

SEGURANÇA DE SOFTWARE

Moises Brandalise e Avelino Zorzo

“

A programação em par incentiva muito o processo de troca e de colaboração.

”

Guilherme Lacerda

Conheça o livro da disciplina

CONHEÇA SEUS PROFESSORES 3

Conheça os professores da disciplina.

EMENTA DA DISCIPLINA 4

Veja a descrição da ementa da disciplina.

BIBLIOGRAFIA DA DISCIPLINA 5

Veja as referências principais de leitura da disciplina.

O QUE COMPÕE O MAPA DA AULA? 6

Confira como funciona o mapa da aula.

MAPA DA AULA 7

Links de artigos científicos, informativos e vídeos sugeridos.

RESUMO DA DISCIPLINA 31

Relembre os principais conceitos da disciplina.

AVALIAÇÃO 32

Veja as informações sobre o teste da disciplina.

Conheça seus professores



MOISES BRANDALISE

Professor Convidado

Atua como Especialista em Segurança da Informação em uma instituição financeira. Na carreira, atuou no ramo da indústria por 10 anos no papel de líder técnico em infraestrutura de tecnologia e 3 anos como Analista de desenvolvimento de Sistemas em fábrica de software. Em segurança da informação, atuou na indústria da mídia por 6 anos como Analista e no segmento financeiro, por 4 anos como Especialista, além de 2 anos como Especialista em Proteção de dados pessoais, totalizando cerca de 25 anos de mercado.

AVELINO ZORZO

Professor PUCRS

Associado da Sociedade Brasileira de Computação (SBC) e da IEEE. Possui graduação em Ciência da Computação pela Universidade Federal do Rio Grande do Sul (1986-1989), mestrado em Ciência da Computação pela Universidade Federal do Rio Grande do Sul (1990-1994), doutorado em Ciência da Computação pela University of Newcastle Upon Tyne (1995-1999) e pós-doutorado na área de segurança no Cybercrime and Computer Security Centre da Newcastle University (2012-2013). Atualmente é professor titular da Escola Politécnica da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Coordenador de Programas Profissionais da área de Computação da CAPES/MEC, avaliador de condições de ensino do Ministério da Educação, consultor ad hoc do CNPq, CAPES e da FAPERGS.



Ementa da Disciplina

Estudo sobre os métodos e utilização de criptografia para transmissão e armazenamento. Estudo sobre protocolo de comunicação em navegadores (HTTPS) ou aplicativos de conversa (LibSignal). Estudo sobre segurança no desenvolvimento de software. Estudo sobre os problemas mais frequentes indicados pela OWASP. Estudo sobre métodos de autenticação e autorização.

Bibliografia da Disciplina

As publicações destacadas têm acesso gratuito.

Bibliografia básica

OWASP. Open Web Application Security Project® (OWASP).

HOFFMAN, A. Web Application Security: Exploitation and Countermeasures for Modern Web Applications. O'Reilly, 2020.

KUROSE, J.; ROSS, K. Redes de computadores e a internet: uma abordagem top-down. 8a. Ed. Person do Brasil, 2020.

Bibliografia complementar

SINGH, S. O Livro dos códigos. Editora Record, 2004.

ORIYANO, S. Penetration Testing Essentials. Indiana: Sybex, 2017.

STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas. 6a. Ed. São Paulo: Pearson Education do Brasil, 2015.

FERGUSON, N., SCHNEIER, B., KOHNO, T. Engineering Design Principles, and Practical Applications. John Wiley & Sons, 2016.

STINSON, D. Cryptography: Theory and practice. 4a. Ed. CRC Press, 2018.

O que compõe o Mapa da Aula?

MAPA DA AULA

São os capítulos da aula, demarcam momentos importantes da disciplina, servindo como o norte para o seu aprendizado.



EXERCÍCIOS DE FIXAÇÃO

Questões objetivas que buscam reforçar pontos centrais da disciplina, aproximando você do conteúdo de forma prática e exercitando a reflexão sobre os temas discutidos. Na versão online, você pode clicar nas alternativas.



PALAVRAS-CHAVE

Conceituação de termos técnicos, expressões, siglas e palavras específicas do campo da disciplina citados durante a videoaula.



VÍDEOS

Assista novamente aos conteúdos expostos pelos professores em vídeo. Aqui você também poderá encontrar vídeos mencionados em sala de aula.



PERSONALIDADES

Apresentação de figuras públicas e profissionais de referência mencionados pelo(a) professor(a).



LEITURAS INDICADAS

A jornada de aprendizagem não termina ao fim de uma disciplina. Ela segue até onde a sua curiosidade alcança. Aqui você encontra uma lista de indicações de leitura. São artigos e livros sobre temas abordados em aula.



FUNDAMENTOS

Conteúdos essenciais sem os quais você pode ter dificuldade em compreender a matéria. Especialmente importante para alunos de outras áreas, ou que precisam relembrar assuntos e conceitos. Se você estiver por dentro dos conceitos básicos dessa disciplina, pode tranquilamente pular os fundamentos.

CURIOSIDADES

Fatos e informações que dizem respeito a conteúdos da disciplina.



DESTAQUES

Frases dos professores que resumem sua visão sobre um assunto ou situação.



ENTRETENIMENTO

Inserções de conteúdos para tornar a sua experiência mais agradável e significar o conhecimento da aula.



CASE

Neste item, você relembra o case analisado em aula pelo professor.



MOMENTO DINÂMICA

Aqui você encontra a descrição detalhada da dinâmica realizada pelo professor.



Mapa da Aula

Os tempos marcam os principais momentos das videoaulas.

AULA 1 • PARTE 1

PALAVRAS-CHAVE

SQL injection: Técnica usada para explorar vulnerabilidades em sistemas que utilizam a linguagem SQL para se comunicar com um banco de dados, que consiste na inserção de códigos maliciosos em campos de entrada de formulários de uma aplicação web.

PALAVRAS-CHAVE

LGPD: A Lei Geral de Proteção de Dados entrou em vigor no Brasil em 2020. Ela estabelece regras para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, visando proteger a privacidade e a segurança das informações. Empresas que não cumprem as disposições da lei podem sofrer sanções e multas.

PALAVRAS-CHAVE

Kaspersky: É uma empresa russa de segurança da informação, fundada em 1997 por Eugene Kaspersky. Oferece soluções de segurança cibernética para indivíduos, empresas e governos, incluindo software antivírus, anti-malware, firewall e soluções para dispositivos móveis.

06:59



Segurança no desenvolvimento

Em um contexto de trabalho cada vez mais remoto e distribuído pela internet, há uma necessidade de desenvolvimento seguro de softwares. As legislações de proteção de dados e a exposição de dados dos usuários são as principais preocupações do mercado.

As vulnerabilidades surgem constantemente, sendo visível a necessidade de treinamentos para gestão de acessos e autorizações de usuários. Destaca-se a indústria como principal alvo de ataques, principalmente para a exploração em aplicativos e o phishing.

08:38



09:47



PALAVRA-CHAVE

11:12



IBM: IBM é uma empresa multinacional de tecnologia e consultoria com sede nos Estados Unidos. Oferece uma ampla gama de produtos e serviços de tecnologia, incluindo hardware, software, serviços em nuvem, inteligência artificial e consultoria em tecnologia da informação.

13:34



Principais ameaças

Entre os principais riscos de segurança enfrentados pelos desenvolvedores de software, podemos citar: ataques hackers, vazamento de dados, phishing e malware. Sendo que a exposição de dados pessoais é o risco mais comum atualmente.

O professor Moisés Bandalise traz alguns casos de instituições públicas e privadas que sofreram prejuízos devido a falhas na segurança de seus sistemas, gerando perda de reputação e confiança. E destaca a importância de se manter atualizado sobre as legislações de proteção de dados e notificar autoridades em caso de violações.

FUNDAMENTO

Métodos ágeis

O Manifesto Ágil, publicado em 2001, estabeleceu os valores fundamentais dos métodos ágeis: o foco nas pessoas, na entrega contínua, na colaboração e na resposta a mudanças.

Os métodos ágeis são caracterizados por processos iterativos e incrementais, com ciclos de feedback contínuos, que permitem que os projetos sejam ajustados conforme as necessidades e os requisitos mudam. Eles são usados principalmente no desenvolvimento de software, mas também são aplicados em outros projetos de gestão.

PALAVRAS-CHAVE

OWASP: Criado em 2001, a OWASP é uma comunidade global de voluntários dedicados à segurança de aplicativos da web. Ela fornece informações sobre as principais ameaças de segurança da web, ferramentas de segurança e melhores práticas para mitigar essas ameaças.

16:31



17:10



PALAVRA-CHAVE

RDP: O Remote Desktop Protocol é um protocolo de comunicação desenvolvido pela Microsoft que permite a conexão remota entre computadores. Ele permite que um usuário controle um computador remoto através da rede, visualizando e interagindo com o desktop do computador remoto como se estivesse fisicamente presente na frente dele.

23:26



24:59



25:08



PALAVRA-CHAVE

TAP: Empresa aérea portuguesa, fundada em 1945, que opera voos regulares para mais de 90 destinos em todo o mundo, incluindo Europa, África, América do Norte e do Sul e Ásia. A TAP é a maior companhia aérea de Portugal e membro da Star Alliance, uma aliança global de companhias aéreas.

31:37



“

Essa responsabilidade de fazer com que o software seja seguro é de todos vocês.

”

Principais organizações: parte I

A padronização de normas e práticas é muito importante no desenvolvimento de softwares e na segurança da informação. As principais organizações envolvidas são a ISO, que regulamenta processos e apresenta boas práticas, e a USP, que traz um catálogo das principais vulnerabilidades.

Além disso, a colaboração entre as empresas de um mesmo segmento de mercado no compartilhamento de informações e ataques, é outro fator que contribui para a segurança. A padronização é uma forma de permitir a interação entre empresas e equipamentos.



32:43

EXERCÍCIO DE FIXAÇÃO

Qual é o objetivo da ISO 27001?

34:55



PALAVRA-CHAVE

ISO: Uma organização internacional independente que desenvolve e publica normas técnicas para vários setores. As normas ISO cobrem uma ampla variedade de tópicos, incluindo qualidade, meio ambiente, segurança de informações e saúde ocupacional.

34:55



PALAVRA-CHAVE

ABNT: A Associação Brasileira de Normas Técnicas é o órgão responsável por fazer a adaptação e normatização das normas ISO para o mercado brasileiro.

AULA 1 • PARTE 2

Principais organizações: parte II

Outras organizações envolvidas são:

Consórcio W3C: responsável pela padronização de diversos elementos da comunicação e do desenvolvimento de software. Também criou padrões importantes como o HTML e o protocolo TLS, e mantém a padronização para que os protocolos funcionem em conjunto com os padrões web;

ICANN: responsável pela denominação de nomes de domínio e pela tradução do DNS;

OWASP: famosa por disponibilizar a lista das 10 principais vulnerabilidades no desenvolvimento de software e por trabalhar com pesquisa e desenvolvimento de ferramentas;

NIST: agência do governo americano que promove padrões para desenvolvimento seguro;

ETF: responsável por muitos padrões de criptografia e protocolos, padrões TCP IP;

PCI SSC: padronizar a transação de cartão e a forma com os dados são armazenados.

00:00



07:10



Quando a gente vai falar de risco, há uma necessidade de tentar entender como é que aquilo acontece.

13:07



Criptografia

Criptografia e seus métodos têm grande importância para garantir a privacidade das informações. Ela é utilizada tanto para armazenamento quanto para transmissão de dados, envolvendo algoritmos matemáticos complexos para transformar informações legíveis em informações cifradas.

A segurança dos dados está relacionada com a integridade, confidencialidade e autenticidade das informações, e a criptografia é essencial para garantir esses aspectos, podendo essa ser: simétrica, quando usa uma mesma chave para criptografar e descriptografar uma mensagem, ou assimétrica, quando usa um par de chaves pública e privada.

EXERCÍCIO DE FIXAÇÃO

O que é criptografia simétrica?



16:49



Quando a gente fala em criptografia, a gente fala em transformar.



19:02



PALAVRA-CHAVE

Cifra de César: Método simples de criptografia de substituição, que envolve a substituição de cada letra do alfabeto por outra letra que esteja três posições adiante no alfabeto. O método é considerado inseguro atualmente, pois é muito fácil de ser decifrado, no entanto, o método é ainda utilizado em jogos ou como introdução à criptografia em programas educacionais.

“Não tentem inventar uma criptografia, utilizem os algoritmos que já temos à disposição, em suas últimas versões.”



21:42

25:46



Tipos de Criptografia

Existem as criptografias simétrica, assimétrica e hash. A criptografia simétrica é uma técnica mais rápida do que a criptografia assimétrica, mas a segurança depende do compartilhamento seguro da chave. Lembrando que é muito importante pensar na segurança dos dados e na proteção da privacidade das pessoas ao desenvolver sistemas e softwares.

EXERCÍCIO DE FIXAÇÃO

Qual das alternativas é uma característica da criptografia simétrica?



A criptografia assimétrica, também conhecida como chave pública, envolve o desenvolvimento de duas chaves: uma pública e outra privada. Enquanto a chave pública pode ser distribuída e vista por todos, a chave privada deve ser mantida em segredo. A segurança da criptografia assimétrica está diretamente relacionada à capacidade de armazenar as chaves de forma segura.

33:14



“ Às vezes a solução é mais simples do que parece.”

AULA 1 • PARTE 3

Criptografia na comunicação

No uso de criptografia em transações online é de extrema importância garantir a segurança da comunicação de dados. Para isso são utilizadas chaves simétricas e assimétricas, criptografia de dados em trânsito e em repouso, além da comunicação cifrada entre aplicação e servidor, geralmente por meio dos protocolos HTTPS e TLS. É importante desenvolver uma arquitetura segura para evitar interceptações de dados e proteger as comunicações eletrônicas por meio de certificados digitais, que validam a autenticidade e integridade dos documentos.



00:00



EXERCÍCIO DE FIXAÇÃO

Qual é a diferença entre assinatura eletrônica e assinatura digital?

PALAVRAS-CHAVE

AES: Algoritmo de criptografia de blocos utilizado para proteger dados sensíveis em sistemas de computador e dispositivos móveis. Considerado um dos mais seguros e eficientes algoritmos de criptografia disponíveis atualmente, utilizando uma chave de criptografia simétrica para criptografar e descriptografar dados.



10:11

PALAVRA-CHAVE



10:23

Sha256: É uma função criptográfica utilizada em sistemas de segurança da informação para verificar a integridade dos dados e garantir que eles não tenham sido modificados ou corrompidos durante a transmissão ou armazenamento.

Armazenando e transmitindo dados

A utilização da criptografia para proteger dados é importante tanto em repouso quanto em movimento. A implementação correta dos algoritmos de criptografia inclui a gestão adequada das chaves e questões relacionadas à auditoria e testes. Temos, como exemplos de aplicação da criptografia, o BitLocker da Microsoft para dados em repouso e protocolos de comunicação, como SSL, HTTPs e VPN, para proteger dados em movimento. O objetivo é garantir a privacidade e segurança dos dados, prevenir fraudes e minimizar danos à imagem corporativa ou dos clientes.



13:16



16:09

PALAVRA-CHAVE

BitLocker: É um recurso de criptografia de disco completo integrado no sistema operacional Windows, que ajuda a proteger dados armazenados em discos rígidos internos e externos, bem como em dispositivos removíveis. Ele usa criptografia de chave simétrica e requer uma senha ou chave de recuperação para acessar os dados criptografados.



18:19

Gerenciamento de chaves criptográficas

O gerenciamento de chaves é muito importante para a segurança de dados corporativos e de negócios. Chaves criptográficas são tão fortes quanto a capacidade de protegê-las, gerenciar um grande número de chaves pode ser facilitado por um cofre de senha, onde as aplicações são desenvolvidas considerando a existência desse cofre. A gestão do ciclo de vida das chaves é essencial, assim como a prevenção de ataques, que pode ser alcançada por meio de criptografia e o uso de Salt, uma sequência aleatória adicionada a uma senha para torná-la mais segura.



18:31

“A criptografia é tão forte quanto a capacidade de proteger as suas chaves.**”**

PALAVRAS-CHAVE



22:50

SALT: Técnica de criptografia usada para proteger senhas em bancos de dados, que adiciona um valor único e secreto, conhecido como “salt”, a cada senha antes de criptografá-la e armazená-la.



28:18

“Se alguém do outro lado tem interesse em descobrir a sua senha e ela tiver 10 dígitos, a pessoa vai dar um jeito de descobrir.**”**

Algoritmos seguros



31:37

Moisés explica como as chaves de criptografia são usadas para proteger os dados armazenados, transferidos e autenticados. E enfatiza a importância da troca segura de chaves e da resistência a colisões para garantir a segurança dos dados.

O algoritmo AES é muito rápido e utilizado na maioria das organizações para criptografar dados armazenados. O algoritmo RSA é um sistema criptográfico de chave pública que usa um par de chaves, uma pública e outra privada, para realizar a criptografia e a descriptografia. O algoritmo SHA-256 é resistente a colisões e é utilizado para gerar impressões digitais de mensagens, tornando praticamente impossível reverter esse processo.

AULA 1 • PARTE 4

01:00



Modelo referencial OSI

Surgindo entre as décadas de 70/80, o modelo de referência OSI é uma estrutura organizada em sete camadas independentes, mas que trabalham entre si, que permite que diferentes dispositivos se conectem e se comuniquem. As camadas sete camadas são aplicação, apresentação, sessão, transporte, rede, enlace e físico, sendo a camada de apresentação e aplicação as que mais se relacionam com o desenvolvimento, e cada camada tem uma função específica.

04:54



“ O bit é o nível mais baixo da comunicação. **”**

EXERCÍCIO DE FIXAÇÃO

Qual é o objetivo principal da camada física do modelo OSI?



Os protocolos são conjuntos de regras que permitem a troca de informações entre os dispositivos, seguindo padrões definidos por instituições. A estrutura de camadas permite que diferentes equipamentos se comuniquem e a padronização garante que essa comunicação seja automatizada e padronizada.

06:12



A informação não trafega sempre pelo mesmo caminho.



12:30



Principais protocolos: parte I

Os protocolos de comunicação segura permitem que os dispositivos troquem informações de forma estruturada e organizada. O TCP é um protocolo que abstrai algumas camadas e simplifica o modelo de entendimento, permitindo que os dados sejam transmitidos de forma confiável e em ordem. Já o protocolo UDP é mais rápido, mas não oferece garantia de entrega e é usado em aplicações que não requerem confiabilidade de entrega. O protocolo HTTP é um exemplo de protocolo utilizado em servidores web para garantir a comunicação segura entre cliente e servidor.

19:18



PALAVRAS-CHAVE

Porta 443: É uma porta de rede usada para comunicação segura com servidores web. É a porta padrão usada para o protocolo HTTPS (HTTP Seguro), que é uma versão segura do protocolo HTTP utilizado para o acesso a sites na Internet. O uso da porta 443 permite que os dados sejam criptografados durante a transferência.

21:59



Principais protocolos: parte II

O protocolo FTP é um protocolo de transferência de arquivos utilizado, principalmente, em aplicações de pequeno porte que não requerem um repositório centralizado. Ele funciona com autenticação de usuário e senha, é recomendado usar o FTPS para garantir a criptografia do protocolo. O SFTP também é uma opção, que utiliza a porta 22 e uma comunicação estabelecida de forma segura. Ele é utilizado para transferência de e-mails e a autenticação é importante para garantir a entrega correta. É recomendado utilizar o SMTPS com a porta 465 ou 587 para comunicação com o servidor de meio. A troca de chaves, certificado digital assinado e criptografia são comuns em ambos os protocolos para garantir a segurança da comunicação.

23:44



PALAVRAS-CHAVE

Porta 22: É uma porta de rede usada para comunicação segura através do protocolo SSH (Secure Shell), que permite o acesso remoto a sistemas de computador de forma segura. É a porta padrão usada pelo SSH, mas pode ser alterada para outra porta para evitar ataques automatizados por varreduras de portas.

PALAVRA-CHAVE

26:01



PALAVRAS-CHAVE

AES-256: É uma variação do algoritmo de criptografia simétrica AES (Advanced Encryption Standard) que utiliza uma chave de 256 bits para proteger dados sensíveis. O AES é um algoritmo de criptografia amplamente utilizado e aprovado pelo governo dos EUA.

27:08



Porta 465 e 587: São duas portas de rede usadas para comunicação segura com servidores de e-mail usando o protocolo SMTP (Simple Mail Transfer Protocol) com criptografia SSL (Secure Sockets Layer) ou TLS (Transport Layer Security). O uso dessas portas permite que os clientes de e-mail enviem e-mails com segurança.

27:20



PALAVRAS-CHAVE

Libsignal: É uma biblioteca criptográfica de código aberto, desenvolvida pela Open Whisper Systems, que fornece criptografia de ponta a ponta para comunicações de mensagens instantâneas. Projeto para fornecer segurança robusta e fácil de usar para mensagens instantâneas, protegendo a privacidade dos usuários e suas comunicações online.

35:06



Principais protocolos: parte III

O protocolo DNS é responsável por converter nomes de domínios em endereços IP, permitindo que a comunicação na internet aconteça de forma mais fácil e organizada. Quando um usuário faz uma solicitação, o servidor DNS consulta outros servidores para encontrar o endereço IP correspondente ao nome de domínio solicitado. Existem vários servidores de DNS em todo o mundo, que trabalham em conjunto para garantir a continuidade da internet, mesmo que alguns servidores parem de funcionar. A padronização dos nomes de domínio é regulamentada pela ICANN e o processo de registro de um novo domínio é complexo.

AULA 2 • PARTE 1

Principais desafios de segurança

É muito importante identificar riscos e vulnerabilidades em aplicações para evitar possíveis ameaças e falhas de segurança. Uma análise de risco pode ser realizada por meio de testes e simulações hipotéticas baseadas em situações reais, com o objetivo de mapear ameaças e identificar ativos que precisam ser protegidos. Além disso, é essencial avaliar o impacto potencial dessas ameaças e classificar o risco de acordo com a probabilidade de ocorrer e sua importância para a empresa. Para mitigar esses riscos, é preciso implementar medidas para eliminá-los ou minimizá-los. Por fim, é importante fazer um monitoramento posterior para garantir que os controles implementados estejam funcionando corretamente e para evitar possíveis complicações.



01:43

05:57



12:09



14:51



“ O risco tem muito a ver com pesos e o que é mais ou menos importante para aquela empresa. ”

“ Dentro da análise a gente precisa garantir que os dados sejam protegidos. ”

DevSecOps

Uma das principais maneiras de integrar a segurança no processo de desenvolvimento é utilizar a metodologia DevSecOps. Essa metodologia consiste em ter um time dedicado a pensar em segurança desde o início do processo de desenvolvimento e integrá-la em todas as etapas do ciclo de desenvolvimento. Para isso, são utilizadas diretrizes de segurança, padrões de codificação seguro, políticas de segurança, testes de penetração, ferramentas de segurança de código, ferramentas de teste de segurança e ferramentas de automação. É recomendado fazer validações na entrada de dados, gerenciamento de sessão, sanitização de entrada, e outras práticas de segurança de software.

EXERCÍCIO DE FIXAÇÃO

Qual é o objetivo da metodologia DevSecOps no processo de desenvolvimento de software?



PALAVRA-CHAVE

19:57



PALAVRAS-CHAVE

Waspzap: É um software de código aberto, que oferece uma plataforma de comunicação segura e criptografada para smartphones Android. É um fork do aplicativo de mensagens instantâneas Signal, que usa criptografia de ponta a ponta para garantir a privacidade das comunicações dos usuários.

19:57



Snyk: É uma ferramenta de segurança que ajuda a proteger aplicativos e bibliotecas de terceiros contra vulnerabilidades conhecidas. Ele verifica as dependências do código-fonte e alerta os desenvolvedores sobre as vulnerabilidades e brechas de segurança que precisam ser corrigidas.

24:15



PALAVRAS-CHAVE

BugHunt: Primeira plataforma brasileira de Bug Bounty, programa de recompensa por identificação de falhas, fundada por especialistas em Segurança da Informação, movidos pelo propósito de democratizar o acesso à segurança da informação e com isso tornar a Internet um lugar mais seguro.

26:52



A análise de vulnerabilidades é uma técnica que se concentra em analisar a aplicação.

28:25



Ciclo de vida

A segurança da informação é importante em todas as etapas do ciclo de vida de um software, desde o planejamento até a manutenção. Para isso, é necessário identificar os ativos que se deseja proteger e avaliar as possíveis ameaças e vulnerabilidades, a fim de definir e implementar as medidas de segurança necessárias. É preciso também realizar testes de segurança para garantir que as medidas implementadas estejam funcionando corretamente. A modelagem de ameaças é outra ferramenta importante para identificar possíveis ataques à aplicação. O método Strike é usado para avaliar a efetividade das medidas de segurança e identificar as vulnerabilidades que precisam ser corrigidas.



41:31

AULA 2 • PARTE 2

Métodos e ferramentas: parte I

O docente apresenta as principais ferramentas utilizadas para garantir a proteção de dados e reduzir custos e prejuízos para as empresas, como a análise estática e dinâmica de código, testes de invasão e gerenciamento de configuração segura. A análise estática se aplica à verificação do código-fonte antes da execução do software, enquanto a análise dinâmica é utilizada durante a execução deste. O professor destaca a importância da criptografia e do gerenciamento de chaves na proteção de dados.



04:46



EXERCÍCIO DE FIXAÇÃO

Qual é a principal diferença entre uma solução estática e uma solução dinâmica?

“A consequência da correção é a proteção.**”**



12:25



12:40



FUNDAMENTO

Black box e white box

Black box e white box são termos muito utilizados no contexto de testes de software, especificamente na área de testes de segurança.

Black box (caixa-preta) refere-se a um método de teste de software em que o testador não tem conhecimento sobre a estrutura interna do sistema ou aplicação sendo testada. O objetivo desse tipo de teste é avaliar a funcionalidade e a usabilidade do software do ponto de vista do usuário final.

Já a White box (caixa-branca) refere-se a um método de teste de software em que o testador tem conhecimento sobre a estrutura interna do sistema ou aplicação sendo testada. Esse tipo de teste é mais apropriado para identificar problemas que possam estar relacionados à lógica interna do software.

Métodos e ferramentas: parte II

Os testes de invasão e avaliação de vulnerabilidades são muito importantes em sistemas operacionais e aplicativos. Para isso, é necessário definir o escopo do teste e selecionar as ferramentas adequadas para identificar falhas e melhorar a segurança. É importante documentar as falhas encontradas para acompanhá-las e verificar se estão sendo corrigidas. O gerenciamento de configuração segura vai garantir a configuração da infraestrutura e fazer a gestão de servidores de aplicação, banco de dados e firewall. As equipes de desenvolvimento e infraestrutura devem trabalhar juntas para garantir que as políticas de segurança sejam aplicadas de forma consistente em toda a infraestrutura.

Simulação

Moisés demonstra uma simulação de configuração e implantação segura de infraestrutura de rede, com a configuração de duas máquinas. Destaca-se que é possível automatizar diversas configurações em outras máquinas, utilizando módulos disponíveis para criação de passos a serem seguidos. Apresenta o uso de chave pública e privada de criptografia para garantir a segurança da comunicação entre as máquinas. A autenticação e autorização são importantes para garantir que apenas usuários autorizados tenham acesso a dados sensíveis, mas que esse assunto será abordado posteriormente.

33:01



PALAVRA-CHAVE

Role Based: No modelo de controle de acesso baseado em funções, as permissões de acesso são atribuídas com base nas funções ou cargos que as pessoas desempenham na organização. É um modelo flexível e escalável, pois as permissões são definidas uma vez e aplicadas a todos os usuários que ocupam a mesma função.

33:01



PALAVRA-CHAVE

Rule based: No modelo de controle de acesso baseado em regras, as permissões de acesso são determinadas com base em um conjunto de regras definidas pelo administrador do sistema. As regras podem ser baseadas em diversos critérios, como hora do dia, endereço IP, tipo de dispositivo, entre outros.

AULA 2 • PARTE 3

API Manager

A ideia de um servidor de identidade para autenticar usuários em diferentes aplicações, é que o usuário utilize uma senha única para acesso a todas as aplicações. O WSO2 é uma tecnologia open source que permite que o usuário seja autenticado em um único lugar, o que facilita o processo e aumenta a segurança. Assim, o servidor de identidade será o responsável por armazenar as credenciais dos usuários e não as aplicações em si. Outra opção, é um processo de autenticação em duas aplicações diferentes, onde o servidor de identidade é responsável por autenticar o usuário em ambas. Isso é possível graças ao uso de tokens que são armazenados em cookies no navegador do usuário e validados pelo servidor de identidade.

00:00

00:50



“ Sempre que vocês puderem utilizar uma solução, vocês estão facilitando a vida do usuário também. **”**

Criptografia gerenciamento de chaves



12:21

O armazenamento das chaves criptográficas é fundamental para garantir a segurança das senhas de aplicações e bancos de dados, e cofres de senhas são utilizados para esse fim. É recomendado o uso de soluções como o Vault, que permitem o armazenamento hierárquico de chaves e a autenticação de usuários e serviços para acessá-las.

Também se destaca o risco de vazamento de chaves em caso de falhas na segurança da aplicação. É importante, ainda, definir o que será monitorado para detectar incidentes de segurança, e destaca a necessidade de configuração adequada de dispositivos de rede e sistemas operacionais para garantir a segurança dos dados.

EXERCÍCIO DE FIXAÇÃO



Qual é o objetivo do gerenciamento de chaves criptográficas?

OWASP e TOP 10: parte I



20:54

A instituição Open Web Application Security Project (OWASP), é uma entidade sem fins lucrativos que visa melhorar a segurança do desenvolvimento de software. A instituição é famosa por manter uma lista atualizada periódica das principais vulnerabilidades de aplicações web, mantida por voluntários e a instituição aceita doações. O “Top 10” é baseado em situações reais e tem como objetivo ajudar as organizações a criar aplicativos mais seguros. As vulnerabilidades mais comuns incluem a injeção de SQL, quebra de autenticação e quebra de controle de acesso, alteradas de acordo com o mercado.



27:16

PALAVRA-CHAVE

Mitre: Organização sem fins lucrativos que se dedica a resolver problemas complexos de interesse público, incluindo segurança cibernética. Ela propôs uma metodologia chamada “MITRE ATT&CK” para modelar e prevenir ameaças de segurança da informação.

31:37



“ Sempre vai ter alguém motivado a explorar alguma falha por motivos financeiros ou outros motivos. ”

OWASP e TOP 10: parte II

As três primeiras vulnerabilidades são exploradas com mais detalhes e são a quebra do controle de acesso, falhas criptográficas e injeção de código. As outras sete aconselham-se que sejam verificadas através de um checklist de situações para garantir que o software esteja protegido. É recomendado implementar controle de acesso e autenticação forte para evitar a quebra do controle de acesso e gerenciamento de grupos para gestão do acesso. Para evitar falhas criptográficas, deve-se implementar a criptografia de forma adequada. Além disso, o monitoramento e prevenção de ataques de força bruta é muito importante.



31:34



EXERCÍCIO DE FIXAÇÃO

Qual é o principal método utilizado em ataques de injeção de SQL?

43:42



Sempre pensando com olho na segurança e no top 10.



AULA 2 • PARTE 4

Autenticação

O processo de autenticação é amplamente utilizado no nosso dia a dia para garantir que apenas usuários autorizados tenham acesso a recursos protegidos. Ela pode ser baseada em algo que o usuário sabe, como uma senha, algo que ele possui ou na biometria, como reconhecimento facial ou de impressão digital. É importante destacar que, às vezes, as senhas utilizadas por algumas instituições financeiras e serviços são muito simples, o que pode colocar em risco a segurança do usuário. Por isso, a autenticação multifatorial, que inclui mais de um fator de autenticação, é uma forma mais segura de autenticação. O armazenamento das senhas e a transmissão dos dados durante o processo de autenticação também devem ser seguros.



00:00

01:18



Se a senha for muito difícil, às vezes a pessoa deixa de utilizar a aplicação.



EXERCÍCIO DE FIXAÇÃO



Qual é o objetivo do controle de acesso?

Métodos de autenticação



10:49

A validação da identidade é importante para garantir a segurança da informação e envolve saber, possuir e ser, ou seja, algo que a pessoa saiba, possua ou seja, como reconhecimento biométrico. A combinação de mais de uma forma de autenticação, como senha, SMS e reconhecimento biométrico, aumenta a segurança. A autenticação adaptativa é onde são aplicadas diferentes regras e procedimentos de acordo com o tipo de transação, valor envolvido e localização. Protocolos de segurança, criptografia e outros controles são utilizados para garantir a segurança do usuário e evitar engenharia social. A combinação de vários fatores de autenticação é importante para aumentar a segurança e evitar fraudes.

18:04



“ O usuário geralmente é o ponto mais fraco. **”**

PALAVRAS-CHAVE



22:57

23:33



Implementação

Autenticação 3D: É um protocolo de autenticação de transações online utilizado para aumentar a segurança nas compras com cartões de crédito ou débito. A autenticação 3D reduz a possibilidade de fraudes e aumenta a segurança do processo de compra.

O professor apresenta alguns sistemas de gerenciamento de usuários, que são comumente utilizados para realizar a autenticação e autorização. O protocolo LDAP, padrão da indústria de gerenciamento de serviço de diretórios, é dividido em duas operações padrão: autenticação e busca, além de outras funcionalidades, como a exclusão de objetos.

As soluções de identidade podem auxiliar as empresas em questões como a criação de contas de usuários. Dois exemplos de protocolos comuns são: o Windows baseado em corporativa e o software livre OpenLDAP. A troca de senha entre esses protocolos é um exemplo de complicação que pode surgir com a utilização de mais de um controlador de domínio.

Gestão de identidades

É importante centralizar a gestão em um único sistema para garantir a segurança e facilitar a inclusão de novos fatores de autenticação. O WS2 Open, por exemplo, é um sistema aberto que permite a gestão de usuários e permissões de acesso. A base de usuários é salva no hotel data e que, a partir daí, é possível gerar tokens de autenticação para os usuários. Também, é importante definir funções e regras de acesso para os usuários de acordo com seus perfis e necessidades dentro do sistema. Sendo possível integrar diferentes sistemas de autenticação, mas com cuidado ao definir qual será o controlador de domínio principal.



31:08

41:50



A segurança é feita em camadas e sempre que possível implementem uma camada a mais.



AULA 3 • PARTE 1

Mundo digital

A sociedade está em constante mudança e evolução, mas a velocidade dessas mudanças aumentou significativamente nos últimos anos. O mundo atual é digital e desconhecido para a maioria da sociedade. A tecnologia está cada vez mais presente em nossas vidas, no entanto, muitas pessoas ainda não entendem como essas tecnologias funcionam. Essa evolução é importante para aqueles que moldam esse mundo digital, como desenvolvedores de software, criptógrafos e cientistas de inteligência artificial.



03:28

04:51



A velocidade das mudanças que estão acontecendo atualmente, é muito grande.



08:31



Esse mundo digital é um mundo mágico.



Segurança

É necessário entender os diferentes tipos de ataques e vulnerabilidades existentes e desenvolver sistemas robustos e seguros. Para isso, é preciso entender a teoria e a prática da segurança digital, incluindo o uso correto de primitivos de criptografia e protocolos de segurança, as implementações adequadas garantem a segurança dos sistemas utilizados. Assim como no mundo físico, o mundo digital está suscetível a ataques e a segurança digital é fundamental para evitar prejuízos e proteger as pessoas.



12:39

“ A gente aprendeu por diversos séculos a como se comportar neste mundo físico e como ter segurança. ”



14:05

FUNDAMENTO

Primitivas de criptografia



16:22

Primitivas de criptografia são algoritmos fundamentais usados na construção de sistemas de criptografia. Elas fornecem a base para garantir a confidencialidade, integridade e autenticidade dos dados em um sistema criptográfico.



20:21

As principais primitivas de criptografia incluem: funções de hash, cifras simétricas e assimétricas, protocolos de autenticação de chave pública, assinaturas digitais, dentre outros. Elas são usadas para proteger a informação em diversos cenários, incluindo comunicação online, armazenamento de dados, transações financeiras, dentre outros.

“ Não saiam por aí implementando, fazendo um desenvolvimento de software, sem antes verificar se o que vocês estão fazendo não está gerando algum problema de segurança. ”



22:11



22:22

“ Na prática eu tenho segurança, se for bem-feito. ”



26:03

PALAVRAS-CHAVE

DES: Data Encryption Standard é um algoritmo de criptografia simétrica usado para proteger a confidencialidade dos dados. Ele opera em blocos de 64 bits de dados e usa uma chave de criptografia de 56 bits, e funciona por meio de uma série de substituições e permutações que transformam os dados de entrada em texto cifrado.

Teoria e Prática

O docente usa exemplos de números grandes para mostrar a magnitude do tempo necessário para quebrar uma chave de criptografia de 256 bits, o que demonstra que, na prática, é muito difícil violar a segurança. E discute dois problemas na área de segurança da informação, o primeiro é a engenharia social, em que muitas pessoas caem em ataques simples por falta de conhecimento sobre como viver no mundo digital, o segundo é a vulnerabilidade das informações pessoais que podem ser exploradas por criminosos. É importante fazer escolhas seguras ao utilizar algoritmos, bibliotecas e primitivas, para garantir a segurança na prática.

EXERCÍCIO DE FIXAÇÃO

Qual é um dos principais problemas na segurança da informação?

“ A gente tá aprendendo por tentativa e erro. ”

28:53

Heartbleed

O ataque chamado Heartbleed explorou um problema no protocolo do HTTPS que tinha como objetivo melhorar a performance e não a segurança. O ataque permitia que um cliente malicioso acessasse informações confidenciais armazenadas em um servidor, como senhas e dados de outros usuários. O problema poderia ter sido evitado se o desenvolvedor tivesse implementado verificações simples, como checar o tamanho da mensagem enviada pelo cliente. Portanto, deve-se levar em conta diferentes metas de segurança ao desenvolver um software, como privacidade, autenticidade, integridade e não-repúdio.



32:27

EXERCÍCIO DE FIXAÇÃO

Qual foi o problema explorado pelo ataque Heartbleed no protocolo HTTPS?

“ O cliente, tu tem que partir do pressuposto que ele pode ser malicioso. ”

36:16

“ Vocês são responsáveis por fazer modificações nesse mundo digital. ”

41:10

42:29

“ Pensar em desenvolvimento fullstack sem pensar em segurança é um problema muito grave. ”

AULA 3 • PARTE 2

Como funciona?

A criptografia pode ser usada para garantir a segurança na comunicação entre um remetente e um receptor, seja entre duas pessoas diferentes ou entre a mesma pessoa, que está armazenando informações. Todas as informações são vistas como números dentro do computador e os algoritmos de cifragem e decifragem transformam as mensagens em texto cifrado e texto claros, respectivamente. O texto cifrado deve parecer um texto aleatório para garantir sua segurança e quebrá-lo pode permitir a descoberta da chave de criptografia e, consequentemente, do texto original.



00:00

04:13



O que a gente faz em computação, no final das contas, é uma manipulação de números.



EXERCÍCIO DE FIXAÇÃO

Qual é o nome do algoritmo de criptografia que utiliza a mesma chave para cifrar e decifrar?

PALAVRAS-CHAVE

Aritmética modular: É uma parte da teoria dos números que lida com números inteiros e suas propriedades quando considerados em relação a um número fixo chamado de “módulo”.



07:40

13:00



Criptografia simétrica

A criptografia simétrica é aquela em que a mesma chave é utilizada para cifrar e decifrar uma mensagem. As cifras modernas são cifras de bloco, em que um bloco de bits é misturado de uma só vez, proporcionando maior entropia e, consequentemente, um texto cifrado mais aleatório. O tamanho da chave é importante, uma vez que ela deve ter o mesmo tamanho do bloco de bits a ser cifrado, e a segurança efetiva é metade do número de bits utilizados. O AES é um exemplo de cifra utilizada atualmente, com chaves de 128 ou 256 bits, sendo mais recomendado utilizar a de 256 bits para garantir uma segurança maior.

PALAVRAS-CHAVE

One-Time Pad: O termo se refere a um problema que pode ocorrer em sistemas operacionais baseados em Unix, como o Linux. Esse problema ocorre quando um programa deixa um arquivo aberto por um longo período de tempo, criando um “caminho de longa duração” para o arquivo.



14:49

EXERCÍCIO DE FIXAÇÃO

Qual é o tamanho das chaves utilizadas na cifra AES?

19:19



PALAVRA-CHAVE

Paradoxo do aniversário: É um problema matemático que envolve a probabilidade de que duas ou mais pessoas em um grupo tenham a mesma data de aniversário. Embora pareça ser uma questão simples, os resultados são surpreendentes e contra intuitivos.

Exemplo de cifra

Avelino apresenta uma animação sobre uma cifra de 128 bits, que é utilizada como um padrão para criptografia. E destaca que a segurança do algoritmo depende da força da chave e não deve depender do algoritmo em si, que é conhecido. A tabela de substituição pode ser gerada de maneira fixa ou por uma função, mas é importante que a chave seja mantida em segredo, pois é ela que garante a segurança da cifragem.

24:01



Um algoritmo de cifragem ele deve me trazer confusão e difusão.

26:20



PALAVRA-CHAVE

Criptografia AES

O algoritmo de criptografia AES (Advanced Encryption Standard) tem um processo de escalonamento de chave, que gera chaves diferentes para cada uma das rodadas de criptografia, esse processo é diferente dependendo da versão do AES utilizada. A chave é o ponto crítico do sistema, pois se alguém tiver acesso a ela, pode decifrar o texto criptografado. O processo de criptografia é feito por meio de operações que envolvem a substituição e permutação de bits, e a chave é utilizada para gerar diferentes chaves para cada rodada.

26:37



36:31



Cifra de RaideL: Também conhecida como cifra de Rail Fence, é um método simples de criptografia por substituição que envolve a transposição de letras em uma mensagem. Seu nome vem do fato de que as letras da mensagem são escritas em um padrão que se assemelha a uma cerca em forma de “V”.

43:06



PALAVRA-CHAVE

Efeito cascata: Ocorre quando uma mudança feita em uma parte do código afeta outras partes do programa de maneira imprevista, muitas vezes gerando erros ou comportamentos inesperados. Muitos programas são construídos em camadas ou módulos interconectados, e mudanças em parte do código podem afetar o comportamento de outras partes do programa que dependem dela.

AULA 3 • PARTE 3

Modo de operação: parte I

Modo de operação é uma forma que se utiliza para aplicar uma cifra de bloco. Existem diferentes modos de operação que podem ser utilizados na aplicação de cifras de blocos, como o CBC e o Counter Mode. É importante escolher o modo de operação correto para garantir a segurança da criptografia, evitando que um atacante possa decifrar a mensagem com base em informações determinísticas. O uso correto do vetor de inicialização vai garantir que os valores cifrados de um mesmo bloco sejam diferentes.



00:00

07:24



“ Se eu não usar de maneira correta eu vou criar vulnerabilidade no meu desenvolvimento de software.”

10:12



11:54



Modo de operação: parte II

O modo de operação CTR ou Counter é uma cifra de fluxo utilizado na criptografia simétrica. Esse modo de operação permite cifrar e decifrar em paralelo e é muito apropriado para ser usado em máquinas com diversos processadores. O vetor de inicialização é chamado de contador inicial, que é gerado seguindo algumas regras e é um número de 128 bits. Além disso, é importante usar modos de operação na criptografia simétrica e como funciona o preenchimento de padding para completar a mensagem quando ela não é múltipla de 128 bits.

PALAVRAS-CHAVE

Padding: Refere-se à adição de bits ou bytes adicionais a um bloco de dados para atingir um tamanho específico ou formato necessário. Seu objetivo é tornar o tamanho dos blocos de dados uniforme, a fim de atender a requisitos específicos de criptografia, compactação ou transmissão de dados.

Problema do logaritmo discreto

O problema do logaritmo discreto em aritmética modular consiste em descobrir o valor de x na equação $g^x \equiv a \pmod{p}$, em que g e p são números primos e a é um número inteiro. Para números pequenos, a solução é trivial, mas para números grandes é um problema difícil que requer muita computação. O conceito de gerador é introduzido como um valor que, elevado em qualquer expoente, gera um conjunto de valores diferentes que compõem o conjunto Z de p^* . O logaritmo discreto é um problema difícil da matemática, sem algoritmo polinomial para resolvê-lo para números grandes.



21:51

EXERCÍCIO DE FIXAÇÃO

O que é o módulo na aritmética modular?

PALAVRAS-CHAVE

Protocolo Diffie-Hellman: É um protocolo de criptografia de chave pública utilizado para estabelecer uma chave secreta compartilhada entre dois participantes em uma rede não segura. O protocolo foi desenvolvido em 1976 pelos criptógrafos Whitfield Diffie e Martin Hellman.

“ Parece mágica mas é só matemática. **”**

34:37



PALAVRA-CHAVE

Curva elíptica: É uma curva definida por uma equação do tipo $y^2 = x^3 + ax + b$, onde a e b são constantes reais (ou complexas). São usadas em criptografia para a geração de chaves criptográficas.

35:15



36:10



Criptografia RSA

A escolha de números primos é uma das primeiras etapas do processo de criptografia RSA. Os números primos são multiplicados para criar um número composto, que é usado como o módulo para a criptografia. Para escolher a chave pública, é necessário escolher um número que seja relativamente primo ao módulo escolhido, e para escolher a chave privada é necessário encontrar o inverso multiplicativo do número escolhido para a chave pública. Para obter mais segurança, são utilizados números com mais de 2048 bits, sendo o algoritmo RSA um dos algoritmos mais utilizados para criptografia.

45:34



AULA 3 • PARTE 4

00:00



Exemplo prático: parte I

Alguns conceitos são importantes para entender a importância da segurança na comunicação. O WhatsApp é um exemplo prático que demonstra a cifragem de ponta a ponta, que protege as mensagens de ataques e hackers. O protocolo de comunicação utilizado pelo WhatsApp é baseado em curvas elípticas, em que é gerado um segredo entre as duas partes. Cada mensagem enviada pelo WhatsApp é cifrada com uma chave diferente, chamada de One Time Pad. Para isso, é utilizado um algoritmo de expansão de chaves, que gera chaves únicas para cada mensagem.

PALAVRAS-CHAVE

One time pre key: É um conceito utilizado em protocolos de criptografia de chave pública. Essa técnica é utilizada para estabelecer uma chave secreta temporária entre duas partes que desejam se comunicar de forma segura em uma rede não confiável.



05:01

PALAVRAS-CHAVE

HMAC: Hash Message Authentication Code é um algoritmo de autenticação de mensagens que usa uma combinação de uma chave secreta e uma função de hash para produzir um código de autenticação de mensagem. Ele é frequentemente usado em protocolos de segurança, como SSL/TLS, SSH, IPsec e outros.

Exemplo prático: parte III

Seguindo a explicação do funcionamento da criptografia no WhatsApp, o professor Avelino destaca que o algoritmo utilizado inclui algumas fases como a geração de uma chave pública, a troca de chaves e a criação da próxima chave. O áudio, vídeo, imagem ou texto que é transmitido é cifrado usando uma chave específica e um MAC para integridade, sendo armazenado cifrado no WhatsApp. Quando o receptor recebe a mensagem, ele decifra a mensagem e busca o objeto correspondente para decifrar. É importante estudar a implementação do algoritmo para compreender completamente a criptografia no WhatsApp.

“ Vocês não precisam trabalhar com segurança, mas você tem que pensar que o que vocês estão fazendo pode ter influência na parte de segurança. **”**



09:44



10:21

Exemplo prático: parte II

O docente explica como funciona o protocolo de segurança do WhatsApp. Quando um usuário instala o aplicativo, um par de chaves pública e privada é gerado em seu dispositivo, e apenas as chaves públicas são enviadas para o servidor do WhatsApp. Essas chaves são usadas para estabelecer uma sessão cifrada entre usuários, mesmo que o destinatário não esteja ativo no momento. O iniciador da comunicação pede as chaves públicas do destinatário para o servidor do WhatsApp e, em seguida, gera uma chave efêmera para ser usada na comunicação. Esse processo é repetido sempre que o destinatário acaba suas chaves públicas, e as chaves privadas permanecem apenas no dispositivo do usuário. Garantindo que apenas os usuários envolvidos na comunicação tenham acesso às informações transmitidas.



21:51



23:58

PALAVRA-CHAVE



33:20

Hash Ratchet: Mecanismo de segurança utilizado em protocolos de criptografia de ponta a ponta para renovar as chaves criptográficas usadas na comunicação entre dois dispositivos. Usado em aplicativos de mensagens instantâneas e outros sistemas que exigem criptografia segura de ponta a ponta.

Resumo da disciplina

Veja, nesta página, um resumo dos principais conceitos vistos ao longo da disciplina.

AULA 1

Criptografia é transformação.



A criptografia é tão forte quanto a capacidade de proteger as suas chaves.

A informação não trafega sempre pelo mesmo caminho, ela vai se adaptando para o caminho mais fácil.



AULA 2

A consequência da correção é a proteção.



Dentro da análise a gente precisa garantir que os dados sejam protegidos.



Sempre vai ter alguém motivado a explorar alguma falha.



AULA 3

O mundo digital é um mundo mágico.



A velocidade das mudanças que estão acontecendo atualmente, é muito grande.



Se eu não usar de maneira correta eu vou criar vulnerabilidade no meu desenvolvimento de software.



Avaliação

Veja as instruções para realizar a avaliação da disciplina.

Já está disponível o teste online da disciplina. O prazo para realização é de **dois meses a partir da data de lançamento das aulas**.

Lembre-se que cada disciplina possui uma avaliação online.
A nota mínima para aprovação é 6.

Fique tranquilo! Caso você perca o prazo do teste online, ficará aberto o teste de recuperação, que pode ser realizado até o final do seu curso. A única diferença é que a nota máxima atribuída na recuperação é 8.

