Nov 10
2023

THE MOBILE APPLICATION SECURITY COMMANDMENTS BY HEART...

#dcKe23

With:

Tanui [themadbit]

WHOMAI (WHY ME?)

Junior Security Analyst,
Yelbridges (was)

Research Assistant,
CeDReCS (is)

@themadbit

EDITOR’S NOTE

No photo. Why snap a picture when you can have a live performance? I invited the audience to gaze upon me instead.

MOBILE SECURITY & TESTING (Q/A)

How do you stay updated with the latest Android security vulnerabilities?

What kind of security testing do you perform on your Android applications?

What are the potential risks of improper implementation of OAuth in Android apps?

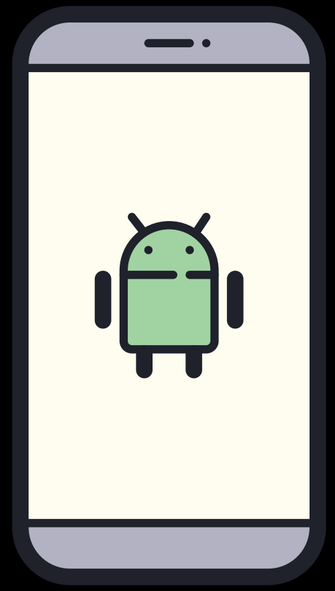
MAS OWASP

mas.owasp.org

STRUCTURE OF THE COMMANDMENTS(mas owasp)

MASVS

(SYLLABUS)



(EXAM)

MASTG

(MARKING SCHEME)

EDITOR'S NOTE

To paint a clearer picture of MAS OWASP, I used an analogy. I think it helped the audience understand better how they'd approach the security verification standard & the testing guide.

MASVS

The OWASP MASVS (Mobile Application Security Verification Standard) is the industry standard for mobile app security. It can be used by mobile software architects and developers seeking to develop secure mobile applications and security testers to ensure completeness and consistency of test results.

MASVS CONTROL GROUPS/DOMAINS

MASVS-STORAGE: Secure storage - (data-at-rest).

MASVS-CRYPTO: Cryptographic functionality.

MASVS-AUTH: Authentication and authorization.

MASVS-NETWORK: Secure network communication - (data-in-transit).

MASVS-PLATFORM: Underlying mobile platform and other installed apps.

MASVS-CODE: Security best practices for data processing and keeping the app up-to-date.

MASVS-RESILIENCE: Resilience to reverse engineering and tampering attempts.

LAYERS OF IMPLEMENTATION

Different apps need different levels of security...

CASE IN POINT

STORAGE

MASVS-STORAGE-1

-

app securely stores sensitive data

MASVS-STORAGE-2

-

app prevents leakage

cont... CASE IN POINT

AUTHENTICATION

MASVS-AUTH-1

-

app uses secure authentication and authorization

MASVS-AUTH-2

-

app performs local authentication

MASVS-AUTH-3

-

app secures sensitive operations

MASTG

The OWASP Mobile Application Security Testing Guide (MASTG) is a comprehensive manual for security testing and reverse engineering. It describes technical processes for verifying the controls listed in the OWASP MASVS.

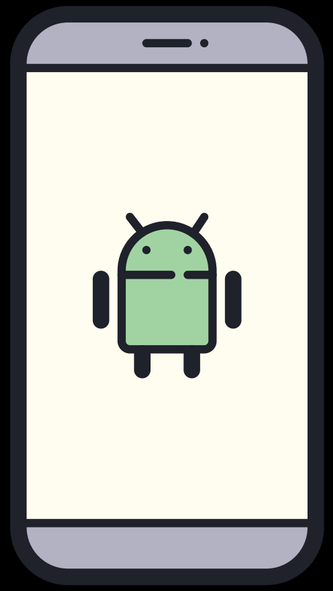
EXPLORING THE TEST GUIDE

Tests
Techniques
Tools
Apps

STRUCTURE OF THE COMMANDMENTS

MASVS

(SYLLABUS)



(EXAM)

MASTG

(MARKING SCHEME)

DEMO

EDITOR'S NOTE

During the demo, I helped the audience understand some of the tools, techniques, and apps that we can use to test for potential vulnerabilities our apps have.

and the gods were with me....

RESOURCE(S)

mas.owasp.org

marktanui.com