

How To Build Security

IN FRONTEND DEVELOPMENT?



> _ Whoami: Arlindo Cossa Junior

Arlindo Cossa Júnior is a professional with international experience in Cybersecurity consulting / MSSP, speaker/instructor/mentor on Information Security @ Cyber Security Manager at ATHSec.



<u>@</u>SwagneyCod3











. Schedule:

- 1. Overview
- 2. Front End Application Security Risk Overview
- 3. Secure Software Development Life Cycle SSDLC
- 4. Process Models and Framework
- 5. Hands on Practical Code Security Review
- 6. Any Questions?





. Say something about application security





Some front end vulnerabilities



CSRF

is a browser exploit where an attacker tricks someone into executing unwanted actions against a website to which their browser is already authenticated.

CSS INJECTION

CSS Injection vulnerability involves the ability to inject arbitrary CSS code in the context of a trusted web site which is rendered inside a victim's browser.

XSS

This is a rather widespread set of vulnerabilities that allow an attacker to pass malicious code as input to some input field in the app.

Third Party Libraries

Third-party libraries can improve your app, but you may run the risk of introducing flawed and vulnerable applications to your APP





. What are the causes of insecure apps?

- 1. sloppy programmers
- 2. Not meeting the minimum security requirements
- 3. Deploy faulty applications





1. How to Build Application Security From Scratch?





Requirements

In this initial phase, requirements for new features are collected from various stakeholders, identifying all possible risks.

Design

The design phase involves using established patterns of application architecture and software development.

05 01 04 03 02

3. Software Development Life Cycle "SDLC"

Maintenance and evolution

Progressive Application Security

Verification

he Verification phase is where applications go through a thorough testing cycle to ensure they meet the original design & requirements.

Development

When it's time to actually implement the design and make it a reality, concerns usually shift to making sure the code well-written from the security perspective.



. What is a Secure SDLC?

- 1. sloppy programmers
- 2. Not meeting the minimum security requirements
- 3. Deploy faulty applications





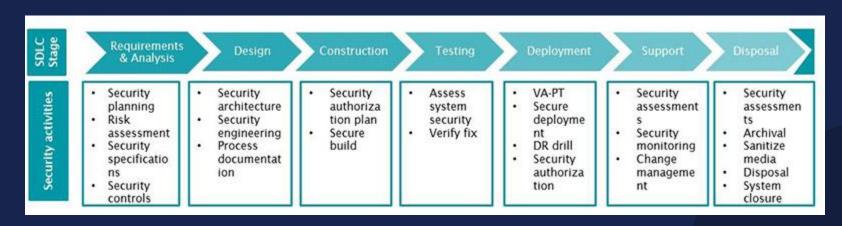
The Importance of a Secure SDLC

- 1. sloppy programmers
- 2. Not meeting the minimum security requirements
- 3. Deploy faulty applications





. Secure Software Development Life Cycle " SSDLC "





Process Models and Framework

- 1. **SDLC Models:** Agile, Waterfall, V-Shaped, Iterative, Spiral
- 2. Frameworks: NIST SDSF





We can Hack Some App's?



Thanks for listening!





Maputo Frontenders

@mptfrontenders



. Roadmap

- 1. Make the initial business case.
- 2. Adopt a formal process to build security into the SDLC.
- 3. Have a plan for the implementation.
- 4. Integrate Software Security with Information Security Risks.
- 5. Review the business case and commit to it.