

۱۳۰۶۵۵۵

تست نفوذ اندروید

ترجمه و تالیف:

مهندس علیرضا تاضی سیدی

دکتر زهرا مهربان

www.ketab.ir

سرناسه	قاضی سعیدی، علیرضا، ۱۳۶۲
عنوان و نام پدیدآور	تست نفوذ اندروید/ ترجمه و تألیف علیرضا قاضی سعیدی، زهرا مهربان
مشخصات نشر	تهران: انتشارات ناقوس، ۱۳۹۳.
مشخصات ظاهری	۱۱۶ ص.: مصور، جدول: ۲۹×۲۲ س.م.
شابک	۳-۷۳۳-۳۷۷-۹۶۴-۹۷۸ : بها : ۱۰۰۰۰۰۰۰۰ ریال
وضعیت فهرست نویسی: فیا	
یادداشت	کتاب حاضر برگرفته از دو کتاب "XDA Developers' Android Hacker's Toolkit..." و "Learning Pentesting for Android Devices..."
موضوع	اندروید (منبع الکترونیکی) — دستنامه‌ها
موضوع	نرم افزار کاربردی — طراحی و توسعه
موضوع	تلفن های هوشمند — برنامه نویسی
شناسه افزوده	مهربان، زهرا، ۱۳۴۲
رده بندی کتبی	۱۳۹۳ ق ۲ ۱۸۴ الف / ۷۶ / ۷۶ QAV۶
رده بندی دیجی	۰۰۵/۲۷۶۸
شماره کتابشناسی ملی	۳۶۸۰۵۴۴



برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoospress.com

انتشارات ناقوس

چاپ اول

S.M.S : ۳۰۰۰۴۵۲۳۲۲

کلیه حقوق را برای سرمایه گذار محفوظ است. تیر تمامی یا قسمتی از این اثر به صورت حروفچینی یا چاپ مجدد، چاپ افست، پلی کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

نام کتاب : تست نفوذ اندروید

ناشر : انتشارات ناقوس

ترجمه و تألیف : علیرضا قاضی سعیدی و زهرا مهربان

چاپ اول : ۱۳۹۳

تیراژ : ۳۰۰ جلد

چاپ و صحافی : نارنجستان

حروفنگار و صفحه آرا : واحد تولید

قیمت : ۱۰۰۰۰۰۰۰ ریال

شابک : ۳-۷۳۳-۳۷۷-۹۶۴-۹۷۸

ISBN : 978-964-377-733-3

مراکز پخش:

۱- انتشارات ناقوس: میدان انقلاب، خیابان کارگر جنوبی، خیابان روانمهر، کوچه دولتشاهی، پلاک ۲

تلفن و فاکس: ۰۲۱-۶۶۴۰۸۵۲۰ - ۶۶۴۰۱۷۹۸ - ۶۶۴۱۷۰۷۲ - ۶۶۴۶۶۷۹۳

۲- کتابفروشی الیاس: خیابان انقلاب، نبش فروردین تلفن: ۰۲۱-۶۶۴۰۵۰۸۴

۳- کتابفروشی گلریزان، ضلع جنوب شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۰۲۱-۶۶۹۷۶۲۳۰

فهرست مطالب

فصل اول ۱	
۱.۱	امنیت در اندروید
۱.۲	مقدمه‌ای در خصوص اندروید
۱.۳	شناخت عمیق‌تر از اندروید
۱.۴	جعبه شنی و Permission Model
۱.۵	امضای برنامه کاربردی در اندروید
۱.۶	پروژه Startup در اندروید
فصل دوم	
۲.۱	راه اندازی محیط تست اندروید
۲.۲	راه‌اندازی محیط توسعه اندروید
۲.۳	راه‌اندازی یک Android Virtual Device
۲.۴	ابزارهای مفید برای تست نفوذ اندروید
۲.۵	Android Debug Bridge
۲.۶	Burp Suite
۲.۷	APKTool
فصل سوم	
۳.۱	مهندسی معکوس و ارزیابی برنامه‌های کاربردی اندروید
۳.۲	تقسیم‌بندی برنامه‌های کاربردی اندرویدی
۳.۳	مهندسی معکوس برنامه‌های کاربردی اندرویدی
۳.۴	استفاده از APKTool برای مهندسی معکوس برنامه‌های کاربردی اندرویدی
۳.۵	ارزیابی برنامه‌های کاربردی اندرویدی
۳.۶	نشت Content Provider
۳.۷	ذخیره ناایمن فایل‌ها
۳.۸	آسیب‌پذیری پیمایش مسیر یا Local file inclusion
۳.۹	حملات تزریق client-side
۳.۱۰	آسیب‌پذیری برای دستگاه‌های موبایل از دید OWASP
۳.۱۱	کنترل ضعیف سمت سرور
۳.۱۲	ذخیره ناایمن اطلاعات
۳.۱۳	حفاظت ناکافی در لایه انتقال

۵۸	نشست ناخواسته اطلاعات	۳.۱۴
۵۸	ضعف در Authentication و Authorization	۳.۱۵
۵۸	رمزنگاری شکسته شده	۳.۱۶
۵۸	تزریق Client-side	۳.۱۷
۵۸	تصمیمات امنیتی از طریق ورودی‌های غیر واقعی	۳.۱۸
۵۸	Session Handling نامناسب	۳.۱۹
۵۹	فقدان حفاظت‌های بایزری	۳.۲۰
۶۱	فصل چهارم	
۶۲	آنالیز ترافیک در دستگاه‌های اندرویدی	۴.۱
۶۲	ریافت ترافیک اندروید	۴.۲
۶۲	راه‌های آنالیز ترافیک اندروید	۴.۳
۶۳	آنالیز سیو	۴.۴
۶۴	آنالیز اکتیر	۴.۵
۶۶	استخراج اطلاعات براساس استفاده از شنود ترافیک شبکه	۴.۶
۶۹	فصل پنجم	
۷۰	انواع Forensics	۵.۱
۷۰	اکتساب منطقی	۵.۲
۷۰	اکتساب فیزیکی	۵.۳
۷۰	انواع فایل سیستم	۵.۴
۷۱	پارتیشن‌های فایل سیستم اندروید	۵.۵
۷۲	استفاده از dd برای استخراج اطلاعات	۵.۶
۷۵	استفاده از Andriller برای استخراج اطلاعات برنامه کاربردی	۵.۷
۷۷	استفاده از AFlogic برای استخراج Contact ها، تماس‌ها و Message ها	۵.۸
۷۹	بدست آوردن پایگاه داده برنامه‌های کاربردی بصورت دستی	۵.۹
۸۱	استفاده از Logcat	۵.۱۰
۸۷	فصل ششم	
۸۸	کار بر روی SQLite	۶.۱
۸۸	فهم عمیق SQLite	۶.۲
۸۸	آنالیز یک برنامه کاربردی با استفاده از SQLite	۶.۳
۹۷	فصل هفتم	
۹۸	حملات کمتر شناخته شده اندروید	۷.۱

۷.۲	آسیب‌پذیری Webview در اندروید	۹۸
۷.۳	آلوده کردن برنامه‌های قانونی اندروید	۱۰۱
۷.۴	آسیب‌پذیری در ad libraries	۱۰۲
۷.۵	Cross- Application Scripting در اندروید	۱۰۲
۱۰.۵	فصل هشتم	
۸.۱	گزارش تست نفوذ	۱۰۶
۸.۲	اصول گزارش دهی در تست نفوذ	۱۰۶
۸.۳	نوشتن گزارش تست نفوذ	۱۰۶
۸.۴	خلاصه اجرایی	۱۰۷
۸.۵	آسیب‌پذیری‌ها	۱۰۷
۸.۶	حوزه کار	۱۰۷
۸.۷	ابزارهای مورد استفاده	۱۰۸
۸.۸	متدولوژی مورد استفاده	۱۰۸
۸.۹	پیشنهادهای و توصیه‌ها	۱۰۸
۸.۱۰	نتیجه‌گیری	۱۰۸
۱۰.۹	ضمائم و پیوست‌ها	
۹.۱	بدافزارهای اندرویدی	۱۱۰
۹.۲	DroidDream	۱۱۰
۱۱۳	منابع	

مقدمه

امروزه دستگاه‌های هوشمند قابل‌حمل همچون تلفن‌های همراه هوشمند و تبلت‌ها، جزء جدایی‌ناپذیر زندگی انسان‌ها شده‌اند. قابل‌حمل و کاربرپسند بودن دستگاه‌های فوق، در کنار پیشرفت در فناوری‌های نرم‌افزاری و سخت‌افزاری و همچنین ارائه محصولات جدید با قابلیت‌های شگفت‌انگیز را می‌توان علل اصلی تمایل افراد به استفاده از این ابزارها دانست. در این میان سیستم عامل اندروید که از سال ۲۰۰۵ پا به عرصه وجود گذاشت تا کنون توانسته است جایگاه بسیار خوبی در میان تلفن‌های هوشمند و تبلت‌ها کسب کند. استقبال از این سیستم عامل تنها به استفاده در ابزارهای ارتباطی محدود نشده و امروزه استفاده از این سیستم عامل در کتاب‌خوان‌ها، تلویزیون‌ها، و نت‌بوک‌ها را هم شاهد هستیم. این استقبال منجر گردیده است که سیستم عامل اندروید به تنهایی در برابر رقاباتی بزرگ همچون iOS و WinPhone بتواند به تنهایی بالغ بر هفتاد درصد فروش بازار ابزارهای هوشمند را به خود اختصاص دهد.

در کنار تمامی این پیشرفت‌ها، و تسخیر شدن بازار ابزارهای قابل‌حمل هوشمند توسط اندروید شرکت گوگل، دغدغه‌ها و مسایل امنیتی کماکان برای خود باقی هستند. علاوه بر این ذات قابل‌حمل بودن این ابزارها و همچنین دارا بودن اطلاعات حساس مشتریان مانند اطلاعات هویتی و بانکی آن‌ها، توجه هرچه بیشتر به مسئله امنیت در این حوزه را نمایان می‌کند.

با توجه به اهمیت فراوان مقوله امنیت برای کاربران از روند و رشد استفاده از این سیستم عامل در کشور عزیزمان جمهوری اسلامی ایران و با توجه به اینکه تعداد دهنندگان بسیاری در کشورمان اقدام به ارائه برنامه‌های کاربردی اندرویدی می‌نمایند، برآن شدیم تا با ارائه این کتاب، گامی کوچک در جهت کمک به توسعه دهنندگان این دسته از برنامه‌های کاربردی، با فراهم آوردن امکان آشنایی با ماهه کاربردی از دیدگاه امنیتی برداریم.

از آنجایی که هیچ نوشتاری عاری از خطا و اشتباه نیست از دریافت نظرات، پیشنهادات و انتقادات شما خوانندگان فرهیخته در این حوزه، بسیار خشنود خواهیم شد.

علیرضا قاضی ساعدی

زمستان ۱۳۹۳