TRACEABLE | ASPEN LABS

API Security Checklist

The Basics

□ **Know your attack surface**

□ Know the number of APIs you have

□ Know which APIs are publicly accessible

□ Know which public APIs should be internal only

□ **Review access control**

□ Check for authentication on every API point

□ Ensure permission levels of each account is be minimized

□ **Ensure the API never trusts client input**

□ Review request and response data

□ Check that database queries are using prepared statements

□ **Remove unnecessary API keys and endpoints**

□ Remove source maps if not necessary

API Security Programs

□ **Design a vulnerability management process**

□ Accept vulnerability reports into tracking software

□ Prioritize by severity and business impact

□ Build into existing developer pipelines and processes

□ Test after fix is deployed to ensure vulnerability has been resolved

□ **Inventory your APIs on a continual basis**

□ Flag any newly discovered APIs

□ Test for access control, encryption and authentication

□ **Deploy a continuous API protection solution**

□ Block and investigate malicious requests and attacks

□ **Regularly run automated API security testing**

□ Monitor live traffic for data exfiltration, fraud and business logic abuse

□ Ensure the output enters the vulnerability management and remediation process

□ **Invest talent and time into threat hunting for a proactive approach to handling threats**

□ Spot suspicious API activity that may be indicative of an attack

□ Read recent API breaches and technical analysis