من چند روز پیش مقاله ای پیدا کردم که واستون می فرستم توی این مقاله ابزاری برای برای برنامه های native code اندروید ارائه شده که از طریق روش concolic آسیب پذیری logic bomb رو پیدا می کنه. کاری که من قراره انجام بدم تشخیص آسیب پذیری تزریق بود با تاکید بر تریق کدهای JS ابتدا می خواستم که روی کدهای native اندروید انجام بدم ولی این مقاله رو که دیدم به نظرم بهتر اومد که تاکید روی کدهای Hybrid باشه که از Web technology برای پیاده سازی استفاده می کند و در صورت نیاز از native code برای پیاده سازی پلاگین های برای دسترسی به APIهای اندروید یا هر سیستم عامل دیگری استفاده می کند (<http://cordova.apache.org/docs/en/latest/guide/overview/index.html> معماری این گونه سیستم ها آورده شده است) در لینک <http://cordova.apache.org/docs/en/latest/guide/appdev/security/index.html> هم در مورد امنیت صحبت شده است که در انتها مقاله ای که در مورد آسیب پذیری های webView که قبلا براتون فرستادم هم آورده شده است(لینک آخر در recommended articles)

برای پیاده سازی برنامه های Hybrid از فریم ورک هایی مثل (Cordova (<https://en.wikipedia.org/wiki/Apache_Cordova> استفاده می شود. که برنامه را محدود به پلتفرم خاصی نمی کنند. برنامه نویس برنامه خود را به زبان JS می نویسد و در صورت لزوم برای استفاده از APIخاصی از کدهای java برای نوشتن پلاگین استفاده می کند. در آخر همه این کدها توسط cordova به webView داده می شود تا اجرا شوند.

در قسمت limitatin مقاله هم آمده که کار انجام شده محدود به byte code هست نه native code و همچنین مشکل دیگر ابزار در این است که با وجود objectهای پیچیده مثل context مشکل دارد ولی با primitive typeها خوب عمل میکند.