



GUIA DO CANDIDATO – SFSD

Security Forge Software Developer

1. Apresentação

A certificação **SFSD (Security Forge Software Developer)** é voltada para profissionais da área de desenvolvimento de software que desejam comprovar competências essenciais em **segurança no ciclo de vida do desenvolvimento (Secure SDLC)**, codificação segura, análise de vulnerabilidades e boas práticas em segurança de aplicações.

A **prova é realizada anualmente**, e o **direito de participação somente pode ser adquirido por meio da nossa loja oficial**. Ao adquirir o direito de certificação, o candidato terá acesso às informações oficiais sobre a data da prova, estrutura e instruções. Ressaltamos que **a compra não garante a certificação**, apenas o direito de realizar a avaliação.

A loja também disponibiliza **cursos preparatórios específicos** para a trilha SFSD, voltados à capacitação técnica nos temas exigidos.

2. Estrutura da Avaliação

A certificação SFSD é composta por duas etapas:

- **Prova Teórica:** 30 questões de múltipla escolha. É necessário **acertar no mínimo 80%** (24 questões) para ser aprovado.
- **Desafio Prático de Programação:** O candidato deverá desenvolver e entregar uma aplicação funcional ou script, respeitando critérios de segurança, boas práticas de codificação e especificações do problema.

A prova prática será corrigida com base na funcionalidade, segurança, organização do código e aderência às boas práticas de desenvolvimento seguro.



3. Conteúdos Abordados

A certificação SFSD abrange temas fundamentais e práticos relacionados a **desenvolvimento seguro de software**, incluindo:

- Fundamentos de segurança da informação para desenvolvedores
- Princípios do Secure Software Development Life Cycle (Secure SDLC)
- Ameaças comuns segundo OWASP Top 10
- Boas práticas de codificação segura (input validation, encoding, etc.)
- Gestão segura de autenticação e sessões
- Criptografia aplicada no desenvolvimento
- Gestão de erros e exceções seguras
- Proteção contra injeções (SQL, comando, LDAP, etc.)
- Segurança em APIs e microsserviços
- Ferramentas e técnicas de análise estática e dinâmica de código
- Revisão de código seguro (code review)
- Vulnerabilidades em aplicações web e mobile
- Gestão de dependências e bibliotecas externas
- Práticas DevSecOps (segurança na esteira CI/CD)
- Controle de versão e histórico seguro (Git)

4. Requisitos Técnicos

O candidato deve estar apto a:

- Desenvolver scripts ou aplicações simples com foco em segurança.
- Utilizar ferramentas básicas de desenvolvimento e versionamento.
- Trabalhar com boas práticas de organização e documentação do código.
- Entregar o projeto dentro do prazo estipulado (geralmente 48h após liberação).
- Realizar build, teste e execução local da aplicação (instruções devem acompanhar o código enviado).

5. Avaliação

- **Nota mínima da prova teórica:** 80%.
- **Desafio prático:** Avaliado com base em critérios objetivos de segurança, funcionalidade e clareza do código.



- **Entrega:** Código-fonte comentado, documentação de uso e explicação das medidas de segurança adotadas.
-

6. Considerações Finais

- O candidato aprovado receberá certificado, número de registro e selo digital válido.
 - O exame é individual e sem consulta, sendo vetada qualquer forma de colaboração externa durante a execução.
 - A responsabilidade pela preparação é inteiramente do candidato; os cursos oficiais são opcionais, mas fortemente recomendados.
 - Quaisquer atualizações ou alterações no edital serão comunicadas exclusivamente pelos canais oficiais.
-

Loja oficial: <https://securityforge.org/loja/>

© 2025 – Equipe de Certificação SFOE