GOHACKING APPSEC, SECURE CODING AND DEVSECOPS

(GHSCD)

GoHacking

CYBER SECURITY TRAININGS

NÍVEL INTERMEDIÁRIO

Carga Horária: 40hs

GoHacking

(GHSCD)

Magno Logan

Cyber Security Specialist

Magno Logan é Especialista em Segurança da Informação, com foco em Segurança de Aplicações, e conta com mais de 15 anos de experiência no mercado. Atualmente, trabalha como Staff Security Engineer em uma healthtech do Canadá, onde tem focado na implementação do programa de Security Champions. Foi palestrante em conferências de segurança mundiais como DEFCON, OWASP AppSec, SecTor, NorthSec, NDC Security, TyphoonCon, Hackfest, H2HC e várias BSides no Brasil, no Canadá e nos EUA. Idealizador da JampaSec Security Conference e do capítulo da OWASP na Paraíba, onde atuou como líder por 5 anos. Também foi membro ativo do Grupo de Interesses Especiais de Segurança da Cloud Native Computing Foundation (CNCF SIG-Security) da OpenSSF (Open Source Security Foundation). Possui diversas certificações internacionais de Segurança, Nuvem e DevSecOps pela SANS, EC-Council, AWS, Azure, entre outras.

FORMAÇÃO:

Graduação em Tecnologia em Sistemas para Internet
INSTITUTO FEDERAL DA PARAÍBA - IFPB

Pós-Graduação em Segurança da Informação
FACULDADE DE TECNOLOGIA DE JOÃO PESSOA - FATEC-JP

Certificado em Forense Computacional
TC3, NY, EUA

CERTIFICAÇÕES:

- **GIAC Cloud Security Automation** *GCSA*
- **Microsoft Certified Azure Fundamentals** *AZ-900*
- **EC-Council Certified DevSecOps Engineer** *(ECDE)*
- **EXIN Secure Programming** *EXIN*
- **CompTIA Cybersecurity Analyst** *CYSA+*
- **EXIN Ethical Hacking Foundation** *EXIN*
- **CompTIA Penetratin Testing** *PENTEST+*
- **AWS Certified Solutions Architect – Associate** *SAA-C03*
- **CompTIA Cloud Essentials** *CLOUD ESSENTIALS+*
- **AWS Certified Cloud Practitioner** *CLF-C01*

GoHacking

(GHSCD)

Eduardo Santos

Instrutor Substituto
Especialista em Segurança de Aplicações

Eduardo Santos é Especialista em Segurança de Aplicações com ampla atuação no mercado, exercendo atualmente o papel de especialista de AppSec em uma multinacional. É professor desde 2007, onde já lecionou em cursos técnicos e de graduação. Atualmente ensina em cursos livres e de pós-graduação. Já palestrou em conferências nacionais e internacionais, como OWASP@Home, You Shot The Sheriff, GTS (NIC.br), BSides São Paulo, OSDFCon (EUA), entre outras.

FORMAÇÃO:

Doutorado em Engenharia da Computação
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE - UFRN

Mestrado em Engenharia da Computação
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE - UFRN

Especialização em Segurança de Redes de Computadores
ESTÁCIO

Graduação em Redes de Computadores
IFRN - (ALUNO LAUREADO)

CERTIFICAÇÕES:

EC-Council CEH
PRACTICAL

Microsoft Azure Fundamentals
AZ-900

CompTIA
PENTEST+

CompTIA
SECURITY+

GoHacking

(GHSCD)

O curso GoHacking AppSec, Secure Coding e DevSecOps (GHSCD) apresenta conceitos fundamentais sobre boas práticas de desenvolvimento seguro e de automação de segurança no processo de desenvolvimento.

Diariamente, novas falhas são descobertas em diversos sistemas, seja uma aplicação web ou mobile, um software customizado ou um componente de terceiros utilizado por uma aplicação. Durante muito tempo, e ainda nos dias atuais, é possível deparar-se com aplicações web ou mobile concebidas com fraquezas em seu processo de desenvolvimento.

Neste treinamento, serão abordadas técnicas básicas de desenvolvimento seguro, com os alunos adquirindo compreensão das vulnerabilidades de segurança de aplicações e aprendendo estratégias para se defender contra elas, por meio de controles proativos de desenvolvimento seguro.

Diversos temas serão abordados, como Segurança de Aplicações, Ciclo de Desenvolvimento Seguro (SDL), OWASP e seus projetos e ferramentas, Testes de Segurança de Aplicações, como DAST, SAST e SCA, CI/CD, Secret Scanning, Container Image Scanning, DevOps, DevSecOps e GitHub Actions, entre outros.

O GHSCD prepara o aluno para cursos mais avançados da GoHacking, como Ethical Hacking Web Exploitation and Security (EHWEB) e Ethical Hacking Modern Web Exploitation (EHMWX).

HABILIDADES

O que vou aprender?

- Entender os princípios básicos de DevOps, DevSecOps, Segurança de Aplicações e Desenvolvimento Seguro
- Entender o funcionamento e utilização de ferramentas SAST, DAST e SCA e como executá-las de forma automatizada na esteira de desenvolvimento
- Analisar códigos vulneráveis em nível da linguagem de programação e compreender, escrever e utilizar aplicações com segurança
- Entender o processo de exploração de vulnerabilidades em aplicações web referentes ao OWASP Top 10
- Analisar e identificar pontos de entrada vulneráveis em aplicações web e criar códigos que protejam contra essas falhas
- Entender os principais mecanismos de defesa contra vulnerabilidades web e aplicar técnicas básicas de automação da detecção e proteção dessas aplicações
- Aprender a utilizar o GitHub Actions para automação da sua pipeline e das ferramentas de segurança
- Utilizar ferramentas de detecção de vazamento de credenciais, segredos e outras informações sensíveis
- Utilizar ferramentas de análise de vulnerabilidades de imagens de containers

GoHacking

(GHSCD)

REQUISITOS

- Conhecimento básico de programação/lógica de programação
- Conhecimento básico de pelo menos uma linguagem de programação
- Conhecimento básico de ferramentas de gerenciamento de código-fonte como Git
- Conhecimentos básicos de HTTP e de aplicações web, HTML, CSS, JavaScript.
- Noções de Containers, Docker e YAML

PUBLICO ALVO

- Desenvolvedores de Software
- Especialistas em Segurança de Aplicações
- Engenheiros de Segurança
- Engenheiros de Software
- Arquitetos de Segurança
- Engenheiro DevOps e DevSecOps
- Programadores e Desenvolvedores de Aplicações
- Analistas de Segurança da Informação
- Penetration Testers de Aplicações e APIs
- Consultores de Segurança
- Pesquisadores de Segurança de Aplicações
- Profissionais de TI com interesse e afinidade na área de Segurança de Aplicações
- Entusiastas de Segurança de Aplicações
- Auditores de Segurança de Aplicações

GoHacking

(GHSCD)

CONTEÚDO ABORDADO

MÓDULO 101 (4h)

1. Segurança de Aplicações
   - O que é segurança de aplicações?
   - Desafios de se proteger aplicações
   - Estado da Segurança de Software

1.1 DevSecOps
   - Princípios e Práticas do DevSecOps
   - Ferramentas DevSecOps

1.2 Ciclo de Desenvolvimento Seguro (SDL)
   - Definição, Overview e Timeline
   - Práticas do SDL

MÓDULO 201 (16h)

2. OWASP

- *O que é e como funciona*
- *Capítulos e Projetos*
- *OWASP Juice Shop*

2.1- OWASP Top 10 v2025
- *Falhas de Controle de Acesso*
- *Falhas de Configuração de Segurança*
- *Falhas na Cadeia de Suprimentos de Software*
- *Falhas Criptográficas*

- *Falhas de Injeção*
- *Designo Inseguro*
- *Falhas de Autenticação*
- *Falhas de Integridade de Software ou Dados*
- *Falhas nos Logs e Alertas de Segurança*
- *Manipulação Incorreta de Condições Excepcionais*

2.2 OWASP Top 10 Controles Pró-Ativos v2024

- *Implemente Controle de Acesso*
- *Use Criptografia para proteger os dados*
- *Valide todas as Entradas e Trate as Exceções*
- *Aborde a segurança desde o início*
- *Configurações seguras por padrão*
- *Mantenha seus componentes seguros*
- *Identidades Digitais Seguras*
- *Aproveite os recursos de segurança do navegador*
- *Implemente logs e monitoramentos de segurança*
- *Elimine o SSRF*

2.3 Overview de outros Top 10s da OWASP

- *OWASP Top 10 para APIs*
- *OWASP Top 10 para LLMs*
- *OWASP Top 10 para CI/CD*

GoHacking

(GHSCD)

MÓDULO 301 (16h)

3. Testes de Segurança de Aplicações

3.1 Metodologias de Testes de Segurança

- *DAST*
- *SAST*
- *SCA*
- *Secret Scanning*
- *Container Image Scanning*

3.2 SCA no CI/CD

- *SBOM*
- *Grype e Syft*
- *Cadeia de Suprimentos (Supply Chain)*
- *OWASP Dependency Check*
- *GHAS (Dependabot)*
- *Snyk SCA*
- *Aikido*

3.3 SAST no CI/CD

- *Semgrep/OpenGrep*
- *GHAS (CodeQL) e CodeQL CLI*
- *Snyk Code*
- *Aikido*

GoHacking

(GHSCD)

3.4 DAST no CI/CD

- *ZAP*
- *Nuclei*
- *StackHawk*

3.5 Segredos e Credenciais

- *O problema do hardcoding*
- *Gerenciando Credenciais*
- *Git-leaks e TruffleHog*
- *GHAS (Secret Scanning)*
- *OWASP Wrong Secrets*

MÓDULO 401 (2h)

4.1 IaC Security

- *Terraform*
- *CloudFormation*
- *Checkov*
- *TFSec*
- *Kics*

MÓDULO 501 (2h)

5.1 Introdução a Containers: Overview e Componentes

5.2 Segurança de Containers

- *Scan de Dockerfiles*
  - *Hadolint*

GoHacking

(GHSCD)

- *Scan de Imagens*
  - *Trivy*
  - *Snyk*
  - *Grype*

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- *Entender os princípios básicos de Segurança de Aplicações*
- *Entender os princípios básicos de Desenvolvimento Seguro*
- *Entender o funcionamento e utilização de ferramentas SAST, DAST e SCA*
- *Entender a arquitetura de uma aplicação web*
- *Entender os fundamentos do Protocolo HTTP*
- *Entender o funcionamento da OWASP*
- *Compreender, escrever e utilizar aplicações com segurança*
- *Utilizar Web Proxies para análise de aplicações web*
- *Analisar códigos vulneráveis em nível da linguagem de programação*
- *Entender o processo de exploração de vulnerabilidades em aplicações web*
- *Compreender vulnerabilidades do OWASP Top 10*
- *Analisar e identificar pontos de entrada vulneráveis em aplicações web*
- *Criar códigos que protejam contra as falhas do OWASP Top 10*
- *Entender os principais mecanismos de defesa contra vulnerabilidades web*
- *Entender técnicas básicas de automação da detecção e proteção dessas aplicações*

GoHacking

CYBER SECURITY TRAININGS