OWASP Mobile vs API Top 10 Whitepaper

Oct, 21st 2019

INTESAR SHANNAN MOHAMMED

CTO
FX LABS, INC

Dr. Abdullah Akbar

ENGINEERING
FX LABS, INC

FX Labs, Inc.
API Security Platform
https://cybersecuriti.ai

Authors

Intesar Shannan Mohammed
CTO
FX Labs, Inc.

Dr. Abdullah Akbar
Engineering
FX Labs, Inc.

Abstract

This whitepaper aims to help organizations understand the difference between OWASP Mobile Top 10 and OWASP API Top 10 security threats.

Audience

CTO, CISO & Engineering Leadership.

Common Assumptions

We took the latest OWASP Mobile Top 10 and API Top 10 published articles to compare them.

Prerequisites

1. OWASP Mobile Top 10 (2016 - most recent)
2. OWASP API Top 10 (Sep 2019 - Release Candidate)

What is OWASP

OWASP (Open Web Application Security Project) is a non-profit and vendor-neutral organization. OWASP publishes AppSec Top 10 critical security risks based on the broad industry consensus.

At the moment, this research is hard to back by data as most organizations still don't reveal the breaches, this may change with new laws like GDPR & CCPA, which requires that organizations report accidental data exposures and breaches.

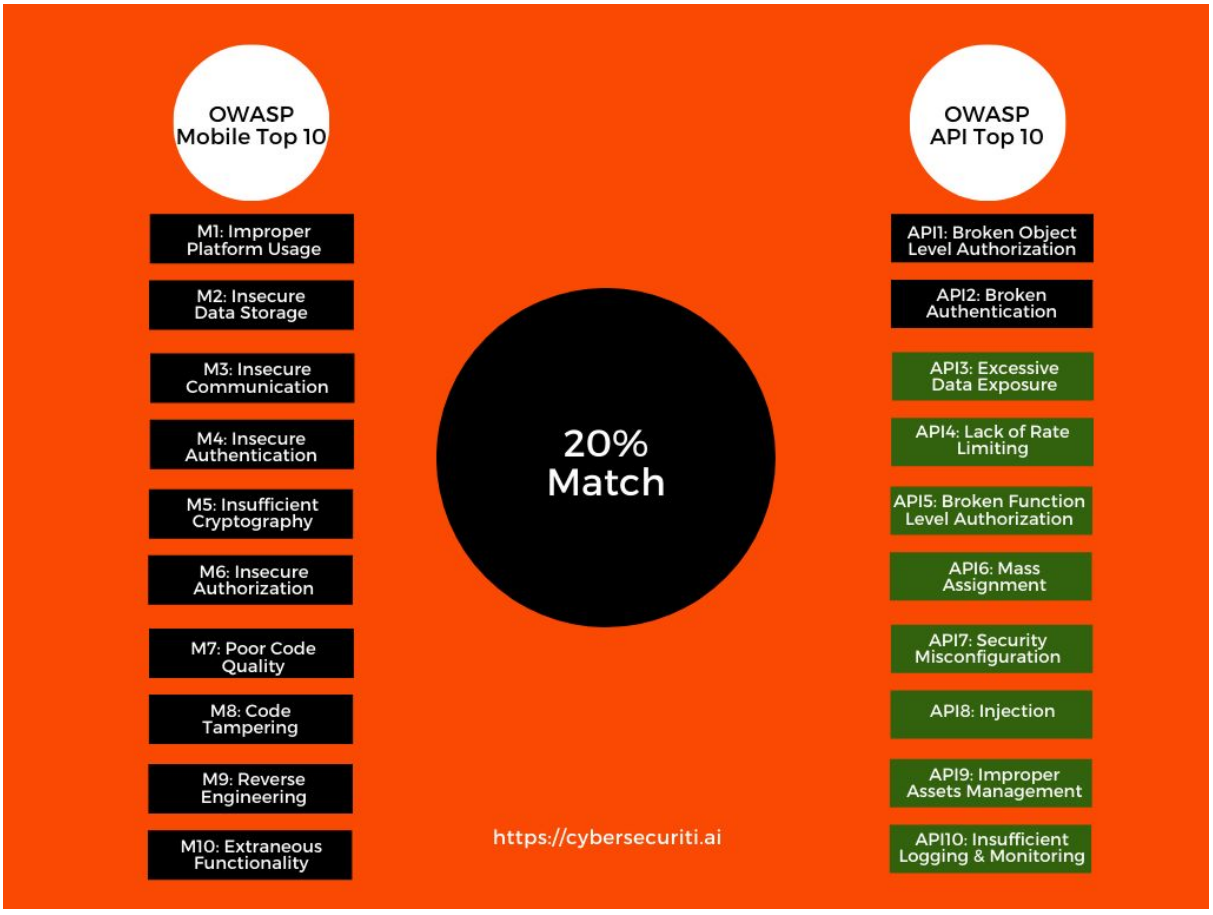
What's in OWASP Mobile Top 10

Rank	Name	Comments
M1	Improper Platform Usage	"Easy to use and hard to misuse" - that is the strategy to be used for the server side implementations.
M2	Insecure Data Storage	You must consider an elaborate analysis of your application data flow and lifecycle so that data is both secure and all data residue is taken care of.
M3	Insecure Communication	Ensure a blanket rule for using SSL/TLS/Certificate trustworthiness so that all communication (inter/intra) isn't prone to loopholes.
M4	Insecure Authentication	Use device specific authentication, password/token policy implementations and opt for server-centric cum lean-client design.
M5	Insufficient Cryptography	Identify and encrypt all sensitive data on the mobile device and employ only recommended algorithms.
M6	Insecure Authorization	Roles/permissions to be verified for all endpoints at the server-side only. Never on the client-side.
M7	Poor Code Quality	Follow code conventions, reviews and inspections for non-functional considerations.
M8	Code Tampering	Client code should maintain integrity at all times and detect runtime integrity violations. Refer : https://www.owasp.org/index.php/OWASP_Reverse_Engineering_and_Code_Modification_Prevention_Project
M9	Reverse Engineering	Client code should be obfuscated effectively and selectively and not get deobfuscated by tools like IDA Pro/Hopper etc.
M10	Extraneous Functionality	The mobile application configurations should not contain any loopholes and ensure client side logging isn't overly descriptive.

What’s in OWASP API Top 10

Rank	Name	Comments
API1	Broken Object Level Authorization	Add authorization tests either by using policies or by reviewing the information or object layer functions.
API2	Broken Authentication	Using strong passwords with invalidation implementations for encrypted storage, session timeout management and token authentication schemes.
API3	Excessive Data Exposure	Identifying and classifying data properties will help to strategize exactly what needs to be sent to users. It also helps to mask irrelevant fields and prevent unnecessary cache.
API4	Lack of Resources & Rate Limiting	DDoS/DoS has a serious impact on businesses with immediate consequences, and AI techniques can help to identify and configure incoming data/operation requests accordingly.
API5	Broken Function Level Authorization	For verification of all possible permutations and variations of your organization's access policies, you would need a comprehensive automatic search and review.
API6	Mass Assignment	Using standard implementations of serialization/deserialization techniques can render you vulnerable to overriding protected areas.
API7	Security Misconfiguration	Having a checklist to check all configurations before production-ready can eradicate most of these types of flaws.
API8	Injection	Such attacks can be effectively avoided by custom validations and parameterization.
API9	Improper Assets Management	Record all installations and restrict/phase out the older ones
API10	Insufficient Logging & Monitoring	Securing logs, ensuring required information is logged and considering convergence of timely warnings with other devices.

Comparison



Conclusion

- Top 10 Mobile security risks are almost on another tangent when compared to the API top 10 risks.
- Authorization and Authentication are the top 2 risks in the API top 10 but are ranked no.4 and no. 6 in the mobile top 10.
- Code integrity and privacy is a major concern in the Mobile top 10 risks (no. 8 and no. 9).
- Client-side/device-based code is a predominant concern in more than 6 of the top 10 mobile security risks but does not find any relevance in the API top 10 risks.
- Overall there is only a **20%** match between the two top 10 lists.

Reviewers:

- Dr. Mohammed Nadeem
- Mohammed Shoukath Ali

References:

https://www.owasp.org/index.php/OWASP_API_Security_Project
https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10