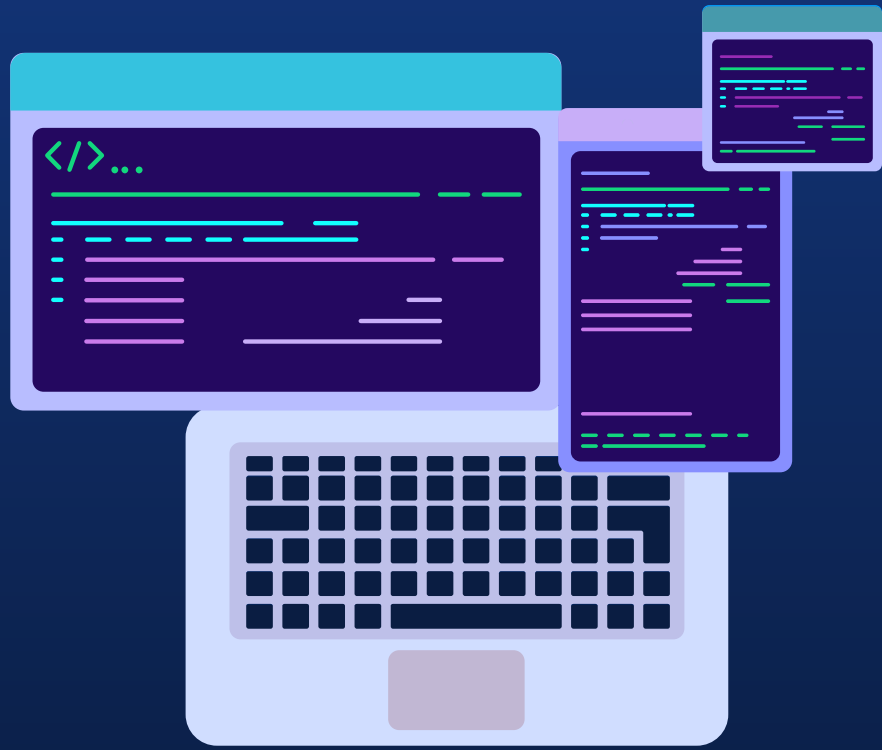
SEGURANÇA E QUALIDADE PODEM ANDAR JUNTAS?



Larissa Fabião da Fonseca

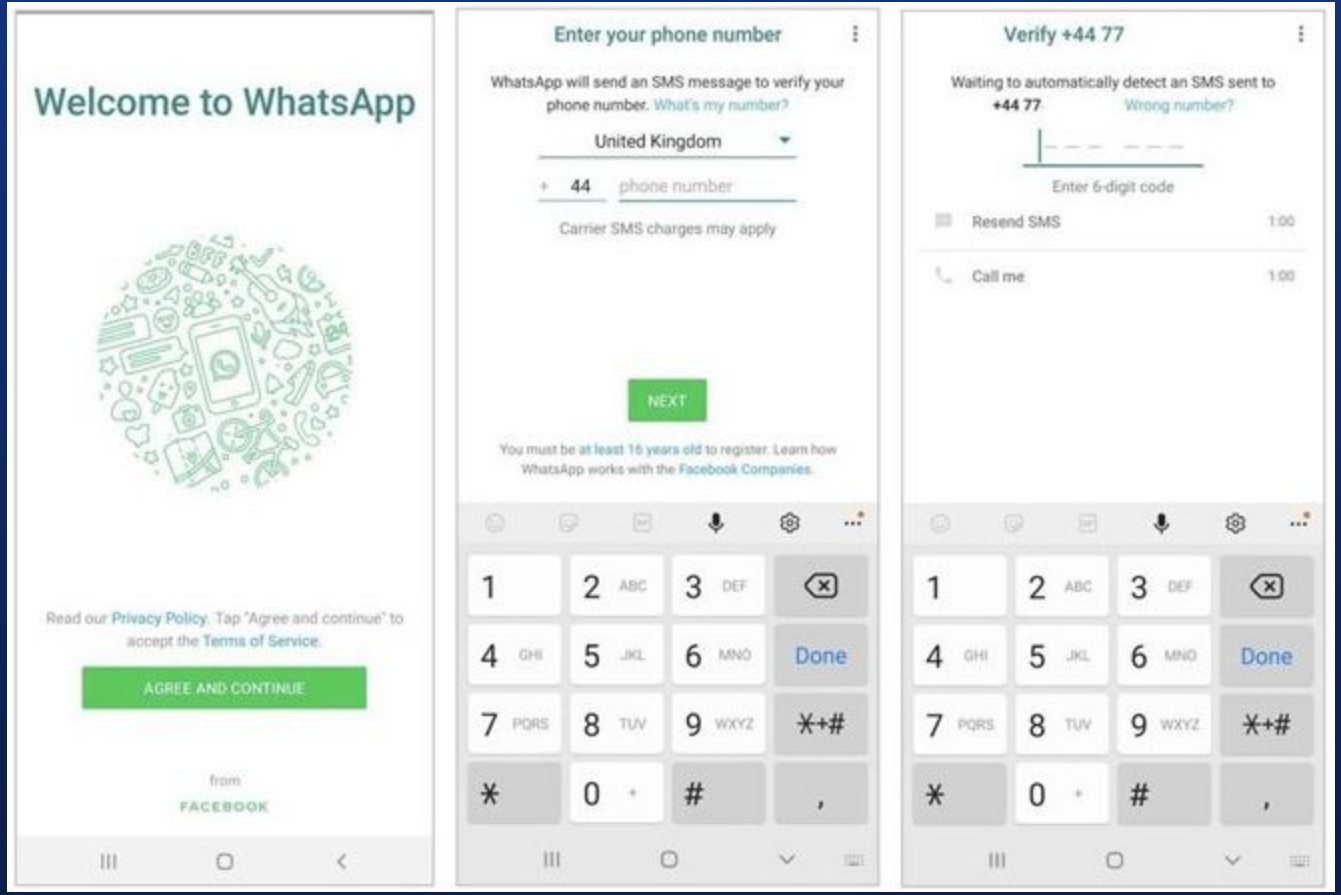
Analista de Segurança da Informação | QA
Zup Innovation

https://www.linkedin.com/in/larissa-fonseca/

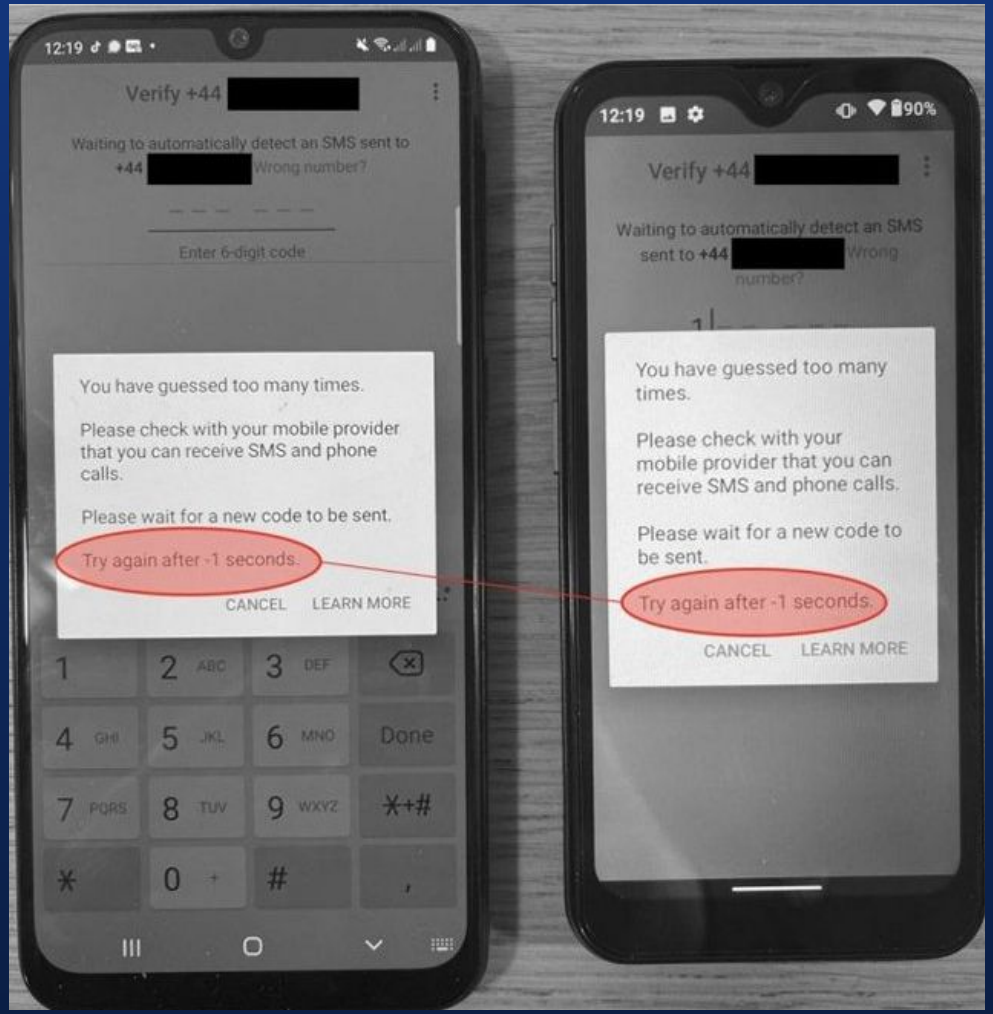
https://github.com/larissafabiao

01

ENTENDENDO A MOTIVAÇÃO



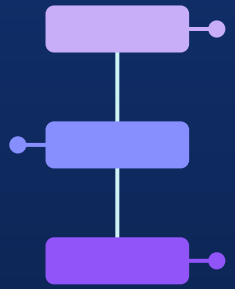
https://www.forbes.com/sites/zakdoffman/2021/04/10/shock-new-warning-for-millions-of-whatsapp-users-on-apple-iphone-and-google-android-phones/?sh=545fb4e27585


12:19
Verify +44 [redacted]
Waiting to automatically detect an SMS sent to +44 [redacted] Wrong number?
Enter 6-digit code
You have guessed too many times.
Please check with your mobile provider that you can receive SMS and phone calls.
Please wait for a new code to be sent.
Try again after -1 seconds.
CANCEL
LEARN MORE
Done
12:19
90%
Verify +44 [redacted]
Waiting to automatically detect an SMS sent to +44 [redacted] Wrong number?
You have guessed too many times.
Please check with your mobile provider that you can receive SMS and phone calls.
Please wait for a new code to be sent.
Try again after -1 seconds.
CANCEL
LEARN MORE

COMO EVITAR ESSA SITUAÇÃO?

MODELAGEM DE AMEAÇAS

Entender os riscos do modelo de negócio adotado



TESTES EXAUSTIVOS

Testar exaustivamente a ferramenta nos mais diversos cenários

TESTES DE SEGURANÇA

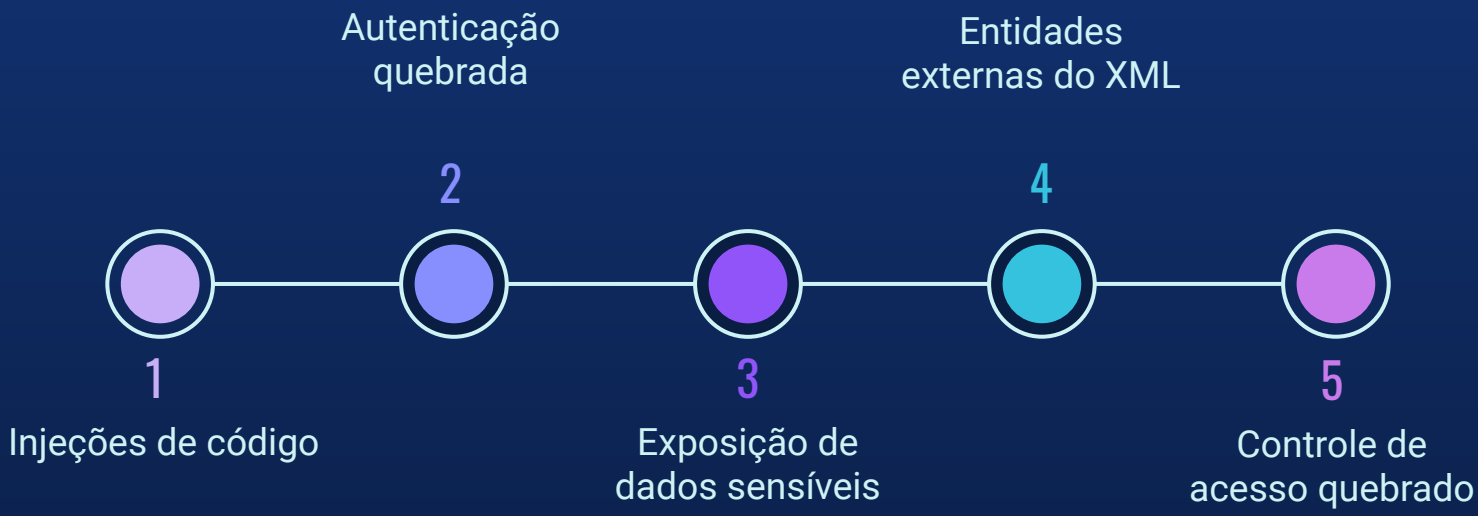
Explorar os cenários alternativos em testes focados em segurança

02

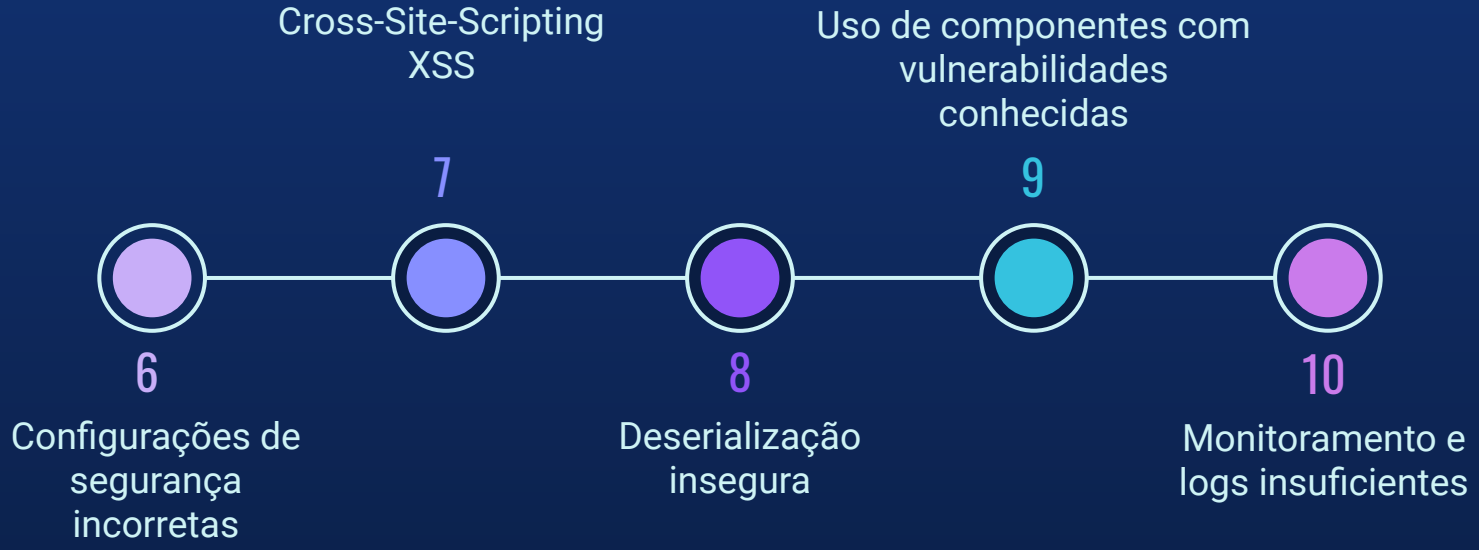
COMO TESTAR A SEGURANÇA?


OWASP
Open Web Application
Security Project

OWASP TOP 10 WEB



OWASP TOP 10 WEB



OWASP

Open Web Application Security Project

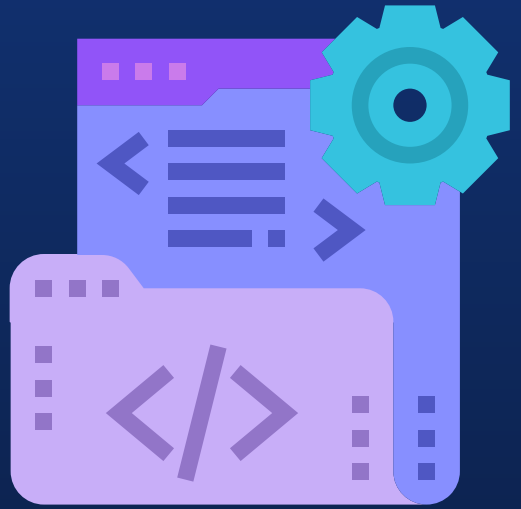
WEB SECURITY TESTING GUIDE

BDD SECURITY

```
@iriusrisk-cwe-614
Scenario: Set the 'secure' flag on the session cookie
  Given a new browser or client instance
  When the default user logs in
  And the user is logged in
  Then the session cookie should have the secure flag set
```

03

E A SEGURANÇA DO TESTE?



E A SEGURANÇA DO TESTE?

PROBLEMA

Como podemos evitar que os testes de qualidade levem a mais vulnerabilidades no nosso sistema?

Solução

Testando o código de testes com ferramentas de Análise de código e com o uso de boas práticas de programação

Uma ferramenta de SAST (Static Application Security Testing) tem o objetivo de analisar o código fonte ou mesmo suas versões compiladas de código, buscando nestes falhas que possam comprometer a segurança


Horusec


sonarqube

E AS MASSAS?

E AS MASSAS?

NECESSÁRIAS PARA TODOS OS TESTES

Fazem parte das automações

DIFEREM DE ACORDO COM O AMBIENTE

É comum termos diferentes massas para diferentes ambientes

GERALMENTE FICAM HARD CODED

Normalmente armazenadas em arquivos json e yaml

→ APONTADO COMO PROBLEMA DE SEGURANÇA POR FERRAMENTAS SAST

AWS SECRET MANAGER

Solução para armazenar segredos na nuvem

LINKS ÚTEIS

- BDD Security
- VAmPi
- OWASP testing guide
- OWASP top ten web
- OWASP ZAP
- Horusec

THANKS

https://www.linkedin.com/in/larissa-fonseca/

https://github.com/larissafabiao