1.

Record Nr.	UNISOBSOBE00059675
Autore	Bembo, Pietro
Titolo	Le prose di messer Pietro Bembo cardinale nelle quali si ragiona della volgar lingua scritte al cardinal De' Medici, ... divise in tre libri
Pubbl/distr/stampa	In Venezia : appresso Guglielmo Zerletti, 1761
Descrizione fisica	312 p. ; 12º
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Illustrazioni calcografiche sul frontespizio Segnatura: A-N^{12}

2.

Record Nr.	UNINA9910827570103321
Autore	Chell Dominic
Titolo	The mobile application hacker's handbook / / Dominic Chell [and three others]
Pubbl/distr/stampa	Indiapolis, Indiana : , : Wiley, , 2015 ©2015
ISBN	1-118-95852-7 1-118-95851-9
Edizione	[1st edition]
Descrizione fisica	1 online resource (1564 p.)
Disciplina	005.8
Soggetti	iPhone (Smartphone) - Security measures iPhone (Smartphone) - Mobile apps Android (Electronic resource) - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Introduction; Overview of This Book; How This Book Is Organized; Who Should Read This Book; Tools You Will Need; What's on

the Website; Chapter 1 Mobile Application (In)security; The Evolution of Mobile Applications; Mobile Application Security; Summary; Chapter 2 Analyzing iOS Applications; Understanding the Security Model; Understanding iOS Applications; Jailbreaking Explained; Understanding the Data Protection API; Understanding the iOS Keychain; Understanding Touch ID; Reverse Engineering iOS Binaries; Summary; Chapter 3 Attacking iOS Applications
Introduction to Transport Security Identifying Insecure Storage; Patching iOS Applications with Hopper; Attacking the iOS Runtime; Understanding Interprocess Communication; Attacking Using Injection; Summary; Chapter 4 Identifying iOS Implementation Insecurities; Disclosing Personally Identifiable Information; Identifying Data Leaks; Memory Corruption in iOS Applications; Summary; Chapter 5 Writing Secure iOS Applications; Protecting Data in Your Application; Avoiding Injection Vulnerabilities; Securing Your Application with Binary Protections; Summary; Chapter 6 Analyzing Android Applications
Creating Your First Android Environment Understanding Android Applications; Understanding the Security Model; Reverse-Engineering Applications; Summary; Chapter 7 Attacking Android Applications; Exposing Security Model Quirks; Attacking Application Components; Accessing Storage and Logging; Misusing Insecure Communications; Exploiting Other Vectors; Additional Testing Techniques; Summary; Chapter 8 Identifying and Exploiting Android Implementation Issues; Reviewing Pre-Installed Applications; Exploiting Devices; Infiltrating User Data; Summary; Chapter 9 Writing Secure Android Applications
Principle of Least Exposure Essential Security Mechanisms; Advanced Security Mechanisms; Slowing Down a Reverse Engineer; Summary; Chapter 10 Analyzing Windows Phone Applications; Understanding the Security Model; Understanding Windows Phone 8.x Applications; Building a Test Environment; Analyzing Application Binaries; Summary; Chapter 11 Attacking Windows Phone Applications; Analyzing for Data Entry Points; Attacking Transport Security; Attacking WebBrowser and WebView Controls; Identifying Interprocess Communication Vulnerabilities; Attacking XML Parsing; Attacking Databases
Attacking File Handling Patching .NET Assemblies; Summary; Chapter 12 Identifying Windows Phone Implementation Issues; Identifying Insecure Application Settings Storage; Identifying Data Leaks; Identifying Insecure Data Storage; Insecure Random Number Generation; Insecure Cryptography and Password Use; Identifying Native Code Vulnerabilities; Summary; Chapter 13 Writing Secure Windows Phone Applications; General Security Design Considerations; Storing and Encrypting Data Securely; Secure Random Number Generation; Securing Data in Memory and Wiping Memory; Avoiding SQLite Injection
Implementing Secure Communications

Sommario/riassunto

See your app through a hacker's eyes to find the real sources of vulnerability   The Mobile Application Hacker's Handbook is a comprehensive guide to securing all mobile applications by approaching the issue from a hacker's point of view. Heavily practical, this book provides expert guidance toward discovering and exploiting flaws in mobile applications on the iOS, Android, Blackberry, and Windows Mobile platforms. You will learn a proven methodology for approaching mobile application assessments, and the techniques used to prevent, disrupt, and remediate the various types of attacks.
Coverage