



راهنمای توسعه امن برنامه‌های کاربردی اندروید

Secure Android Application Development Guide



سرشناسه : شفیعی ثابت ، احمد رضا ، ۱۳۶۷-
 عنوان و نام پدیدآور : راهنمای توسعه امن برنامه های کاربردی اندروید / مولف احمد رضا شفیعی ثابت ، حامد ایزدی
 مشخصات نشر : تهران: ناخوس، ۱۳۹۸.
 مشخصات ظاهری : ۳۰۰ص : مصور جدول بشودار.
 شابک : 978-600-473-197-3
 وضعیت فهرست نویسی : فیا
 موضوع : ۱ اندروید (منبع الکترونیکی) — تدابیر ایمنی
 موضوع : Android (Electronic resource)—Security Measures
 شناسه افزوده : ایزدی ، حامد ، ۱۳۶۴-
 رده ، درج و کنگره : QA ۷۶/۷۶
 رده بندی دیسی : ۰۰۵/۸
 شماره ثبت کتابخانه ملی : ۵۷۲۲۰۰۲



برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoospress.ir

انتشارات ناخوس

نام کتاب : راهنمای توسعه امن برنامه های کاربردی اندروید
 ناشر : انتشارات ناخوس
 مولفین : احمد رضا شفیعی ثابت ، حامد ایزدی
 ویراستار فنی : واحد فنی
 ویراستار : محمد بهشتی آتشگاه
 طراحی جلد : حمید سبوحی
 چاپ اول : ۱۳۹۸
 چاپ اول : ۱۰۰۰ نسخه
 قیمت : ۴۳۰،۰۰۰ ریال
 چاپ و صحافی : چاپ برجسته
 شابک : ۹۷۸-۶۰۰-۴۷۳-۱۹۷-۳
 ISBN : 978-600-473-197-3

حقوق محفوظ است. تکثیر
 تمامی یا بخشی از این اثر به
 صورت رونقدهی یا هر چه
 چاپ افست، بازاری، فتوکپی و
 انواع دیگر چاپ ممنوع است و
 پیگرد قانونی دارد.

انتشارات ناخوس

۱- بلوار کشاورز-خیابان ۱۶ آذر-کوچه پارس-پلاک ۱۰

تلفن و فاکس : ۶۶۳۷۸۹۵۱-۶۶۳۷۸۹۵۲

پیشگفتار

با گسترش کاربردهای نرم افزار و رشد انبوه داده ها، سوء استفاده کنندگان توجه خود را به دستیابی داده ها، نفوذ به سیستم ها و یا اختلال در کارکرد سیستم ها معطوف کرده اند. بخشی از تهدیدات در حوزه امنیت نرم افزار ناشی از کم توجهی برنامه نویسان به اصول برنامه نویسی و قواعد و الزامات سکوها می باشد. توسعه نرم افزار است که فرصت مناسب را در اختیار سوء استفاده کنندگان قرار می دهد. نرم افزارها را کار بردی مبتنی بر اندروید نیز از این قاعده مستثنی نیستند. استفاده از فنون صحیح و رعایت قواعد می تواند سطح امنیت نرم افزار تولید شده را ارتقاء دهد. اطلاع از این قواعد به دلیل مجتمع نبودن و همچنین داشتن ابعاد و زوایای مختلف و تغییرات سریع سکوها توسعه نرم افزار، برای برنامه نویسان دشوار است. هر طوفی صرف دانستن غلط بودن فن استفاده شده کافی نیست و توسعه دهنده باید بداند چگونه اشتباه خود را اصلاح کند. در عین حال اطلاع از روش های صحیح زمان بر خواهد شد. این دو مسئله باعث می شود تا توسعه دهندگان با روش سعی و خطا امنیت محصولات خود را تأمین کنند در حالی که اگر اصول و روش های صحیح آگاهی داشتند استراتژی توسعه خود را منطبق با آن اصول و روش ها تنظیم می کردند.

در این کتاب توصیه ها، فن ها و روش ها در قالب فصل مطرح شده است. فصل اول معماری و مؤلفه های اصلی امنیت اندروید که توسعه دهنده برای درک مکانیسم های امنیتی باید از آن ها مطلع باشد را مورد بحث قرار می دهد. فصل دوم مجوزهای دسترسی و اعمال سطح دسترسی بر مؤلفه های برنامه را مطرح می کند. فصل سوم کلیه مسائل مربوط به داده از قبیل استفاده صحیح از انواع حافظه، پایگاه داده، رمزنگاری، رمزگشایی، چکیده سازی، صحت سنجی داده های ورودی و اصول امنیتی داده در ثبت وقایع و اطلاعاتی ها بررسی شده است. در فصل چهارم توصیه ها و نحوه به کارگیری اعتبارسنجی و ارتباط با شبکه بررسی شده است. فصل پنجم به کیفیت کد در لایه ی کاربرد اندروید پرداخته است. فصل ششم استانداردهای موجود در تولید نرم افزارهای تلفن همراه و ارزیابی آن را معرفی کرده است. همراه این کتاب، نمونه ی اجرایی سازگار با قواعد و اصول مطرح شده ارائه شده است و در طول کتاب

به این پیاده‌سازی‌ها ارجاع داده شده است. این پیاده‌سازی‌ها می‌تواند به‌عنوان مرجعی جهت پیاده‌سازی سریع و ایمن نیازمندی‌های برنامه‌ها، مورد استفاده توسعه‌دهندگان قرار گیرد.

در اینجا از مرکز امنیت فضای تبادل اطلاعات شرکت صافتا، معاونت پژوهش و نویسندگان محترم این مجموعه، به خاطر اهتمام در این امر مهم قدردانی می‌نمایم. امید است بتوان به حول و قوه الهی با پشتکار و تلاش روزافزون، گامی مهم در جهت ارتقاء کیفیت سامانه‌های نرم‌افزاری در کشور برداریم.

مدیر عامل شرکت صنایع امنیت فضای تبادل اطلاعات صایران (صافتا)

کیانوش آزادی

فهرست مطالب

۱۵.....	بخش اول
۱۷.....	فصل اول : آشنایی با معماری امنیت اندروید و مؤلفه‌های اصلی
۱۷.....	۱-۱ معماری اندروید
۱۸.....	۱-۱-۱ مؤلفه‌های هسته‌ای لینوکس
۲۱.....	۲-۱-۱ Native User Interface
۲۲.....	۳-۱-۱ ماشین مجازی Android و Dalvik
۲۵.....	۴-۱-۱ Java Runtime Libraries
۲۶.....	۵-۱-۱ سرویس‌های سیستمی
۲۶.....	۶-۱-۱ لایه کاربرد
۲۶.....	۷-۱-۱ Inter-Process Communication
۳۱.....	۸-۱-۱ کتابخانه‌های چارچوب اندروید
۳۲.....	۹-۱-۱ برنامه‌ها
۳۴.....	۲-۱ مدل امنیتی اندروید
۳۴.....	۱-۲-۱ جعبه‌ی شنی برنامه‌ها
۳۷.....	۲-۲-۱ مجوزها
۳۸.....	۳-۲-۱ امضای کد و کلیدهای سکو
۳۹.....	۴-۲-۱ پشتیبانی از چند کاربری

۴۰.....	SELinux ۵-۲-۱
۴۱.....	۳-۱ به روز رسانی های سیستمی
۴۲.....	۴-۱ منابع اصلی فصل یکم
۴۵.....	فصل دوم : مجوزهای دسترسی و مؤلفه های برنامه
۴۷.....	۱-۲ درخواست مجوز دسترسی یک برنامه
۴۸.....	۲-۲ موزهای دسترسی شخصی سازی شده
۵۰.....	۳-۲ اعمال مجوز دسترسی استفاده از برنامه نویسی
۵۲.....	۴-۲ اعمال مجوزهای دسترسی به صورت پویا
۵۳.....	۵-۲ گروه بندی مجوزها
۵۴.....	۶-۲ مؤلفه های عمومی و اختصاصی
۵۶.....	۷-۲ امن سازی مؤلفه های برنامه های اندروید
۶۰.....	۱-۷-۲ Activity و Service مجوزهای
۶۲.....	۲-۷-۲ Broadcast مجوزهای
۶۳.....	۳-۷-۲ Content Provider مجوزهای
۶۶.....	۴-۷-۲ Pending Intents
۶۷.....	۸-۲ درخواست مجوزهای دسترسی در حال اجرا
۶۹.....	۹-۲ نحوه ی درخواست مجوز
۷۱.....	۱-۹-۲ مدیریت درخواست مجوز
۷۲.....	۱۰-۲ خلاصه ی توصیه ها در رابطه با مجوزهای دسترسی
۷۴.....	۱۱-۲ منابع اصلی فصل دوم

فصل سوم : امنیت داده ها.....	۷۵
۱-۳ حافظه تنظیمات اشتراکی	۷۷
۲-۳ ذخیره سازی در فایل	۷۸
۱-۲-۳ ذخیره در فایل های حافظه‌ی داخلی.....	۷۹
۲-۲-۳ ذخیره سازی در فایل های حافظه‌ی خارجی	۷۹
۳-۳ ذخیره سازی در پایگاه داده ها	۸۱
۴-۳ رمزنگاری	۸۹
۱-۴-۳ روش رمزنگاری با کلید متناهی	۸۹
۲-۴-۳ روش رمزنگاری با کلید متناهی	۹۱
۳-۴-۳ رمزنگاری با استفاده از رمز عبور	۹۲
۵-۳ چکیده‌سازی	۹۴
۱-۵-۳ کاربرد های چکیده‌سازی	۹۵
۶-۳ کلید رمزنگاری	۹۶
۱-۶-۳ تولید کلید رمزنگاری	۹۶
۲-۶-۳ تولید عدد تصادفی	۹۷
۳-۶-۳ مدیریت کلید رمزنگاری	۹۹
۷-۳ انتخاب روش رمزنگاری استاندارد	۱۰۱
۸-۳ صحت سنجی ورودی ها.....	۱۰۶
۹-۳ بررسی ثبت وقایع برنامه ها	۱۰۸
۱۰-۳ بررسی notification در برنامه ها.....	۱۰۸
۱۱-۳ خلاصه ملاحظات مربوط به امنیت داده و اعتبار سنجی	۱۰۹
۱۲-۳ منابع اصلی فصل سوم	۱۱۲

فصل چهارم : امنیت ارتباطات و اعتبارسنجی ۱۱۳

۱-۴ استفاده از SSL/TLS در محیط اندروید..... ۱۱۵

۱-۴-۱ تأیید سرور..... ۱۱۶

۱-۴-۲ تغییر و شخصی سازی مکانیسم SSL/TLS و کاربردهای آن ۱۱۸

۲-۴ انتخاب روش برقراری ارتباط برنامه ۱۲۱

۳-۴ اعتبار سنجی ۱۲۳

۴-۴ نکات پیاده سازی امن مکانیسم اعتبارسنجی..... ۱۲۷

۱-۴-۴ پیام های خدا ۱۲۷

۲-۴-۴ پیاده سازی یک سیستم بازیابی رمز عبور ۱۲۸

۳-۴-۴ خروج کاربران - نقض نمودن نشست ۱۲۹

۴-۴-۴ اعتبار سنجی محلی ۱۲۹

۵-۴ خلاصه ملاحظات مربوط به امنیت ارتباطات شبکه و اعتبار سنجی ۱۳۱

۶-۴ منابع اصلی فصل چهارم ۱۳۲

فصل پنجم : کیفیت کد ۱۳۳

۱-۵ خطاهای رایج در زبان جاوا ۱۳۳

۱-۵-۱ محدود نبودن مدت زمان ماندگاری داده در حافظه ۱۳۳

۲-۵-۱ ذخیره سازی شفاف داده های حساس و مربوط به اعتبارسنجی..... ۱۳۶

۳-۵-۱ ذخیره سازی داده های حساس به صورت قابل رؤیت در سمت مشتری ۱۳۷

۴-۵-۱ صحت سنجی پارامترهای متدهای حساس و امنیتی ۱۴۰

۵-۵-۱ پیشگیری از بارگذاری فایل بدون کنترل ۱۴۲

۶-۵-۱ کنترل مقادیر خروجی به روش جایگذاری ۱۴۵

- ۷-۱-۵ جلویی از حملات code injection..... ۱۴۹
- ۸-۱-۵ جلویی از حمله‌ی XPath Injection..... ۱۵۲
- ۹-۱-۵ جلویی از LDAP injection..... ۱۵۶
- ۱۰-۱-۵ استفاده از توابع چکیده‌ساز برای نگهداری رمز عبور..... ۱۶۰
- ۱۱-۱-۵ تأمین صحیح seed مربوط به کلاس SecureRandom..... ۱۶۴
- ۱۲-۱-۵ استفاده از متد Object.equals برای مقایسه‌ی کلیدهای رمزنگاری..... ۱۶۵
- ۱۱-۱-۵ استفاده از متدهایی که ممکن است توسط کد غیرقابل اعتماد overwrite شود..... ۱۶۶
- ۲-۵ فن‌های کد نویسی دفاعی..... ۱۷۳
- ۱-۲-۵ محدود کردن نام متغیرها..... ۱۷۳
- ۲-۲-۵ محدود نمودن ناحیه اثر @SuppressWarnings..... ۱۷۶
- ۳-۲-۵ حداقل نمودن دسترسی‌ها در class و اعضای آن..... ۱۷۷
- ۴-۲-۵ مستند نمودن mread-safety بودن داده از انوتیشن‌ها..... ۱۸۱
- ۵-۲-۵ همواره بازخوردی برای نتیجه فراوانی یک متد ارائه شود..... ۱۸۵
- ۶-۲-۵ تشخیص نوع فایل با استفاده از مشخصه‌های نوع فایل..... ۱۸۷
- ۷-۲-۵ کد خود را وابسته مکان قرارگیری enumeration در هر enum قرار ندهید..... ۱۹۰
- ۸-۲-۵ رفتارهای جاوا در مورد تقدم انواع عددی برای تبدیل به یکدیگر را در نظر داشته باشید..... ۱۹۱
- ۹-۲-۵ قابلیت compile-time type checking در خصوص متدهای varargs..... ۱۹۴
- ۱۰-۲-۵ متغیرهایی که امکان دارد در نسخه‌های بعدی تغییر کند را به صورت public final تعریف نکنید..... ۱۹۵
- ۱۱-۲-۵ وابستگی حلقه‌ای بین پکیج‌ها پرهیز کنید از پیام‌های خطای قابل فهم به جای پیام‌های کلی استفاده کنید..... ۱۹۷

- ۲۰۰..... ۱۲-۲-۵ امکان بازیابی از وضعیت رخداد خطا را بررسی کنید
- ۲۰۱..... ۱۳-۲-۵ بررسی وضعیت امضای کد
- ۲۰۲..... ۱۴-۲-۵ بررسی شود برنامه قابل اشکال زدایی نباشد
- ۲۰۲..... ۱۵-۲-۵ اعلام اشکال زدایی حذف شود
- ۲۰۲..... ۱۶-۲-۵ بررسی بروز شرایط حملات Injection
- ۲۰۴..... ۱۷-۲-۵ استفاده از امکانات امنیتی
- ۲۰۷..... ۳-۵ به تبع این فصل پنجم

فصل ششم: چارچوب های ارزیابی برنامه، توصیه ها و تهدیدات..... ۲۱۱

- ۲۱۲..... ۱-۶ توصیه های مطرح شده توسط PCI
- ۲۱۲..... ۱-۱-۶ جلوگیری از دسترسی مداخلی غیرمجاز به دستگاه
- ۲۱۲..... ۲-۱-۶ انجام کنترل های سمت دستگاه و ثبت و اعلان دسترسی های غیرمجاز
- ۲۱۲..... ۳-۱-۶ جلوگیری از ارتقا ناخواسته دسترسی و امکان از دور غیرفعال سازی قابلیت پرداخت
- ۲۱۳..... ۴-۱-۶ امکان غیرفعال سازی برنامه پرداخت در
- ۲۱۳..... ۵-۱-۶ تشخیص سرقت و یا گم شدن دستگاه
- ۲۱۳..... ۶-۱-۶ سیستم پشتیبان سفت و سخت
- ۲۱۳..... ۷-۱-۶ ارجحیت تراکنش های برخط
- ۲۱۳..... ۸-۱-۶ تطابق با اصول امن کد نویسی، مهندسی و آزمون نرم افزار
- ۲۱۴..... ۹-۱-۶ محافظت در برابر آسیب پذیری های شناخته شده
- ۲۱۴..... ۱۰-۱-۶ محافظت از دستگاه در برابر برنامه های غیرمجاز
- ۲۱۴..... ۱۱-۱-۶ محافظت از دستگاه در برابر بدافزار
- ۲۱۴..... ۱۲-۱-۶ محافظت از دستگاه در برابر الصاقیات غیرمجاز

- ۶-۱-۱۳ ارائه دستورالعمل‌های به‌کارگیری و پیاده‌سازی ۲۱۵
- ۶-۱-۱۴ رعایت امنیت مربوط به نشر رسید تجاری ۲۱۵
- ۶-۱-۱۵ نمایش نشانه امن بودن انتقال اطلاعات پرداخت ۲۱۵
- ۶-۱-۱۶ ارائه مکانیسم نظارت و ثبت وقایع برای کاربر و دستگاه ۲۱۵
- ۶-۱-۱۷ جلوگیری از سوءاستفاده از اطلاعات کاربری هنگام پردازش و ذخیره‌سازی ۲۱۶
- ۶-۱-۱۸ جلوگیری از فیلتر شدن و استراق سمع اطلاعات کاربری ۲۱۶
- ۶-۲-۲ تویپه‌ها، مطرح‌شده توسط Google ۲۱۶
- ۶-۲-۱ ذخیره‌ری داد ۲۱۶
- ۶-۲-۲ به‌کارگیری مجموعه‌ای دسترسی ۲۱۶
- ۶-۲-۳ به‌کارگیری شبکه ۲۱۷
- ۶-۲-۴ صحت سنجی مقادیر ورودی ۲۱۷
- ۶-۲-۵ مدیریت اطلاعات کاربری ۲۱۷
- ۶-۲-۶ به‌کارگیری webview ۲۱۷
- ۶-۲-۷ به‌کارگیری رمزنگاری ۲۱۸
- ۶-۲-۸ به‌کارگیری IPC ۲۱۸
- ۶-۲-۹ بارگذاری پویای کد ۲۱۸
- ۶-۲-۱۰ امنیت در کدهای بومی ۲۱۸
- ۶-۳ چک‌لیست طرح‌شده توسط google ۲۱۸
- ۶-۴ بررسی تهدیدات و توصیه‌های اصلی مطرح‌شده توسط OWASP ۲۲۴
- ۶-۴-۱ ده تهدید اصلی منتشرشده در سال ۲۰۱۲ ۲۲۴
- ۶-۴-۲ ده تهدید اصلی منتشرشده در سال ۲۰۱۶ ۲۴۴
- ۶-۵ استاندارد ارزیابی امنیتی برنامه‌های موبایل OWASP ۲۷۵

۶-۶ منابع اصلی فصل ششم ۲۸۵

بخش دوم ۲۸۷

فصل هفتم: نمونه های پیاده سازی اجرایی ۲۸۹

۱-۷ نمونه پیاده سازی های اجرایی ساخت و استفاده از Activity ها ۲۸۹

۲-۷ پیاده سازی های مربوط به دریافت و ارسال Broadcast ها ۲۹۰

۳-۷ پیاده سازی های مربوط به ساخت و استفاده از ContentProvider ۲۹۱

۴-۷ پیاده سازی های مربوط به ساخت و استفاده از Service ها ۲۹۲

۵-۷ استفاده از SQLite ۲۹۲

۶-۷ پیاده سازی های مجبور می در مرس ۲۹۲

۷-۷ پیاده سازی استفاده امن از انواع فایل ۲۹۴

۸-۷ پیاده سازی قابلیت Browsable Intent ۲۹۵

۹-۷ پیاده سازی انواع رمزنگاری و رمزگشایی ۲۹۶

۱۰-۷ تشخیص دستکاری داده ها ۲۹۶

۱۱-۷ پیاده سازی ارتباطات ۲۹۷

۱۲-۷ پیاده سازی استفاده از قابلیت اثر انگشت اندروید ۲۹۷

۱۳-۷ استفاده از webview ۲۹۷

۱۴-۷ ثبت وقایع با استفاده از LogCat ۲۹۸

۱۵-۷ استفاده از Notification ۳۰۰