primarily aimed at developers who want to learn how to build ASP.NET Core 2.0 MVC and Razor Page applications. You should be an intermediate level C# developer with some experience in HTML5 and CSS3. The C# language won't be explained in any detail. You will learn ASP.NET Core 2.0 by building three applications. The first application will be built using an empty template, the second with the MVC template, and the third with Razor Pages. The goal with the first basic application is to get you familiar with ASP.NET Core 2.0 by adding middleware and services one piece at a time. Then you will create a solution with three projects; the first project will be used to create a shared database with Entity Framework Core 2.0, the second project is a MVC application for the regular user interface, and the third project is an administrator user interface built with Razor Pages. This solution is a video course website, where users can register to gain access to video courses and administrators can add and modify course content and users. If you are already familiar with MVC 5 or ASP.NET Core 1.0/1.1, the content in this book can get you started with ASP.NET Core 2.0 in a fast, no-fluff way. It's important to mention that this book is practical and tactical, where you will learn as you progress through the modules and build real web applications in the process. To spare you countless

pages of fluff (filler material), only valuable information, pertinent to the task at hand, is discussed. The benefit is a shorter and more condensed book, which will save you time and give you a more enjoyable experience. This experience is something you can put in your CV when applying for a job or a consultant position, or when negotiating a higher salary. Technologies, frameworks and languages you will use: Visual Studio 2017 ASP.NET Core 2.0 MVC and Razor Pages (new in ASP.NET 2.0) Services (To provide your own functionality as a reusable service) Middleware (To provide you own functionality to HTTP Request pipeline) Entity Framework (To crate and communicate with a database) View Component (To render data in the _Layout view with model data) Dependency Injection (To inject objects into constructors) Bootstrap (Used for styling and to create a responsive design) LINQ (To query the database) Tag Helper (to clean up the HTML and enable re-use) HTML Helper methods (to clean up your HTML and enable re-use) Partial views (to clean up your views and enable re-use) Bower and NuGet (To install necessary libraries) What you will implement: A web application from an empty template An MVC web application using a template An Razor Page web application using a template A data-layer project referenced from the MVC and Razor Page applications I hope you love the book! Sincerely, Jonas Fagerberg Now click the Buy button and start reading the book.

Learning ASP.NET Core 2.0 Microsoft Press

This book is about software piracy--what it is and how it's done. Stealing software is not to be condoned, and theft of intellectual property and copyright infringement are serious matters, but it's totally unrealistic to pretend that it doesn't happen. Software piracy has reached epidemic proportions. Many computer users know this, the software companies know this, and once you've read the Introduction to this book, you'll understand why. Seeing how widespread software piracy is, learning how it's accomplished, and particularly how incredibly easy it is to do might surprise you. This book describes how software piracy is actually being carried out. - This book is about software piracy-- what it is and how it's done - This is the first book ever to describe how software is actually stolen and traded over the internet - Discusses security implications resulting from over 1/2 of the internet's computers running illegal, unpatched, pirated software

Related with Hacking The Code Asp Net Web Application Security:

- Family Feud Hosts History : [click here](#)