Mon, Mar 30, 2020

OrangeBank Version 1.34

Risk Assesment of API Specifications

Max Risk Score 9/10 **Critical**

App Services **100** | APIs Analyzed **325**

Application Services Risk Distribution

App Services by Highest Severity Violations

Top 3 by Risk Score *

orangebank_meta

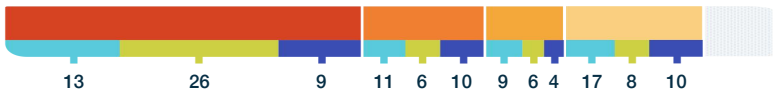
orangebank_stores

orangebank_payments

*Risk Score as identified by the highest severity violations of the APIs

48	27	19	2	4
Critical	High	Medium	Low	No Risk

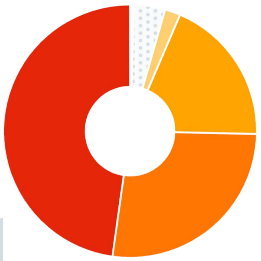
Distribution of Severity Across Risk Categories



Risk Categories: Security Data Format

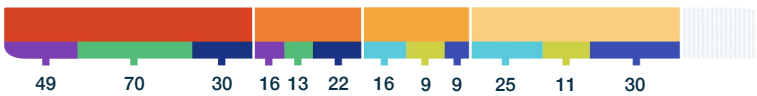
API Risk Distribution

APIs by Highest Severity Violations



149	51	34	61	30
Critical	High	Medium	Low	No Risk

Distribution of Severity Across Risk Categories

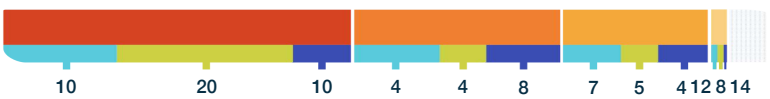


Risk Categories: Security Data Format

Distribution of Severity Across Security Risk Categories

Security

40	16	16	34	12
Critical	High	Medium	Low	No Risk



Security Risk Categories: Authentication Authorization Transport

Insights

243 Number of violations based on 6576 checks.

Data In

24% of APIs have critical violations among POST/PUT ops and bring data into your environment.

Data Out

24% of APIs have critical violations among GET/POST/PUT ops and push data out.

Violations

100% of the APIs have more than 3 parameters that have contributed to a violation

Risk Themes

- Top violations across all apps belonging to Security:Transport was the lack of HTTPS. In addition, we found the most frequently occurring violations within orangebank_invoice.json
- 3 application services had Authorization and Authentication violations. Interestingly, the majority of APIs containing violations were found in orangebank_user.json

Next Steps

- Prioritize addressing Authentication related issues
- Define "maxLength" in parameters for maximum reduction in risk
- Get started with a continuous and automated API 360 Risk Assessment that considers your API specification and runtime application API data

CLOUDVECTOR