Desenvolvimento Web Seguro

Plano de Ensino

Prof. Dr. Jefferson O. Andrade

2024/1

1 Descrição do Curso:

O curso de Desenvolvimento Web Seguro visa fornecer aos alunos uma compreensão abrangente das práticas e técnicas necessárias para desenvolver aplicativos web seguros. Os alunos aprenderão sobre as ameaças mais comuns enfrentadas pelos aplicativos web, bem como as melhores práticas para mitigar essas ameaças. O curso incluirá uma combinação de pré-leituras, atividades práticas e discussões em tempo real durante as aulas síncronas.

2 Objetivos:

- Compreender os princípios fundamentais da segurança de aplicativos web.
- Identificar e mitigar vulnerabilidades comuns em aplicativos web, como XSS, CSRF e injeção de SQL.
- Implementar práticas de autenticação e autorização seguras.
- Configurar e manter comunicações seguras entre clientes e servidores.
- Desenvolver e implementar uma mentalidade defensiva ao escrever código para aplicativos web.

3 Estrutura do Curso:

3.1 Semana 1: Introdução à Segurança de Desenvolvimento Web

- Pré-aula: Leitura de material sobre segurança de aplicativos web
- Aula Síncrona: Discussão sobre as ameaças e vulnerabilidades mais comuns

3.2 Semana 2: Autenticação e Autorização

- Pré-aula: Assista a vídeos sobre métodos de autenticação e autorização
- Aula Síncrona: Resolução de problemas e estudos de caso sobre autenticação e autorização

3.3 Semana 3: Cross-Site Scripting (XSS) e Cross-Site Request Forgery (CSRF)

- Pré-aula: Estudo de casos de XSS e CSRF
- Aula Síncrona: Discussão e prática de prevenção de XSS e CSRF

3.4 Semana 4: Injeção de SQL e Gerenciamento de Sessão Segura

- Pré-aula: Exercícios de injeção de SQL e práticas de gerenciamento de sessão
- Aula Síncrona: Revisão dos exercícios e discussão de boas práticas

3.5 Semana 5: Comunicação Segura (SSL/TLS)

- Pré-aula: Material sobre SSL/TLS e HTTPS
- Aula Síncrona: Demonstração de configuração de SSL/TLS e discussão de melhores práticas

3.6 Semana 6: Headers de Segurança e Política de Segurança de Conteúdo (CSP)

- Pré-aula: Leitura sobre headers de segurança e CSP
- Aula Síncrona: Implementação e configuração prática de CSP

3.7 Semana 7: Upload e Download de Arquivos Seguros

- Pré-aula: Tutoriais sobre segurança de upload e download de arquivos
- Aula Síncrona: Discussão e prática de técnicas de segurança

3.8 Semana 8: Práticas de Codificação Segura

- Pré-aula: Revisão de código e identificação de vulnerabilidades
- Aula Síncrona: Revisão dos conceitos e feedback sobre projetos individuais

4 Avaliação:

- Participação nas discussões e atividades síncronas: 30%
- Tarefas práticas e projetos individuais: 50%
- Exame final online: 20%

5 Bibliografia:

Bibliografia Básica

LI, Vickie. **Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilities**. San Francisco, CA: No Starch Press, 7 dez. 2021. 416 p. ISBN 978-1-71850-154-6.

SEITZ, Justin; ARNOLD, Tim; MILLER, Charles Alfred. **Black Hat Python: Python Programming for Hackers and Pentesters**. 2nd edition. San Francisco, CA: No Starch Press, 2021. 190 p. ISBN 978-1-71850-112-6.

STUTTARD, Dafydd; PINTO, Marcus. **The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws**. 2nd. ed. Indianapolis, Ind: Wiley, 2011. 878 p. ISBN 978-1-118-02647-2.

Bibliografia Complementar

BALL, Corey. **Hacking APIs: Breaking Web Application Programming Interfaces**. San Francisco: No Starch Press, 2022. 1 p. ISBN 978-1-71850-245-1.

HOFFMAN, Andrew. **Web Application Security: Exploitation and Countermeasures for Modern Web Applications**. First edition. Beijing Boston Farnham Sebastopol Tokyo: O'Reilly, 2020. 298 p. ISBN 978-1-4920-5311-8.

HOPE, Paco; WALTHER, Ben. **Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast**. Sebastopol, CA: O'Reilly Media, 14 out. 2008. 314 p.

OWASP FOUNDATION. **OWASP Top Ten | OWASP Foundation**. en. OWASP Foundation. 2021. Disponível em: <https://owasp.org/www-project-top-ten/>. Acesso em: 5 mai. 2024.

YAWORSKI, Peter. **Real-World Bug Hunting: A Field Guide to Web Hacking**. San Francisco: No Starch Press, 2019. 235 p. ISBN 978-1-59327-861-8.

6 Observação:

Este plano de ensino está sujeito a ajustes conforme necessário para atender às necessidades dos alunos e garantir uma experiência de aprendizado eficaz em um ambiente de sala de aula invertida.