



INSTITUTO FEDERAL

Sul-rio-grandense
Câmpus Charqueadas

Aula 10

- Autenticação de usuários

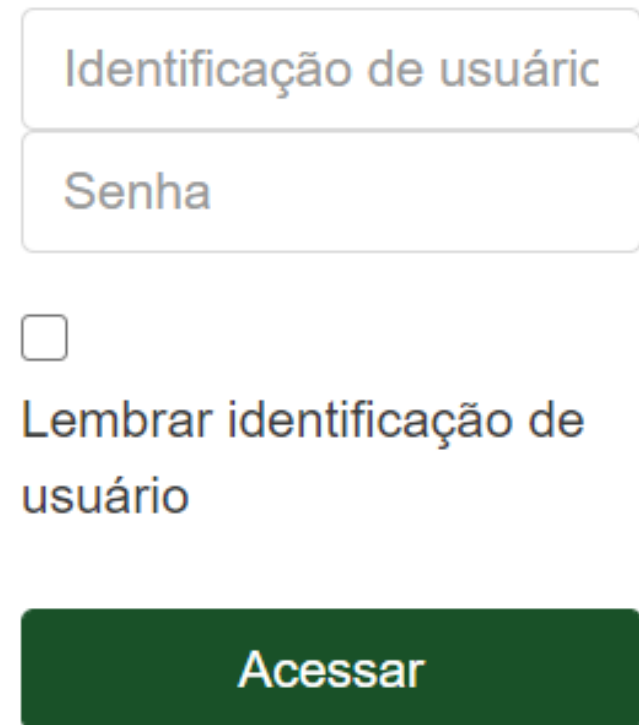
Desenvolvimento Back-end 1

Prof. Sérgio Yoshimitsu Fujii

Autenticação

Para que serve?

- Autenticação é utilizada para garantir que um usuário tenha acesso exclusivo às suas informações;
 - E-mail, caixa eletrônico etc.
- O acesso geralmente é dado através de nome de usuário e senha;



A mockup of a login form with a light gray border. It contains two input fields: the top one is labeled 'Identificação de usuáric' and the bottom one is labeled 'Senha'. Below these fields is a checkbox with the label 'Lembrar identificação de usuário'. At the bottom of the form is a dark green button with the text 'Acessar' in white.

Autenticação

Senha

- A parte mais importante da autenticação é a senha;
- É a chave para o acesso do usuário;
- Como armazenar a senha de forma segura?



A user authentication form with a light gray border. It contains a label 'Identificação de usuáric' in gray text. Below it is a text input field with the placeholder 'Senha', which is highlighted by a thick red rectangular border. Underneath the input field is a checkbox and the text 'Lembrar identificação de usuário'. At the bottom of the form is a dark green button with the white text 'Acessar'.

Autenticação

Senha - Criptografia

- A forma mais segura de armazenar uma senha é aplicando algoritmos de criptografia;
- Geralmente é utilizado um algoritmo de hash;
 - Gera um valor a partir de uma fórmula matemática que é praticamente impossível de reverter;
 - Ex.: MD5, Crypt_Blowfish, Argon2 etc.

Autenticação

MD5

- Algoritmo de Hash de 128 bits e 32 caracteres;
- Amplamente utilizado para checar a integralidade dos dados através da soma de verificação (checksum).

```
1  <?php
2      $hashmd5 = md5('senha123');
3  ?>
```

Autenticação

MD5

- Atualmente, não é mais utilizado para criptografia de senhas;
- Rainbow Table;
 - “*É uma tabela pré-computada para reverter funções hash criptográficas, geralmente para quebrar hashes de senhas*”.
- https://pt.wikipedia.org/wiki/Tabela_arco-íris

Autenticação

PHP – Funções de Criptografia

- **password_hash()**
- **crypt()**
- **password_verify()**

Autenticação

PHP – Funções de Criptografia

- **password_hash()**
 - Cria uma senha utilizando um determinado algoritmo de hash;
 - *PASSWORD_BCRYPT* - Usa o algoritmo bcrypt;
 - *PASSWORD_ARGON2I* - Usa o algoritmo Argon2;
 - *PASSWORD_DEFAULT* - Usa o algoritmo padrão (bcrypt).

Autenticação

PHP – Funções de Criptografia

- **password_hash()**

```
1  <?php
2      $hash = password_hash("sergio",PASSWORD_DEFAULT);
3  ?>
```

Autenticação

PHP – Funções de Criptografia

- **crypt()**
 - Faz a criptografia de qualquer string
 - *CRYPT_STD_DES* - Codificação Standard DES-based;
 - *CRYPT_EXT_DES* - Codificação Extended DES-based;
 - *CRYPT_MD5* - Codificação MD5;
 - *CRYPT_BLOWFISH* - Codificação Blowfish.

Autenticação

PHP – Funções de Criptografia

- **password_verify()**
 - Verifica um hash criado pela função *password_hash()*;
 - *Retorna TRUE se o password e o hash corresponderem.*

Autenticação

Leitura

- https://www.php.net/manual/pt_BR/function.password-hash.php
- https://www.php.net/manual/pt_BR/function.password-verify.php
- https://www.php.net/manual/pt_BR/function.crypt.php