1. Record Nr. UNINA9910164016003321

Autore	Harwood Mike
Titolo	Internet security : how to defend against attackers on the Web / / Mike Harwood
Pubbl/distr/stampa	Burlington, MA : , : Jones & Bartlett Learning, , [2016] ©2016
ISBN	1-284-09064-7
Edizione	[Second edition.]
Descrizione fisica	1 online resource (1 volume) : illustrations
Collana	Jones & Bartlett Learning Information systems security & assurance series
Altri autori (Persone)	HarwoodMike
Disciplina	302.30285
Soggetti	Online social networks - Security measures Application software - Security measures Internet - Security measures World Wide Web - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Originally published under title: Security strategies in Web applications and social networking, by Jones & Bartlett, 2011.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Title Page -- Copyright -- Contents -- Preface -- Acknowledgments -- Part One Evolution of Computing, Risks, and Social Networking -- Chapter 1 From Mainframe to Client/Server to World Wide Web -- The Evolution of Data Processing -- Understanding Data, Data Processing, and Information -- 1900s and Rapid Growth -- Mainframe Computers -- Client/Server Computing -- Distributed Computing on a Network -- Transformation of Brick-and-Mortar Businesses to E-commerce Businesses -- E-commerce Today -- The World Wide Web Revolution -- Pre-Internet Era -- Groupware and Gopher -- Emergence of the World Wide Web -- The Changing States of the World Wide Web -- Web 1.0 -- Web 2.0 -- Web 3.0 -- Introducing the Internet of Things (IoT) -- Cloud Computing and Virtualization -- Cloud Computing -- Virtualization -- Chapter Summary -- key concepts and terms -- Chapter 1 Assessment -- Chapter 2 Security Considerations for Small Businesses -- The Evolution of Business from Brick and Mortar to the Web -- E-commerce: A Brick-and-Mortar Model -- Customer-Focused E-commerce -- Emerging Trend: Distributed E-commerce -- The Process

of Transformation into an E-business -- Managing and Security the Customer Life Cycle -- Highly Available and Secure Web Site Hosting -- E-commerce and Enhanced Customer-Service Delivery -- One-Way Communication -- Limited Two-Way Communication -- Full Two-Way Communication -- E-businesss with Integrated Applications -- Risks, Threats, and Vulnerabilities for Business Web Sites -- Connecting to the Internet Means Connecting to the Outside World -- The Risks of Handling Revenues Online -- Credit, Charge, and Debit Cards -- Electronic Cash and Wallets -- Vulnerabilities of Web-Enabled Applications -- Managing the Risks Inherent in Unsecure Systems -- System and Protocol Security -- Securing IP Communications. Managing Application and Coding Security -- Using Service Packs -- Telecommuting and Secure Access for Remote Employees -- Chapter Summary -- Key Concepts and Terms -- Chapter 2 Assessment -- Chapter 3 Security Considerations for Home and Personal Online Use -- Common Security Terms and Threats -- Social Engineering -- Phishing -- Identity Theft -- Malware and Ransomware -- Cookies -- Securing Common Online Activities -- Banking and Investing -- Shopping Online -- Social Networking -- Online Gaming -- Protecting Against E-mail Scams -- The OWASP Top 10 Privacy Risks Project -- 1. Web Application Vulnerabilities -- 2. Operator-Sided Data Leakage -- 3. Insufficient Data Breach Response -- 4. Insufficient Deletion of Personal Data -- 5. Non-transparent Policies, Terms, and Conditions -- 6. Collection of Data Not Required for the Primary Purpose -- 7. Sharing of Data with Third Party -- 8. Outdated Personal Data -- 9. Missing or Insufficient Session Expiration -- 10. Unsecure Data Transfer -- Chapter Summary -- Key Concepts and Terms -- Chapter 3 Assessment -- Part Two Secure Web-Enabled Application Deployment and Social Networking -- Chapter 4 Mitigating Risk When Connecting to the Internet -- Threats When Connecting to the Internet -- Risks and Threats -- Vulnerabilities and Exploits -- Perpetrators -- Web Site Hosting -- External Web Hosting -- Internal Web Hosting -- Domain Name Server -- The Seven Domains of a Typical IT Infrastructure -- Protecting Networks in the LAN-to-WAN Domain -- Perimeter Defense Strategies -- Firewalls -- Demilitarized Zones (DMZs) -- Proxy Servers -- Intrusion Detection Systems and Intrusion Protection Systems -- Best Practices for Connecting to the Internet -- Chapter Summary -- Key Concepts and Terms -- Chapter 4 Assessment -- Chapter 5 Mitigating Web Site Risks, Threats, and Vulnerabilities.
Who Is Coming to Your Web Site? -- Whom Do You Want to Come to Your Web Site? -- Accepting User Input on Your Web Site -- Forums -- Web Site Feedback Forms -- Online Surveys -- The Open Web Application Security Project Top 10 Threats -- 1. Injection -- 2. Broken Authentication and Session Management -- 3. Cross-Site Scripting (XSS) -- 4. Unsecure Direct Object References -- 5. Security Misconfigurations -- 6. Sensitive Data Exposure -- 7. Missing Function Level Access Control -- 8. Cross-Site Request Forgery (CSRF) -- 9. Using Components with Known Vulnerabilities -- 10. Unvalidated Redirects and Forwards -- Additional Web Threats Not in the Top 10 -- Malicious File Execution -- Information Leakage and Improper Error Handling -- Unsecure Cryptographic Storage -- Unsecure Communications -- Failure to Restrict URL Access -- Best Practices for Mitigating Known Web Application Risks, Threats, and Vulnerabilities -- Chapter Summary -- Key Concepts and Terms -- Chapter 5 assessment -- Chapter 6 Introducing the Web Application Security Consortium (WASC) -- The Threats to Web Application Security -- Common Web Site Attacks -- Abuse of Functionality -- Brute-Force Attacks -- Buffer Overflow -- Content Spoofing -- Credential/Session

Prediction -- Cross-Site Scripting -- Cross-Site Request Forgery -- Denial of Service -- Fingerprinting -- Format String -- HTTP Response Smuggling -- HTTP Response Splitting -- HTTP Request Smuggling -- HTTP Request Splitting -- Integer Overflows -- LDAP Injection -- Mail Command Injection -- Null Byte Injection -- OS Commanding -- Path Traversal -- Predictable Resource Location -- Remote File Inclusion (RFI) -- Routing Detour -- Session Fixation -- SOAP Array Abuse -- SSI Injection -- SQL Injection -- URL Redirector Abuse -- XPath Injection -- XML Attribute Blowup -- XML External Entities -- XML Entity Expansion -- XML Injection.
XQuery Injection -- Common Web Site Weaknesses -- Application Misconfiguration -- Directory Indexing -- Improper File System Permissions -- Improper Input Handling -- Improper Output Handling -- Information Leakage -- Unsecure Indexing -- Insufficient Anti-Automation -- Insufficient Authentication -- Insufficient Authorization -- Insufficient Password Recovery -- Insufficient Process Validation -- Insufficient Session Expiration -- Insufficient Transport Layer Protection -- Server Misconfiguration -- Best Practices for Mitigating Web Attacks -- Best Practices for Mitigating Weaknesses -- Chapter Summary -- Key Concepts and Terms -- Chapter 6 Assessment -- Chapter 7 Securing Web Applications -- When Your Application Requires User Input into Your Web Site -- Get to Know Your Syntax with Request for Comments (RFC) -- Technologies and Systems Used to Make a Complete Functional Web Site -- Hypertext Markup Language (HTML) -- Common Gateway Interface (CGI) Script -- JavaScripting -- SQL Database Back-End -- Your Development Process and the Software Development Life Cycle (SDLC) -- Designing a Layered Security Strategy for Web Sites and Web Applications -- Incorporating Security Requirements Within the SDLC -- Systems Analysis Stage -- Designing Stage -- Implementation Stage -- Testing Stage -- Acceptance and Deployment Stage -- Maintenance -- Using Secure and Unsecure Protocols -- How Secure Sockets Layer Works -- SSL Encryption and Hash Protocols -- Selecting an Appropriate Access Control Solution -- Discretionary Access Control -- Mandatory Access Control -- Rule-Based Access Control -- Role-Based Access Control -- Create Access Controls That Are Commensurate with the Level of Sensitivity of Data Access or Input -- Best Practices for Securing Web Applications -- Chapter Summary -- Key Concepts and Terms -- Chapter 7 assessment.
Chapter 8 Mitigating Web Application Vulnerabilities -- Causes of Web Application Vulnerabilities -- Authentication -- Input Validation -- Session Management -- Vulnerabilities Are Caused by Non-Secure Code in Software Applications -- Developing Policies to Mitigate Vulnerabilities -- Implementing Secure Coding Best Practices -- Incorporating HTML Secure Coding Standards and Techniques -- Incorporating JavaScript Secure Coding Standards and Techniques -- Incorporating CGI Form and SQL Database Access Secure Coding Standards and Techniques -- SQL Database Security -- Implementing Software Development Configuration Management and Revision-Level Tracking -- Revision-Level Tracking -- Best Practices for Mitigating Web Application Vulnerabilities -- Chapter Summary -- Key Concepts and Terms -- Chapter 8 assessment -- Chapter 9 Maintaining PCI DSS Compliance for E-commerce Web Sites -- Credit Card Transaction Processing -- Batch Processing -- Real-Time Processing -- What Is the Payment Card Industry Data Security Standard? -- If PCI DSS Is Not a Law, Why Do You Need to Be in Compliance? -- Designing and Building Your E-commerce Web Site with PCI DSS in Mind -- What Does a PCI DSS Security Assessment Entail? -- Scope of Assessment --

Instructions and Content for Report on Compliance -- Detailed PCI DSS Requirements and Security Assessment Procedures -- Security Assessment Marking Procedure -- Best Practices to Mitigate Risk for E-commerce Web Sites with PCI DSS Compliance -- Build and Maintain a Secure Network -- Protect Cardholder Data -- Maintain a Vulnerability Management Program -- Implement Strong Access Control Measures -- Regularly Monitor and Test Networks -- Maintain an Information Security Policy -- Chapter Summary -- Key Concepts and Terms -- Chapter 9 Assessment -- Chapter 10 Testing and Quality Assurance for Production Web Sites.
Development and Production Software Environments.

Sommario/riassunto

The Second Edition of Security Strategies in Web Applications and Social Networking provides an in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, this book provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking and discusses how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the internet. Using examples and exercises, this book incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications.