OWASP Web 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 Web Top 10 and OWASP API Top 10 security threats.

Audience

CTO, CISO & Engineering Leadership.

Common Assumptions

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

Prerequisites

1. OWASP Web Top 10 (2017 - 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.

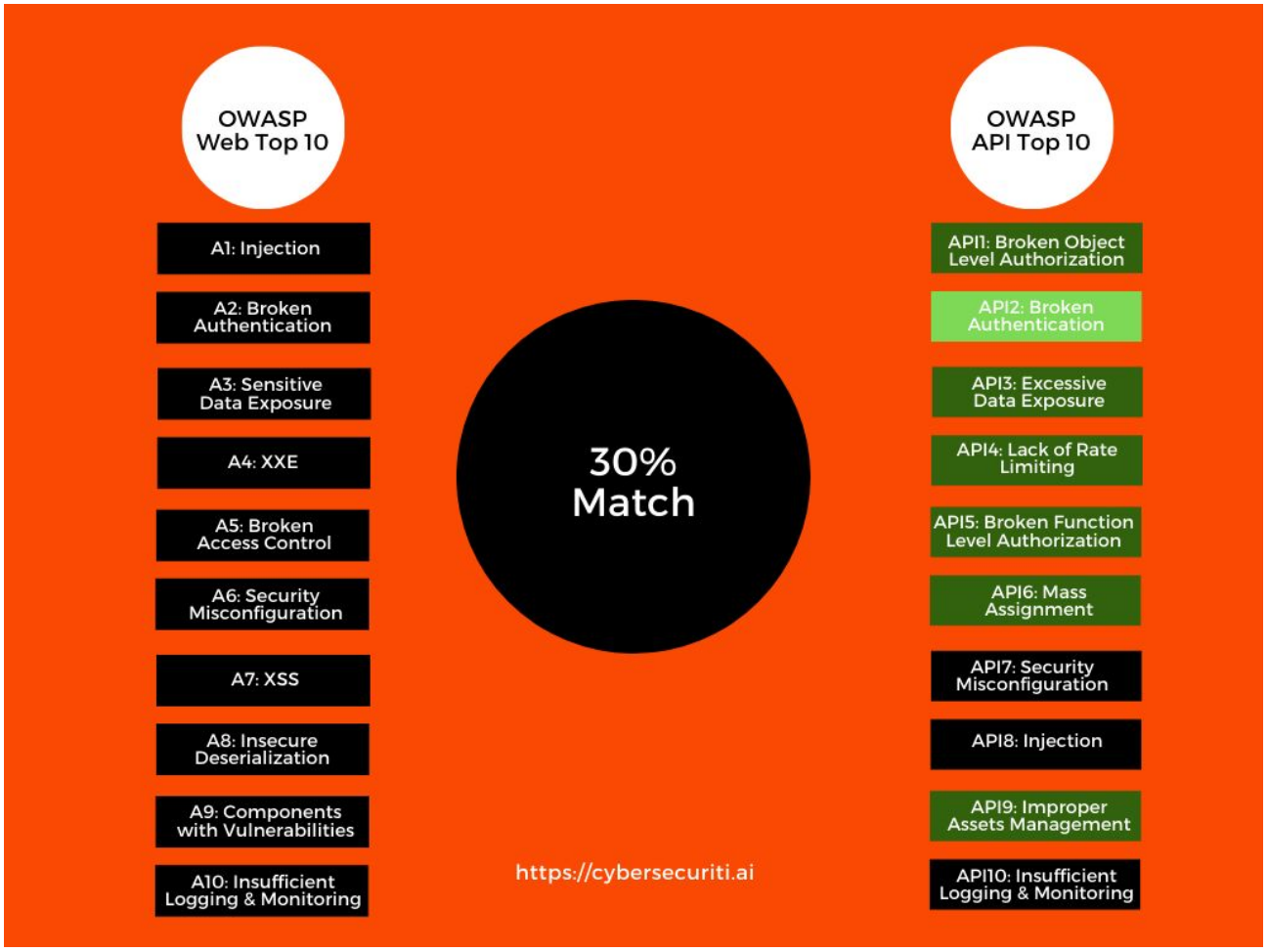
What's in OWASP Web Top 10

Rank	Name	Comments
A1	Injection	Make sure you've done some testing. Otherwise, the reported bugs volume can overwhelm you.
A2	Broken Authentication	It is critical, so you don't regress and end up paying for the same thing again and again.
A3	Sensitive Data Exposure	Can easily detect a wide array of issues early on and allow you to fix and release them at your pace.
A4	XML External Entities (XXE)	Can be lengthy and most done just before the release.
A5	Broken Access Control	Make sure you run automated scans as you build and ship new software.
A6	Security Misconfiguration	Train engineering on security best practices and top 10 vulnerabilities best practices. Otherwise, simple fixes can end up taking 10x time.
A7	Cross-Site Scripting (XSS)	You need to identify a yearly $100K - $200K budget for this even if you're just getting started.
A8	Insecure Deserialization	Identify engineering resource who can triage, assign, fix, and ship accordingly.
A9	Using Components with Known Vulnerabilities	Don't have a too rigid nor a wide-open policy around what type of issues are acceptable like XSS, SQL, etc. Otherwise, you'll miss out on new threats or your team will be overwhelmed with new problems which they don't know how to fix.
A10	Insufficient Logging & Monitoring	The key here is to maintain enough logging, continuous observation and tracking using integrated incident management tools so that breaches can be detected both early and internally within the organization.

What's in OWASP API Top 10

Rank	Name	Comments
API1	Broken Object Level Authorization	Add authorization checks using either policies or by verifying roles at the data or the object layer.
API2	Broken Authentication	Use strong passwords with encrypted storage, session timeout management and authentication token invalidation implementations.
API3	Excessive Data Exposure	Identifying and classifying data properties will help in strategizing what exactly is needed to be sent to users. Masking irrelevant fields and preventing cache also helps here.
API4	Lack of Resources & Rate Limiting	DDoS/DoS severely impacts businesses with immediate consequences, AI techniques can help here in identifying and accordingly configuring incoming requests for data/operations.
API5	Broken Function Level Authorization	You will require a comprehensive automated scan and test to verify all possible permutations and combinations of your organization access policies.
API6	Mass Assignment	Using generic serialization/deserialization implementations can make you susceptible to overriding protected fields.
API7	Security Misconfiguration	Having a checklist to verify all configurations before production-ready can eradicate most of these types of flaws.
API8	Injection	Custom Validations and Parameterization can prevent these attacks to a great extent.
API9	Improper Assets Management	Document all deployments and limit/phase out the older ones.
API10	Insufficient Logging & Monitoring	Securing Logs, making sure all required information gets logs and consider integration with other tools for timely alerts.

Comparison



Conclusion

- Most Web security threats did not make it to the API top 10.
- Broken Authentication retained as Top 2 but API challenges are a bit different than the web.
- Security Misconfiguration dropped one point to no. 7 position in the APIs top 10 list.
- Injection threat dropped 8 points to no.8 position
- Insufficient Logging & Monitoring is more of a compliance check and it retained the no. 10 position
- Overall there is only a **30%** 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/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf