

**TABLE OF CONTENTS**

<b>INTRODUCTION</b>	1
<b>PREFACE</b>	3
<b>WHAT THIS BOOK COVERS</b>	4
<b>WHAT YOU NEED FOR THIS BOOK</b>	6
<b>CHAPTER 1 GETTING STARTED WITH ANDROID SECURITY</b>	7
• Introduction	9
• Introduction to Android	9
• Digging deeper into Android	13
• Sandboxing and the permission model	19
• Application signing	25
• Android Startup Process	27
• Summary	30
<b>CHAPTER 2 PREPARING THE BATTLEFIELD</b>	31
• Introduction	33
• Setting up the development environment	33
• Creating an Android virtual Device	38
• Useful utilities for Android Pentest	40
• Android Debug Bridge	41
• Burp Suite	44
• APK Tool	46
• Summary	48

**TABLE OF CONTENTS**

<b>CHAPTER 3 REVERSING AND AUDITING ANDROID APPS</b>	49
• Introduction	51
• Android Application Teardown	51
• Reversing an Android Application	55
• Using APKTool to Reverse an Android Application	57
• Auditing Android Applications	59
• Content Provider Leakage	60
• Insecure File Storage	66
• Path Traversal Vulnerability or Local File Inclusion	67
• Client-Side Injection Attacks	68
• OWASP top 10 Vulnerabilities for Mobiles	70
• Summary	74
<b>CHAPTER 4 TRAFFIC ANALYSIS FOR ANDROID DEVICES</b>	75
• Introduction	77
• Android Traffic Interception	77
• Ways to analyze Android traffic	78
• Passive Analysis	79
• Active Analysis	84
• HTTPS Proxy Interception	87
• Other ways to intercept SSL Traffic	90
• Extracting sensitive files with packet capture	92
• Summary	94
<b>CHAPTER 5 ANDROID FORENSICS</b>	95
• Introduction	97
• Types of Forensics	97
• Filesystems	98
• Android Filesystem partitions	99
• Using dd to extract data	100
• Using a custom recovery image	103
• Using Andriller to extract an application's data	106
• Using ALogical to extract contacts, calls, and text messages	109
• Dumping application databases manually	111
• Logging the logcat	116

**TABLE OF CONTENTS**

• Using backup to extract an application's data	117
• Summary	120
<b>CHAPTER 6 PLAYING WITH SQLITE</b>	121
• Introduction	123
• Understanding SQLite in depth	123
• Analyzing a simple application using SQLite	124
• Security vulnerability	128
• Summary	132
<b>CHAPTER 7 LESSER-KNOWN ANDROID ATTACKS</b>	133
• Introduction	135
• Android WebView Vulnerability	135
• Using WebView in the application	135
• Identifying the vulnerability	136
• Infecting legitimate APKs	140
• Vulnerabilities in ad libraries	142
• Cross-Application Scripting in Android	143
• Summary	145
<b>CHAPTER 8 ARM EXPLOITATION</b>	147
• Introduction	149
• Introduction to ARM architecture	149
• Execution modes	151
• Setting up the environment	151
• Simple stack-based buffer overflow	154
• Return-oriented programming	158
• Android root exploits	160
• Summary	162