



Serviço Público Federal
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense
Pró-Reitoria de Ensino

DISCIPLINA: Desenvolvimento de Código Seguro	
Vigência: 2021/1	Período letivo: Eletiva
Carga horária total: 30 h	Código: SUP.2278
CH Extensão: 0 h	CH Pesquisa: 0 h
% EaD: 0 %	
Ementa: Introdução ao desenvolvimento de código seguro; estudo das questões de segurança no contexto de front-end e back-end; estudo de aspectos de segurança em sistemas de banco de dados; estudo das vulnerabilidades envolvidas na comunicação entre sistemas; estudo das melhores práticas para desenvolvimento de sistemas seguros.	

Conteúdos:

UNIDADE I – INTRODUÇÃO AO DESENVOLVIMENTO DE CÓDIGO SEGURO

- 1.1 Visão geral do desenvolvimento de sistemas seguros
- 1.2 A segurança nos diferentes domínios do desenvolvimento
- 1.3 Dimensões da segurança aplicadas ao desenvolvimento

UNIDADE II – FRONT-END E BACK-END

- 2.1 Script injection
- 2.2 Tratamento de entrada de dados
- 2.3 Validação de entrada de dados em front- VS back-end
- 2.4 Buffer overflow
- 2.5 Command injection
- 2.6 Tratamento adequado de erros e exceções
- 2.7 Revisando avisos do compilador ou interpretador
- 2.8 Números pseudo aleatórios inseguros
- 2.9 Wraparound
- 2.10 Restrições para caminhos de diretórios
- 2.11 Upload de arquivos maliciosos
- 2.12 Uso de credenciais hard-coded
- 2.13 Uso descontrolado de recursos
- 2.14 Controle de sessão

UNIDADE III – BANCO DE DADOS

- 3.1 SQL injection
- 3.2 Gerenciamento de acesso ao banco de dados
- 3.3 Níveis de acesso e privilégios
- 3.4 Acesso direto VS indireto
- 3.5 Isolamento de informações críticas

UNIDADE IV – COMUNICAÇÃO

- 4.1 Comunicação segura entre sistemas
- 4.2 Cross-site scripting



Serviço Público Federal
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense
Pró-Reitoria de Ensino

4.3 Cross-Site Request Forgery

UNIDADE V – MELHORES PRÁTICAS

- 5.1 Código aberto VS caixa preta
- 5.2 Utilização de padrões
- 5.3 Teste de software
- 5.4 Revisando logs
- 5.5 Lista negra VS lista branca
- 5.6 Isolando componentes críticos
- 5.7 Definindo limites superiores e inferiores
- 5.8 Gerenciamento de segurança em componentes de terceiros

Bibliografia básica

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores – Princípios e Práticas**. Rio de Janeiro: Elsevier, 2014.
GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. São Paulo: Bookman, 2013.
STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. 4. ed. São Paulo, SP: Pearson, 2008.

Bibliografia complementar

BAARS, Hans. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018.
MITNICK, Kevin D.; SIMON, William L. **A arte de Invadir**. São Paulo: Person Prentice Hall, 2005.
DHANJANI, Nitesh; RIOS, Billy; HARDIN, Brett (Aut.). **Hacking: a próxima geração**. Rio de Janeiro, RJ: Alta Books, 2011. xiii, 273 p. ISBN 9788576085331.
IMONIANA, Joshua Onome. **Auditoria de sistemas de informação**. São Paulo: Atlas, 2016.
FONTES, Edison. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2008.
SÊMOLA, Marcos. **Gestão da segurança da informação**. Rio de Janeiro: Elsevier Brasil, 2014.