

Roteiro Aula Prática



ARQUITETURA DE SEGURANÇA

ROTEIRO DE AULA PRÁTICA

NOME DA DISCIPLINA: ARQUITETURA DE SEGURANÇA

Unidade: SEGURANÇA DE COMPUTADORES

Seção: Funções Hash

OBJETIVOS

Definição dos objetivos da aula prática:

- Compreender os tipos de ataques às Funções Hash.
- Explorar como o código hash é constituído e por que aprimora a segurança.
- Listar os principais conceitos das Funções Hash.

INFRAESTRUTURA

Instalações – Materiais de consumo – Equipamentos:

LABORATÓRIO DE INFORMÁTICA

Equipamentos:

- Desktop Lab Informatica - Positivo C6300
- ~ 1 un para cada aluno

SOLUÇÃO DIGITAL

- SHA-256 Online Hash Generator (Web)

Esta ferramenta online SHA256 ajuda a calcular hash de string ou binário. Você pode inserir UTF-8, UTF-16, Hex em SHA256. Ele também oferece suporte a HMAC.

EQUIPAMENTO DE PROTEÇÃO INDIVIDUAL (EPI)

Não se aplica

PROCEDIMENTOS PRÁTICOS

Procedimento/Atividade nº 1 (Físico)

Atividade proposta:

Nesta atividade prática, você será o protagonista e explorará conceitos de Funções Hash, sua importância na segurança e os tipos de ataques a elas.

Procedimentos para a realização da atividade:

Passo 1: Introdução aos Conceitos

Leia sobre Funções Hash e anote os principais conceitos:

- Função de Hash.
- Integridade de dados.
- Propriedades das Funções Hash.

Passo 2: Tipos de Ataques às Funções Hash

Pesquise e defina os principais tipos de ataques às Funções Hash:

- Ataque de Colisão.
- Ataque de Pré-Imagem.
- Ataque de Pós-Imagem.

Passo 3: Estrutura de um Código Hash

Explique como um código hash é constituído, incluindo:

- O processo de transformação.
- O tamanho do resultado.
- O uso de algoritmos de hash.

Realize um experimento prático para gerar um código hash a partir de um texto simples usando uma ferramenta online, como "SHA-256 Online Hash Generator."

Exemplo de aplicação:

Acesse o Gerador de Hash SHA-256 Online

Você pode encontrar várias ferramentas online que geram hashes SHA-256. Para este exemplo, suponha que você esteja usando o site "<https://www.xorbin.com/tools/sha256-hash-calculator>". Abra seu navegador e acesse essa página ou uma similar.

Insira o texto ou carregue o arquivo

Se você deseja calcular o hash de um texto, basta digitar ou colar o texto no campo fornecido.

Se você deseja calcular o hash de um arquivo, procure e selecione o arquivo em seu computador clicando no botão "Procurar" ou "Escolher arquivo", dependendo da página da web.

Calcule o hash

Clique no botão "Calcular Hash SHA-256" ou em uma opção semelhante na página da web que você está usando.

Obtenha o resultado

Depois de clicar no botão, a página fornecerá o valor hash SHA-256 correspondente ao texto ou arquivo que você inseriu. Esse valor será exibido na página ou você receberá um link para baixar um arquivo com o resultado.

Exemplo 1: Calcular o hash de um texto

Suponha que você queira calcular o hash SHA-256 do texto "Olá, mundo!".

Insira "Olá, mundo!" no campo de texto.

Clique no botão "Calcular Hash SHA-256".

A página exibirá o hash SHA-256 correspondente, que se parecerá com isso:
"7509e5bda0c762d2bac7f90d758b5b2263fa01ccbc542ab5e3df163be08e6ca9".

Exemplo 2: Calcular o hash de um arquivo

Suponha que você tenha um arquivo chamado "documento.txt" em seu computador e deseja calcular o hash SHA-256 desse arquivo.

- Clique no botão "Procurar" ou "Escolher arquivo".
- Procure e selecione o arquivo "documento.txt" em seu computador.
- Clique no botão "Calcular Hash SHA-256".

A página fornecerá o valor hash SHA-256 correspondente ao arquivo "documento.txt".

Lembre-se de que o valor hash SHA-256 é único para cada entrada e é útil para verificar a integridade de dados ou para comparar arquivos.

Passo 4: Por que Funções Hash Aprimoram a Segurança

Liste e explique por que o uso de Funções Hash aprimora a segurança em sistemas, destacando a importância na detecção de alterações em dados.

Exemplifique a aplicação de Funções Hash em segurança de senhas, mostrando como uma senha pode ser armazenada de forma segura usando hash.

Checklist:

- Defini os principais conceitos das Funções Hash.
- Identifiquei os tipos de ataques às Funções Hash.
- Expliquei como um código hash é constituído.

Procedimento/Atividade nº 1 (Virtual)

Atividade proposta:

Nesta atividade prática, você será o protagonista e explorará conceitos de Funções Hash, sua importância na segurança e os tipos de ataques a elas.

Procedimentos para a realização da atividade:

Passo 1: Introdução aos Conceitos

Leia sobre Funções Hash e anote os principais conceitos:

- Função de Hash.
- Integridade de dados.
- Propriedades das Funções Hash.

Passo 2: Tipos de Ataques às Funções Hash

Pesquise e defina os principais tipos de ataques às Funções Hash:

- Ataque de Colisão.
- Ataque de Pré-Imagem.

- Ataque de Pós-Imagem.

Passo 3: Estrutura de um Código Hash

Explique como um código hash é constituído, incluindo:

- O processo de transformação.
- O tamanho do resultado.
- O uso de algoritmos de hash.

Realize um experimento prático para gerar um código hash a partir de um texto simples usando uma ferramenta online, como "SHA-256 Online Hash Generator."

Exemplo de aplicação:

Acesse o Gerador de Hash SHA-256 Online

Você pode encontrar várias ferramentas online que geram hashes SHA-256. Para este exemplo, suponha que você esteja usando o site "<https://www.xorbin.com/tools/sha256-hash-calculator>". Abra seu navegador e acesse essa página ou uma similar.

Insira o texto ou carregue o arquivo

Se você deseja calcular o hash de um texto, basta digitar ou colar o texto no campo fornecido.

Se você deseja calcular o hash de um arquivo, procure e selecione o arquivo em seu computador clicando no botão "Procurar" ou "Escolher arquivo", dependendo da página da web.

Calcule o hash

Clique no botão "Calcular Hash SHA-256" ou em uma opção semelhante na página da web que você está usando.

Obtenha o resultado

Depois de clicar no botão, a página fornecerá o valor hash SHA-256 correspondente ao texto ou arquivo que você inseriu. Esse valor será exibido na página ou você receberá um link para baixar um arquivo com o resultado.

Exemplo 1: Calcular o hash de um texto

Suponha que você queira calcular o hash SHA-256 do texto "Olá, mundo!".

Insira "Olá, mundo!" no campo de texto.

Clique no botão "Calcular Hash SHA-256".

A página exibirá o hash SHA-256 correspondente, que se parecerá com isso:
"7509e5bda0c762d2bac7f90d758b5b2263fa01ccbc542ab5e3df163be08e6ca9".

Exemplo 2: Calcular o hash de um arquivo

Suponha que você tenha um arquivo chamado "documento.txt" em seu computador e deseja calcular o hash SHA-256 desse arquivo.

- Clique no botão "Procurar" ou "Escolher arquivo".
- Procure e selecione o arquivo "documento.txt" em seu computador.
- Clique no botão "Calcular Hash SHA-256".

A página fornecerá o valor hash SHA-256 correspondente ao arquivo "documento.txt".

Lembre-se de que o valor hash SHA-256 é único para cada entrada e é útil para verificar a integridade de dados ou para comparar arquivos.

Passo 4: Por que Funções Hash Aprimoram a Segurança

Liste e explique por que o uso de Funções Hash aprimora a segurança em sistemas, destacando a importância na detecção de alterações em dados.

Exemplifique a aplicação de Funções Hash em segurança de senhas, mostrando como uma senha pode ser armazenada de forma segura usando hash.

Checklist:

- Defini os principais conceitos das Funções Hash.
- Identifiquei os tipos de ataques às Funções Hash.
- Expliquei como um código hash é constituído.

RESULTADOS

Resultados de Aprendizagem:

Compreender os conceitos de Funções Hash, os tipos de ataques que podem ocorrer, como os códigos hash são constituídos e por que eles aprimoram a segurança.

ROTEIRO DE AULA PRÁTICA

NOME DA DISCIPLINA: ARQUITETURA DE SEGURANÇA

Unidade: ANÁLISES E POLÍTICA DE SEGURANÇA

Seção: Processos e políticas de segurança

OBJETIVOS

Definição dos objetivos da aula prática:

- Passo a Passo:
- Introduza o conceito de fatores de risco de ataque e forneça um cenário fictício (por exemplo, uma empresa com informações confidenciais).
- Listar os possíveis riscos de ataque nesse cenário.
- Justificar cada risco identificado.

INFRAESTRUTURA

Instalações – Materiais de consumo – Equipamentos:

LABORATÓRIO DE INFORMÁTICA

Equipamentos:

- Desktop Lab Informatica - Positivo C6300
- ~ 1 un para cada aluno

SOLUÇÃO DIGITAL

- MICROSOFT WORD (Software)

Microsoft Word - É um software de processamento de texto amplamente utilizado para criar, editar e formatar documentos.

EQUIPAMENTO DE PROTEÇÃO INDIVIDUAL (EPI)

Não se aplica

PROCEDIMENTOS PRÁTICOS

Procedimento/Atividade nº 1 (Físico)

Atividade proposta:

Interpretação de políticas de segurança e listagem de normas gerais de segurança.

Procedimentos para a realização da atividade:

Parte 1: Identificação de Riscos

Escolher um cenário de sua preferência, como uma empresa fictícia ou uma rede doméstica, e descrever o ambiente, incluindo sistemas, dados e ameaças potenciais.

Com base nesse cenário, o aluno deve listar pelo menos três fatores de risco de ataque, explicando sua escolha.

Parte 2: Interpretação de Políticas de Segurança

Pesquisar online e selecionar uma política de segurança de uma organização real ou fictícia.

Após a escolha, interpretar essa política, identificando seus objetivos e práticas recomendadas.

Parte 3: Listagem de Normas Gerais de Segurança

pesquisar e listar três normas gerais de segurança reconhecidas, como ISO 27001, NIST ou GDPR, explicando brevemente os princípios e requisitos-chave de cada norma.

Parte 4: Experimento Prático em Configuração de Segurança

Escolher um tópico prático, como a configuração de um firewall ou a implementação de criptografia.

Utilizar um guia ou tutorial online, seguir as etapas e documentar o processo de configuração.

Checklist:

- Escolha um tópico prático de segurança.
- Realize o experimento prático com êxito.
- Documente o processo de configuração.

Procedimento/Atividade nº 1 (Virtual)

Atividade proposta:

Interpretação de políticas de segurança e listagem de normas gerais de segurança.

Procedimentos para a realização da atividade:

Parte 1: Identificação de Riscos

Escolher um cenário de sua preferência, como uma empresa fictícia ou uma rede doméstica, e descrever o ambiente, incluindo sistemas, dados e ameaças potenciais.

Com base nesse cenário, o aluno deve listar pelo menos três fatores de risco de ataque, explicando sua escolha.

Parte 2: Interpretação de Políticas de Segurança

Pesquisar online e selecionar uma política de segurança de uma organização real ou fictícia.

Após a escolha, interpretar essa política, identificando seus objetivos e práticas recomendadas.

Parte 3: Listagem de Normas Gerais de Segurança

pesquisar e listar três normas gerais de segurança reconhecidas, como ISO 27001, NIST ou GDPR, explicando brevemente os princípios e requisitos-chave de cada norma.

Parte 4: Experimento Prático em Configuração de Segurança

Escolher um tópico prático, como a configuração de um firewall ou a implementação de criptografia.

Utilizar um guia ou tutorial online, seguir as etapas e documentar o processo de configuração.

Checklist:

- Escolha um tópico prático de segurança.
- Realize o experimento prático com êxito.
- Documente o processo de configuração.

RESULTADOS

Resultados de Aprendizagem:

Ao concluir esta atividade prática, os alunos devem ser capazes de identificar fatores de risco de ataque, interpretar políticas de segurança, listar normas gerais de segurança e aplicar conceitos

de segurança em um experimento prático de configuração. Eles também devem compreender a importância da segurança da informação e ser capazes de aplicar esses conceitos de forma independente em ambientes virtuais.

NORMAS PARA ELABORAÇÃO E ENTREGA DO RELATÓRIO DE ATIVIDADE PRÁTICA

Olá, estudante. Tudo bem?

As atividades práticas visam desenvolver competências para a atuação profissional. Elas são importantes para que você vivencie situações que te prepararão para o mercado de trabalho.

Por isso, trazemos informações para que você possa realizar as atividades propostas com êxito.

1. Que atividade deverá ser feita?

- A(s) atividades a ser(em) realizada(s) estão descritas no Roteiro de Atividade Prática, disponível no AVA.
- Após a leitura do Roteiro, você deverá realizar a(s) atividade(s) prática(s) solicitadas e elaborar um documento **ÚNICO** contendo todas as resoluções de acordo com a proposta estabelecida.
- O trabalho deve ser autêntico e contemplar todas as resoluções das atividades propostas. Não serão aceitos trabalhos com reprodução de materiais extraídos da internet.

2. Como farei a entrega dessa atividade?

- Você deverá postar seu trabalho final no AVA, na pasta específica relacionada à atividade prática, obedecendo o prazo limite de postagem, conforme disposto no AVA.
- Todas as resoluções das atividades práticas devem ser entregues em um **ARQUIVO ÚNICO** de até 10 MB.
- O trabalho deve ser enviado em formato Word ou PDF, exceto nos casos em que há formato especificado no Roteiro.
- O sistema permite anexar apenas um arquivo. Caso haja mais de uma postagem, será considerada a última versão.

IMPORTANTE:

- A entrega da atividade, de acordo com a proposta solicitada, é um critério de aprovação na disciplina.
- Não há prorrogação para a postagem da atividade.

Aproveite essa oportunidade para aprofundar ainda mais seus conhecimentos.

Bons estudos!