Mobile Education Cybersecurity on the Educado App

Luiza, Mai, Marc, Yasmim and Zohra

whoami

Aalborg University

Marc T. Poulsen (BSc, Cyber- and Computer technology)

Cherie Mai Caloyloy Hansen (MSc, Cyber Security)

Zohra Amini (MSc, Cyber Security)

Universidade de Brasília

Luiza Oliveira de Araujo (BSc, Engenharia de Produção)

Yasmim Bezerra Oliveira Altoé (BSc, Engenharia de Produção)

The Problem(s)

How can security be implemented on the Educado App?

Cyber Security and Privacy

Cyber Security

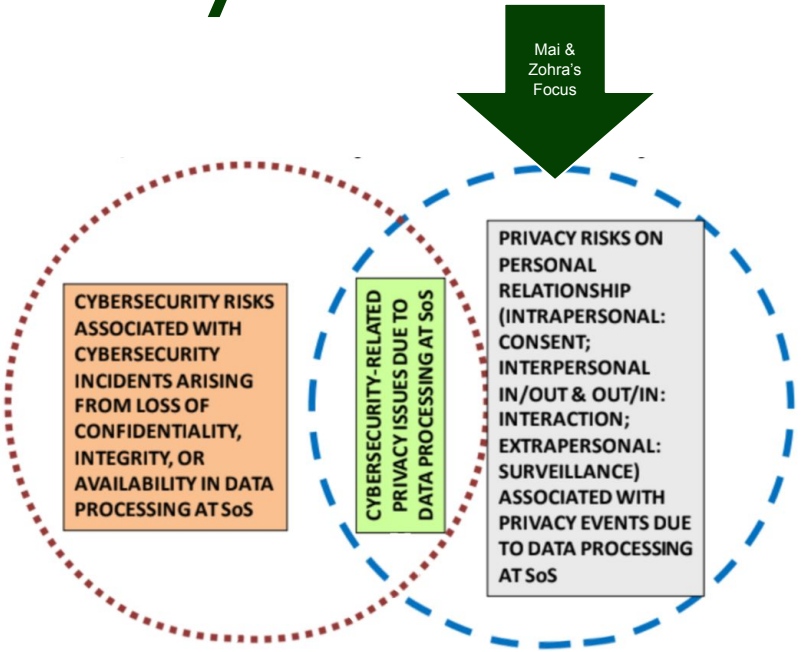
- Incidents with loss of confidentiality, integrity or availability

Privacy

- Protecting relationships and requires consent

Intersection between both

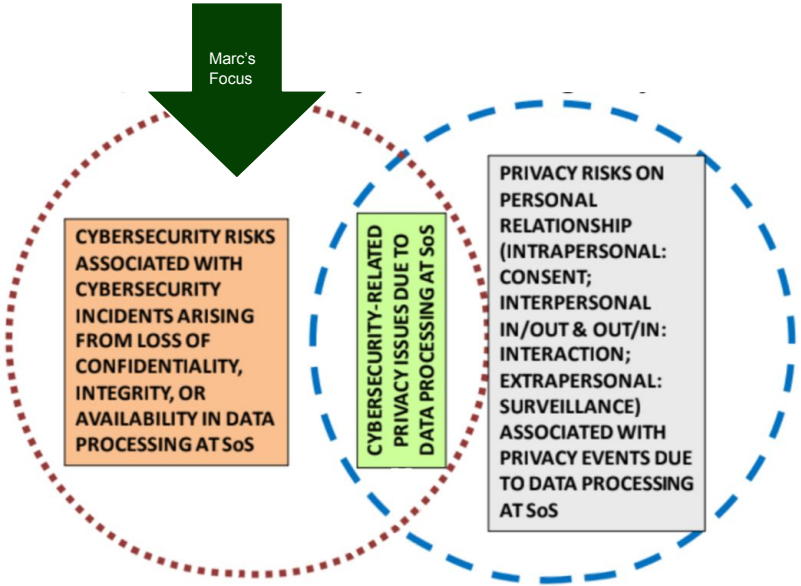
- Cyber security & privacy issues in data processing



Source: João Mello Da Silva & Paulo Celso Dos Reis Gomes, 2022

General app security

- Research/gather data
- Test Educado app
- Implement security based on priority



Source: João Mello Da Silva & Paulo Celso Dos Reis Gomes, 2022

Platform: EDUCADO

- Mobile Application
- Web Application
- One backend and database

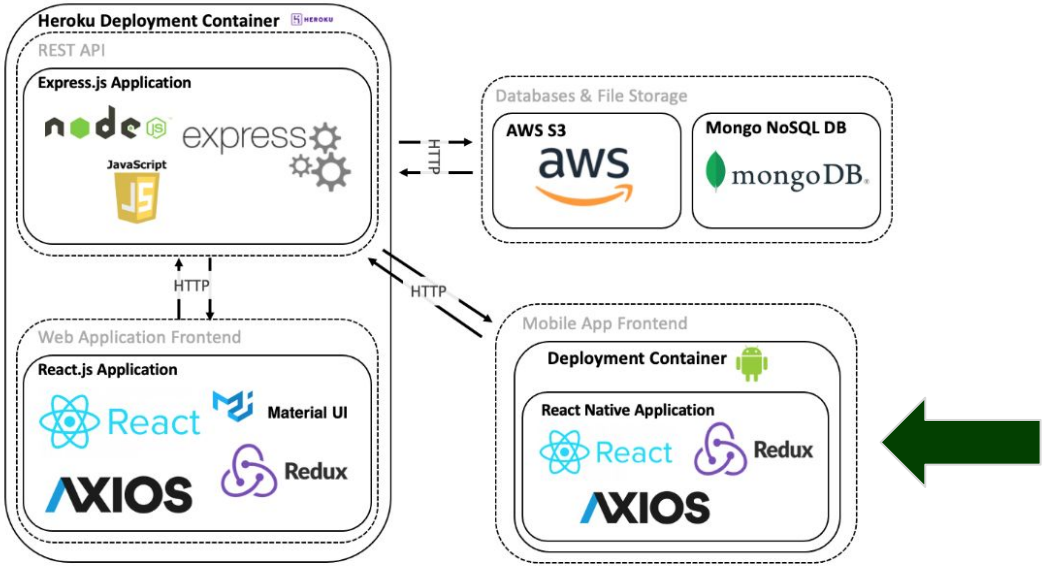


Figure 7.2: Solution microservices architecture

Cite: "*Daniel Britze and Jacob Vejlin Jensen, Digital learning platform for waste- pickers in Brazi, spring semester 2021*"

Integrated Recycling Complex

Script

Interview

The waste picker did not know what LGPD is

On a scale of 0 to 10, the waste picker rated the importance of privacy to be 8

Privacy was important to him only in bank related Apps

The waste picker use only one password to all Apps

LGPD

Differences:

- 10 legal basis for Data Processing
- No storage limitations
- 30 day time limit for businesses to respond to access requests from data subjects
- Not clear whose task it is

Similarities:

- Applies to Data Controllers and Data Processors

GDPR

Differences:

- 6 Legal basis for Data Processing
- Storage limitations
- 15 day time limit for businesses to respond to access requests from data subjects
- Clear where responsibilities lie for enforcement of the law

Similarities:

- Applies to Data Controllers and Data Processors

Research and test

Testing EDUCADO security (OWASP web application top 10 security risk)

- Best practice + standards (for app + cloud)
- Typical attacks on apps
- Security assessment of the Educado App

Source:
https://detectify.com/lpp/owasp?creative=606442759437&keyword=owasp%20top%2010&matchtype=b&network=g&device=c&gclid=CjwKCAiAoL6eBhA3EiwAXDom5gpGfbknZAhmgkHE8a6YGYnZiRqCp1GaNw8tvpCbCJQNqPai_uPqVRoCVKUQAvD_BwE

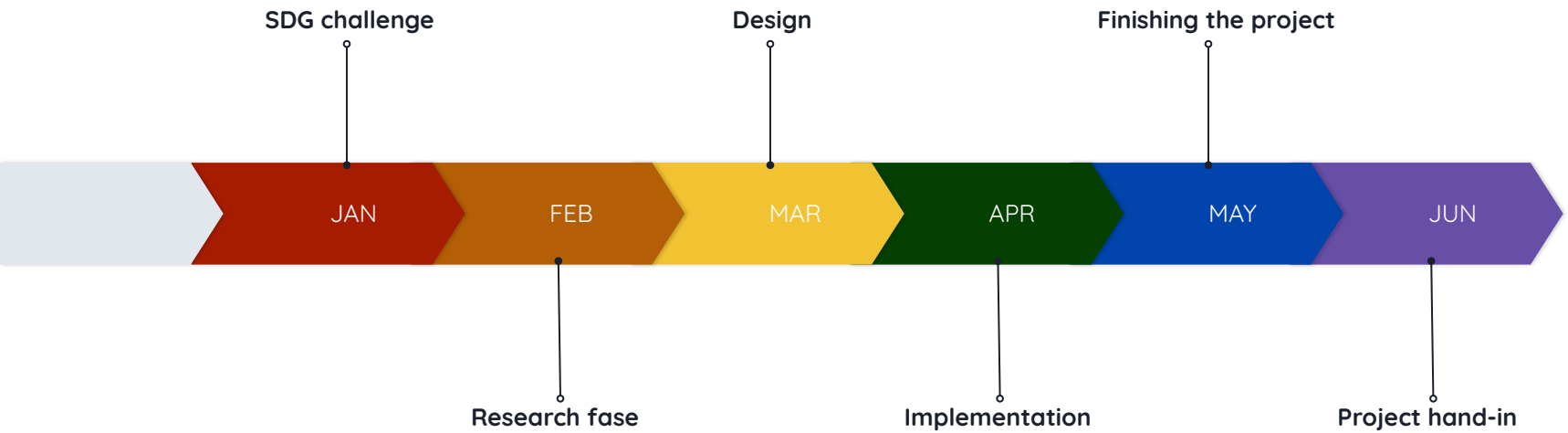
https://www.zscaler.com/blogs/product-insights/what-owasp-top-10

OWASP web application top 10 security risk

1. **Broken Access Control:** Bad control to datasystem
2. **Cryptographic Failures:** Use of weak or no cryptography
3. **Injection:** no protection against malicious input to the database
4. **Insecure Design:** flawed architecture, lack of threat modeling, secure design patterns, and reference architectures.
5. **Security Misconfiguration:** insecure component configuration that can be classified as security misconfiguration.
6. **Vulnerable and Outdated:** Operating system, CMS, web server, plugin, or library used by a plugin.
7. **Identification and Authentication Failures**: all kinds of flaws caused by authentication and/or session management errors.
8. **Software and Data Integrity Failures:** assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity.
9. **Security Logging and Monitoring Failures:** This category is to help detect, escalate, and respond to active breaches.
10. **Server-Side Request Forgery(SSRF) flaws:** occur when a web application fetches a remote resource without validating the user-supplied URL.

Source:
https://detectify.com/lpp/owasp?creative=606442759437&keyword=owasp%20top%2010&matchtype=b&network=g&device=c&gclid=CjwKCAiAoL6eBhA3EiwAXDom5gpGfbknZAhmgkHE8a6YGYnZiRqCp1GaNw8tvpCbCJQNqPai_uPqVRoCVKUQAvD_BwE

Milestones


SDG challenge
Design
Finishing the project
JAN
FEB
MAR
APR
MAY
JUN
Research fase
Implementation
Project hand-in

Thanks