

Snyk & Quokka integration

Deploy high-quality, secure apps – faster

With insights from Quokka’s mobile threat analysis, app developers can keep up with the accelerating pace of development and ship high-quality, secure apps faster – and protect their organizations from the long-term costs associated with security breaches and non-compliance penalties.

Why Snyk and Quokka?

End-to-end AppSec from development to runtime

Get comprehensive layers of mobile security analysis – for both app source code and compiled binary – with Snyk’s visibility into open-source vulnerabilities paired with Quokka’s mobile threat analysis. Developers benefit from earlier detection of zero-day exploits, with cross-validation of findings resulting in fewer false-positives.

Benefits

Deep mobile security analysis

Using dynamic, interactive and static analysis, including SBOM – for both app source code and compiled binary

Earlier detection

Detect zero-day exploits and emerging threats in the SDLC in the local dev environment

Fewer false-positives

Reduce the noise with fewer false-positives with cross-validation of findings

“

Our integration with Snyk marks a significant milestone in our commitment to providing comprehensive mobile threat analysis for app developers. By combining Quokka’s expertise in mobile security with Snyk’s unmatched visibility into open-source vulnerabilities, we empower Security and Developer teams to navigate the fast-paced world of app development with confidence.”

– Vijay Pawar
SVP of product at Quokka



How it works

- Snyk Code scans mobile app source code
- Quokka runs static, dynamic and interactive tests against the compiled mobile app binary
- Quokka shows correlated issues and presents them to developers for immediate remediation before app deployment

ID	Found by	Severity	Problem title	CWE	Project URL
205	Quokka	High	Debuggable enabled	CWE-489	https://emm.krwr.net/#/android-report/4f-184bae-35cf-48c5-9b5b-c63531602785
220	Quokka	High	Vulnerable to known OS attacks	CWE-284	https://emm.krwr.net/#/android-report/4f-184bae-35cf-48c5-9b5b-c63531602785
14d6de1d-3724-41e9-9022-c731fa059832	Snyk	Medium	Android Debug Mode Enabled	CWE-489	https://app.snyk.io/org/quokka-nfr-shared/project/896327f1-7ed0-4b8e-8dc8-d56b-1c6bb9e4
5f6b74d4-8c0e-4140-9979-cf4d-862b30c4	Snyk	Medium	Cross-site Scripting (XSS)	CWE-79	https://app.snyk.io/org/quokka-nfr-shared/project/896327f1-7ed0-4b8e-8dc8-d56b-1c6bb9e4
80b13c17-7174-47c0-8cfa-20a71bb64b8a	Snyk	Medium	Improper Certificate Validation	CWE-295	https://app.snyk.io/org/quokka-nfr-shared/project/896327f1-7ed0-4b8e-8dc8-d56b-1c6bb9e4
90c43e6c-65cd-45f1-bcb3-6d28378c9ea8	Snyk	Medium	Unauthorized File Access	CWE-79	https://app.snyk.io/org/quokka-nfr-shared/project/896327f1-7ed0-4b8e-8dc8-d56b-1c6bb9e4
6	Quokka	Medium	Requested excessive permissions	CWE-250	https://emm.krwr.net/#/android-report/4f-184bae-35cf-48c5-9b5b-c63531602785
206	Quokka	Medium	Allows backup	CWE-497	https://emm.krwr.net/#/android-report/4f-184bae-35cf-48c5-9b5b-c63531602785

Contact information

Ilya Dreytser ilya@quokka.io

Learn more at www.quokka.io

