

**Aluno:** Guilherme Soares Rocha

**Matrícula:** 211039789

## **Testes de software**

### **Módulo 5 – estudo individual**

Aplicações web são sistemas complexos que podem ser vulneráveis a uma ampla gama de ataques. Para garantir a segurança das aplicações web, é importante realizar testes de segurança de forma regular.

O guia de teste de segurança de aplicações web do OWASP é uma referência abrangente para profissionais de segurança e desenvolvedores que desejam testar a segurança de aplicações web. O guia aborda uma ampla gama de vulnerabilidades de segurança de aplicações web, incluindo:

- Vulnerabilidades de injeção, como SQL injection e cross-site scripting (XSS)
- Vulnerabilidades de autenticação e autorização, como força bruta e sequestro de sessão
- Vulnerabilidades de integridade e disponibilidade, como ataques de negação de serviço (DoS)

O guia também recomenda o uso de técnicas de teste automatizadas para aumentar a eficiência e a escalabilidade dos testes de segurança. O guia também enfatiza a importância da colaboração entre desenvolvedores e segurança para garantir que as aplicações web sejam seguras.

Os objetivos do guia são:

- Fornecer uma visão geral dos princípios e práticas de teste de segurança de aplicações web
- Abordar uma ampla gama de vulnerabilidades de segurança de aplicações web
- Recomendar o uso de técnicas de teste automatizadas
- Enfatizar a importância da colaboração entre desenvolvedores e segurança
- Vantagens de testar a segurança de aplicações web
- As vantagens de testar a segurança de aplicações web incluem:
- Reduzir o risco de ataques cibernéticos
- Proteger a privacidade dos dados do usuário
- Manter a reputação da empresa

O guia de teste de segurança de aplicações web do OWASP é uma ferramenta valiosa para profissionais de segurança e desenvolvedores que desejam testar a segurança de aplicações web. O guia fornece uma visão abrangente dos princípios e práticas de teste de segurança, e aborda uma ampla gama de vulnerabilidades de segurança.

O documento Os Seis Pilares do DevSecOps: Automação, da Cloud Security Alliance, discute a importância da automação no DevSecOps. O documento argumenta que a automação é essencial para alcançar a segurança reflexiva, que é a capacidade de identificar, proteger, detectar, responder e se recuperar continuamente de ameaças cibernéticas.

O documento fornece um framework para automatizar atividades de segurança ao longo do ciclo de vida de desenvolvimento de software. O framework inclui cinco classes de atividades de segurança:

- Segurança do design: A segurança deve ser projetada desde o início. As falhas de design são conhecidas por representar uma grande parcela das vulnerabilidades.
- Segurança do código: Vulnerabilidades podem surgir de um código mal escrito, independentemente de quão bem pensada e robusta seja a arquitetura de segurança de um aplicativo.
- Segurança dos componentes de software: Um aplicativo só pode ser tão seguro quanto seus componentes. As vulnerabilidades de seus componentes, sejam produzidos internamente, por terceiros ou de projetos de código aberto, provavelmente comprometerão o aplicativo maior.
- Segurança de aplicações: As aplicações devem ser testadas e verificadas quanto a vulnerabilidades.
- Segurança do ambiente: O ambiente de execução de um aplicativo também deve ser seguro.

O documento também discute a importância de pipelines priorizados por risco. Isso significa que o nível de escrutínio de segurança deve ser adaptado ao risco do aplicativo. Por exemplo, aplicativos que lidam com dados sensíveis devem ser submetidos a testes de segurança mais rigorosos do que aplicativos que não o fazem.

Por fim, o documento fornece diretrizes para a implementação da automação em um ambiente DevSecOps. Essas diretrizes incluem começar pequeno e construir gradualmente, usar ferramentas de código aberto sempre que possível e integrar a automação na pipeline de entrega existente.

A automação é uma ferramenta essencial para o DevSecOps. Ela permite que as organizações implantem software de forma mais segura e eficiente. O framework e as diretrizes fornecidas pelo documento Os Seis Pilares do DevSecOps: Automação podem ajudar as organizações a implementar a automação com sucesso em seu ambiente DevSecOps.