Plano de Ensino

Curso	Semestre/Ano
Tecnologia em Desenvolvimento de Software Multiplataforma	1o Semestre/2024
Disciplina	**Sigla**
Segurança no Desenvolvimento de Aplicações	ISG022

Carga Horária Semanal	Carga Teórica	Carga Prática	Carga Horária Semestral
4	0	4	80

Professor

MARCO ANTONIO TOMÉ

Ementa

Conceitos fundamentais do pilar de segurança: confidencialidade, integridade, disponibilidade e autenticidade. Gestão de Vulnerabilidades e resposta à incidentes de segurança. Redução da superfície de ataque, defesa em profundidade, menor privilégio, padrões seguros, modelagem de ameaças, ferramenta para diagramação e enumeração de ameaças, testes de segurança, Fuzz testing, Teste de invasão, Injeção de SQL, Cross-Site Scripting (XSS), aplicação de conceitos de OWASP (Open Web Application Security Project) e SDL (Security Development Lifecycle), Revisão de código.

Objetivo

Compreender o pilar de Segurança da Informação e empregar técnicas de programação segura para o desenvolvimento de aplicações Web, na proteção os dados de entrada dos usuários. Conhecer e utilizar conceitos de SQL Injection, para testar as vulnerabilidades das aplicações. Aplicar técnicas de validação ou codificação, para assegurar as mensagens enviadas ao navegar. Realizar armazenamento seguro das informações, com a utilização de autenticidade e criptografia

Metodologia

Aula expositiva presencial, com aplicação de atividades

Critérios de Avaliação

Fórmula : iif((((P1*0.3499) > (P2*0.3501)) and ((P3*0.3499) < (P2*0.3501))) or (((P1*0.3499) < (P2*0.3501)) and ((P3*0.3501) < (P1*0.3499))) , (P1*0.35 + P2*0.35 + T*0.3) , iif((P3*0.3499+ P2*0.3501) > (P1*0.3499+ P3*0.3501) ,(P3*0.35 + P2*0.35 + T*0.3) ,(P1*0.35 + P3*0.35 + T*0.3)))

Legendas :

- Prova P1 - - Avaliação Oficial P1
- Prova P2 - - Avaliação Oficial P2
- Prova P3 - - Avaliação de Recuperação P3
- Atividades - - Atividades: Exercícios, Trabalhos e/ou Projetos

Plano de Aula

1 T01 - Apresentações, Planejamento e Introdução ao Tema -> Aula inaugural. Apresentações: professor e alunos. Planejamento: plano de ensino e grupos de trabalho. Introdução à Segurança da Informação (SI): histórico, importância, conceitos e princípios básicos.

2 T02 - Conformidade e os Aspectos Legais da SI -> Conformidade legal e regulatória em segurança da informação. Compliance e responsabilidades legais. GDPR, LGPD, DPO e ABNT/ISO 27000.

3 T03 - Controles de Acesso e Autorização -> Políticas de segurança. Modelos e mecanismos de controle de acesso e autorização. Role-Based Access Control (RBAC); Access Control Lists (ACLs).

4 T04 - Autenticação e Gestão de Sessões -> Métodos e técnicas seguras de autenticação e gestão de sessões. Armazenamento seguro de senhas. OAuth e OpenID Connect. Sessões, cookies e tokens de segurança.

5 T05 - Testes de Segurança em Aplicações -> Fundamentos dos testes de segurança. Penetration testing; ferramentas de teste de segurança; testes automatizados. Testes de penetração, ferramentas de teste de segurança, bug bounty. Gerenciar e mitigar vulnerabilidades em aplicações. Tópicos: Descoberta de vulnerabilidades, gestão de patches, atualizações de segurança. Explorar as 10 principais vulnerabilidades de segurança segundo a OWASP.Top 10.

6 T06 - Prevenção de XSS e SQL Injection -> Conceitos básicos de SQL Injection. Técnicas para prevenir ataques de SQL Injection. Validação de entrada de dados. Uso de Prepared Statements, ORM. Técnicas para prevenir ataques XSS. Tipos de XSS (refletido, armazenado, DOM-based). Técnicas de prevenção e codificação de saídas.

7 T07 - Logs e Monitoração de Aplicações -> Importância dos logs e do monitoramento para a segurança. Geração de

Responsavel pela Disciplina	Coordenador pelo Curso
MARCO ANTONIO TOMÉ	JOÃO CARLOS DE SOUZA
/ /	/ /

Plano de Ensino

logs segura. Monitoramento de aplicações. SIEM.
8 P1 - Semana de Avaliação Oficial -> Aplicação da Prova P1. Avaliação do conteúdo ministrado.
9 P1 - Divulgação da Nota P1 e Revisão de Conteúdo -> Divulgação e ajustes da nota P1. Revisão do conteúdo ministrado. Revisão de atividades desenvolvidas.
10 T08 - Validação e Sanitização de Dados -> Importância da validação e codificação de dados. Diferenças entre validação e sanitização; bibliotecas e ferramentas. Técnicas de validação de dados de entrada e saída. Codificação para prevenção de XSS, whitelist vs. blacklist.
11 T09 - Fundamentos de Criptografia -> Princípios básicos da criptografia e seu papel na segurança da informação. Criptografia simétrica e assimétrica. Hashes. Certificados digitais. Importância do TLS/SSL.
12 T10 - Criptografia em Aplicações e Dados -> Criptografia para proteger dados. Criptografia de dados em trânsito e em repouso. Melhores práticas para armazenamento de senhas e dados sensíveis. Conceitos de criptografia no desenvolvimento seguro. Criptografia em aplicações, melhores práticas e ferramentas.
13 T11 - Introdução à Programação Segura -> A importância da programação segura e boas práticas. Princípios básicos da programação segura. Princípios de menor privilégio. Ciclo de vida do desenvolvimento de software. Revisão de código, e boas práticas de programação.
14 T12 - Segurança em Aplicações Web -> Fundamentos da Web e segurança. Como a web funciona e os pontos críticos para a segurança. Protocolos da web, arquitetura cliente-servidor, e introdução à segurança web. As vulnerabilidades comuns em aplicações web e como protegê-las. Cross-Site Request Forgery (CSRF). Injeção de comandos. Segurança em APIs.
15 T13 - Desenvolvimento de Aplicações Web Seguras -> Desenvolvimento de aplicação web com foco em segurança. Revisão de código entre pares. Planejamento e implementação de projeto prático. Aplicação de técnicas de programação segura.
16 T14 - Revisão do Principais Tópicos do Curso -> Revisão dos conceitos-chave. Revisão dos principais tópicos do curso. Aplicação web segura, documentação. Medidas de segurança implementadas.
17 P2 - Semana de Avaliação Oficial -> Aplicação da Prova P2. Avaliação do conteúdo ministrado.
18 P2 - Divulgação da Nota P2 e Revisão de Conteúdo -> Divulgação e ajustes da nota P2. Revisão do conteúdo ministrado. Avaliação de atividades desenvolvidas.
19 P3 - Recuperação e Avaliação de Atividades -> Aplicação de Prova P3. Avaliação do conteúdo ministrado. Avaliação de atividades desenvolvidas.
20 Fechamento do Semestre Letivo -> Lançamentos finais no sistema SIGA. Fechamento do sistema SIGA. Emissão dos relatórios administrativos.

Bibliografia Basica

MORENO D. Pentest em aplicações web. São Paulo: Novatec, 2017.
MUELLER J. P. Segurança para desenvolvedores web. São Paulo: Novatec ,2016.
SEITZ J. Black Hat Python: Programação Python Para Hackers e Pentesters. São Paulo: Novatec, 2015.

Bibliografia Complementar

ABNT. Tecnologia da informação - Código de prática para a gestão da segurança da informação (NBR ISO/IEC 17799). Rio de Janeiro, RJ: 2001.
FERREIRA, Rodrigo. Segurança em aplicações Web. São Paulo: Casa do Código, 2017.
WEIDMAN G. Testes de Invasão: Uma introdução prática ao hacking. São Paulo: Novatec, 2014.

Bibliografia Referencia

Responsavel pela Disciplina	Coordenador pelo Curso
MARCO ANTONIO TOMÉ	JOÃO CARLOS DE SOUZA
/ /	/ /