FGA 0238 - Testes de Software – T01 **Semestre:** 2024.1

Nome: João Eduardo Pereira Rabelo **Matrícula:** 180053299

Equipe: NeverMind

Estudo Individual – Teste de Segurança / DevSecOps

No que se refere à leitura do capítulo do “Web Security Testing Guide v4.2”, é iniciado apresentando o Projeto de Testes da OWASP (Open Web Application Security Project). Este projeto foi desenvolvido para ajudar a entender o que, por que, quando, onde e como testar aplicações web. Diferente de um simples checklist, ele oferece uma estrutura completa que pode ser usada como modelo para criar programas de teste ou avaliar processos já existentes.

O guia descreve em detalhes tanto a estrutura geral de teste quanto as técnicas necessárias para implementar essa estrutura na prática. Escrever o guia foi desafiador devido à necessidade de consenso entre os participantes e à complexidade de criar conteúdo aplicável em diferentes ambientes e culturas. Um dos objetivos foi mudar o foco dos testes de aplicações web de testes de penetração isolados para testes integrados no ciclo de vida do desenvolvimento de software.

O projeto OWASP Testing Framework é validado por muitos especialistas da indústria e profissionais de segurança, alguns dos quais são responsáveis pela segurança de software em grandes empresas. Este framework ajuda as organizações a testarem suas aplicações web para construir software confiável e seguro, destacando áreas de fraqueza e ajudando a fazer decisões informadas sobre técnicas e tecnologias de teste.

A introdução também aborda os pré-requisitos para testar aplicações web e o escopo dos testes, além de princípios e técnicas de teste bem-sucedidos, melhores práticas para relatórios e justificativas de negócios para testes de segurança.

Por fim, o capítulo discute a dificuldade de medir a segurança, citando que "não se pode controlar o que não se pode medir". Medir a segurança é um processo notoriamente difícil, mas essencial para o controle e melhoria da segurança do software.

Já no material "Six Pillars of DevSecOps", foi lido e retirados os seguintes pontos de importância para o leitor:

- **Introdução** A automação é crucial no DevSecOps para integrar a segurança ao ciclo de desenvolvimento de software, aumentando a eficiência dos processos e permitindo uma resposta rápida às ameaças cibernéticas.

- **Objetivo** Fornecer um framework que permita a integração da segurança de forma automatizada ao ciclo de vida do desenvolvimento de software, melhorando a eficiência e equilibrando as necessidades de desenvolvimento e segurança.
- **Público-alvo** Gerentes e operadores de risco, segurança da informação e TI, incluindo executivos (CISO, CIO, CTO, CRO, COO, CEO) e profissionais de DevSecOps, automação, DevOps, garantia de qualidade, segurança da informação, governança, gestão de risco, mudança e conformidade.
- **Escopo** Descrever a necessidade da automação de segurança, técnicas de automação de testes de segurança e mecanismos para alcançá-la, além de esclarecer equívocos comuns sobre testes de segurança no contexto de DevSecOps.
- **Referências Normativas** Inclui referências como ISO/IEC 27000:2018 e publicações da CSA.
- **Termos e Definições** Define termos como Análise de Composição de Software (SCA), Teste de Segurança de Aplicação Estático (SAST), Teste de Segurança de Aplicação Dinâmico (DAST), entre outros.
- **Pipeline de Entrega de Software da CSA DevSecOps** Apresenta uma estrutura com estágios, gatilhos e atividades, detalhando as práticas recomendadas para a integração de testes de segurança automatizados no pipeline de desenvolvimento de software.
- **Melhores Práticas de Automação** Inclui práticas como mitigação de vulnerabilidades, testes assíncronos, loops de feedback contínuos e a importância de não comprometer a construção do software.