Lição 1

Introdução a Segurança

Objetivos

Ao final desta lição, o estudante será capaz de:

- Conhecer sobre os principais aspectos de segurança
- Aprender boas práticas de segurança
- Observar as práticas de segurança aplicadas à linguagem Java

Introdução a Segurança

- Proteção de sistemas de informação contra o acesso não-autorizado a informação ou sua modificação, seja por meio de armazenamento, processamento ou tráfego, e contra a negação de serviços aos usuários autorizados ou o fornecimento destes para usuários não autorizados, incluindo medidas necessárias para detectar, documentar e bloquear tais ameaças

Principais Aspectos de Segurança

- Confidencialidade
- Integridade de Dados
- Disponibilidade
- Controle de Acesso
- Não-repúdio

Confidencialidade

- Restringe as informações às pessoas que tenham acesso
- Informação não deve ser fornecida ou difundida
- Violação de sigilo quando os dados são acessados
- Assegura que as informações estejam seguras

Integridade

- Modificações não são feitas por pessoal não autorizado aos dados ou processos
- Alterações só podem ser realizadas por pessoal autorizado aos dados ou processos
- Os dados são internamente e externamente consistentes
- Não é lidar com a exatidão dos dados
- Deve ser de confiança

Falsificação de Integridade

- Uma espécie de falsificação é chamada *phising*
- É freqüentemente realizado com um endereço falso
- As vítimas são encaminhadas para outro endereço
- Integridade é ter confiança de que a informação não foi alterada

Disponibilidade

- A informação é exibida e pronta para ser utilizada assim que seja necessária
- *Code Red* explora a vulnerabilidade de um determinado servidor WEB
- É a garantia de que os sistemas sejam responsáveis pela entrega, armazenamento e processamento

Boas práticas de Segurança – Identificação e Autenticação

- Baseada em:
  - O usuário sabe
  - O usuário possui
  - O usuário é
- Implementada para serviços pessoais de aplicações WEB

Boas práticas de Segurança – Autorização

- Três tipos básicos de acesso:
  - Leitura
  - Escrita
  - Execução
- Permissões e direitos são implementadas de maneira diferente

Boas práticas de Segurança – Controle de Acesso

- Proteção contra uso não autorizado de recursos:
  - Uso de recurso de comunicação
  - Leitura, escrita ou deleção em um recurso de informação
  - Execução de um recurso de processamento
- Manter uma Access Control List
- Técnicas de Controle de Acesso:
  - Controle de Acesso Discrecionária (CAD)
  - Controle de Acesso Mandatório (CAM)

Boas práticas de Segurança – Não Repudiação

- Não repudiação de origem protege contra o emissor que nega que a mensagem foi enviada. Prova que o dado foi enviado
- Não repudiação de entrega protege contra o receptor que nega que os dados foram recebidos. Prova que o dado foi recebido

Boas práticas de Segurança – Auditoria

- Os sistemas da organização estarão disponíveis para o negócio sempre que requeridos? (Disponibilidade)
- A informação presente nos sistemas será mostrada apenas para usuários autorizados? (Confidencialidade)
- A informação provida pelo sistema é sempre confiável, precisa, e entregue no prazo? (Integridade)

Práticas de Segurança e a Linguagem Java

	Confidencialidade	*Integridade*	*Disponibilidade*	*Identificação e Autenticação*	*Autorização*	*Não-Repudiação*	*Auditoria*	*Conteúdo*
JVM		**X**	**X**					**X**
Carregadores de Classe		**X**						**X**
Gerenciadores de Segurança		**X**			**X**		**X**	**X**
Domínios de Segurança					**X**			**X**
Criptografar, Encriptar, SSL	**X**							
Sumário de Mensagens				**X**		**X**		
Assinaturas e Certificados Digitais				**X**		**X**		
Lista de Controle de Acesso					**X**			
JAAS				**X**	**X**			

Sumário

- Introdução a segurança
- Principais aspectos de segurança
  - Confidencialidade
  - Integridade
  - Disponibilidade
- Boas práticas de segurança
- Práticas de Segurança e a linguagem Java

Parceiros

- **Os seguintes parceiros tornaram JEDI™ possível em Língua Portuguesa:**