1.	Record Nr.	UNINA9910784271203321
	Autore	Cross Michael
	Titolo	Developer's guide to web application security [[electronic resource] /] / Michael Cross
	Pubbl/distr/stampa	Rockland, MA, : Syngress Publishing, c2007
	ISBN	1-281-06021-6 9786611060213 0-08-050409-4
	Descrizione fisica	1 online resource (513 p.)
	Disciplina	005.8
	Soggetti	Computer networks - Security measures Computer security Web sites - Security measures
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Front Cover; Developer's Guide to Web Application Security; Copyright Page; Contents; Chapter 1. Hacking Methodology; Introduction; A Brief History of Hacking; What Motivates a Hacker?; Understanding Current Attack Types; Recognizing Web Application Security Threats; Preventing Break-Ins by Thinking like a Hacker; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 2. How to Avoid Becoming a Code Grinder; Introduction; What Is a Code Grinder?; Thinking Creatively when Coding; Security from the Perspective of a Code Grinder; Building Functional and Secure Web Applications SummarySolutions Fast Track; Frequently Asked Questions; Chapter 3. Understanding the Risk Associated with Mobile Code; Introduction; Recognizing the Impact of Mobile Code Attacks; Identifying Common Forms of Mobile Code; Protecting Your System from Mobile Code Attacks; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 4. Vulnerable CGI Scripts; Introduction; What Is a CGI Script, and What Does It Do?; Break-Ins Resulting from Weak CGI Scripts; Languages for Writing CGI Scripts; Advantages of Using CGI Scripts; Rules for Writing Secure CGI Scripts; Summary Solutions Fast TrackFrequently Asked Questions; Chapter 5. Hacking

Techniques and Tools; Introduction; A Hacker's Goals; The Five Phases of Hacking; Defacing Web Sites; Social Engineering; The Intentional "Back Door"Attack; Exploiting Inherent Weaknesses in Code or Programming Environments; The Tools of the Trade; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 6. Code Auditing and Reverse Engineering; Introduction; How to Efficiently Trace through a Program; Auditing and Reviewing Selected Programming Languages; Looking for Vulnerabilities; Pulling It All Together; Summary

Solutions Fast TrackFrequently Asked Questions; Chapter 7. Securing Your Java Code; Introduction; Overview of the Java Security Architecture; How Java Handles Security; Potential Weaknesses in Java; Coding Functional but Secure Java Applets; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 8. Securing XML; Introduction; Defining XML; Creating Web Applications Using XML; The Risks Associated with Using XML; Securing XML; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 9. Building Safe ActiveX Internet Controls; Introduction

Dangers Associated with Using ActiveXMethodology for Writing Safe ActiveX Controls; Securing ActiveX Controls; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 10. Securing ColdFusion; Introduction; How Does ColdFusion Work?; Preserving ColdFusion Security; ColdFusion Application Processing; Risks Associated with Using ColdFusion; Summary; Solutions Fast Track; Frequently Asked Questions; Chapter 11. Developing Security-Enabled Applications; Introduction; The Benefits of Using Security-Enabled Applications; Types of Security Used in Applications; Reviewing the Basics of PKI Using PKI to Secure Web Applications

Sommario/riassunto

Over 75% of network attacks are targeted at the web application layer. This book provides explicit hacks, tutorials, penetration tests, and step-by-step demonstrations for security professionals and Web application developers to defend their most vulnerable applications.

This book defines Web application security, why it should be addressed earlier in the lifecycle in development and quality assurance, and how it differs from other types of Internet security. Additionally, the book examines the procedures and technologies that are essential to developing, penetration testing and releasi