UNIVERSIDADE AUGUSTO MOTTA

BONSUCESSO – ANÁLISE E DESENVOLVIMENTO DE SISTEMAS – MANHÃ – 2.2023

Alunos:

* Gil Guimarães
* Ygor da Silva Pinheiro
* Bryan Ferreira de Almeida

**Projeto Back-End - Claro**

**PHP e SQL**

O projeto consiste em:

* Front-End
* Back-End
* Modelo Entidade Relacionamento (MER)

As telas e suas funcionalidades:

* Login

- É a primeira tela que o usuário tem acesso, sendo o index do projeto (da pasta raiz).

- Essa tela contém campos de Login, Senha e qual o Tipo de usuário (“Comum” ou “Master”) que está conectando. E então a validação acontece com base nesses 3 requisitos.

- O formulário presente nessa tela redireciona os dados para o servidor, ocorrendo então a validação, e se as todas as credenciais estiverem corretas, o usuário prossegue para a tela de 2FA (Segundo Fator de Autenticação). As sessões de: Nome, Senha, Login, Tipo e CPF são criadas.

- É nessa validação que ocorre a criação da sessão, assim sendo utilizada para todo o projeto, sendo então uma experiência única para o usuário, pois é através da sessão que as consultas SQL serão feitas nas outras telas. E sem essa validação, não há acesso ao resto do sistema (Junto com a validação de segundo fator). Inclusive, o CPF é chave primária, e não há possibilidade de existir mais de um CPF igual no banco de dados.

- Apenas usuários ativos podem logar.

- Usuários já logados não tem acesso a essa tela, a não ser que realizem o logout.

* Cadastro

- Se o usuário não estiver cadastrado, há uma opção na tela de Login onde redireciona para a tela de cadastro. E então, o usuário preenche suas credenciais no formulário e envia para o servidor validar. É bom lembrar que o CPF do usuário precisará ser válido segundo a Receita Federal, se não, o sistema o avisa que o CPF é inválido e interrompe a entrada dos dados no banco de dados.

- O usuário também terá de escolher um Login único, se houver outro Login no banco de dados idêntico ao que está sendo enviado, a entrada de dados não dará continuidade.

- Se as credenciais estiverem todas corretas, a entrada então é feita, com o usuário já estando ativo e sendo do Tipo “Comum”. O usuário então é redirecionado para a tela de Login.

- Usuários já logados não tem acesso a essa tela, a não ser que realizem o logout.

* 2FA (Segundo Fator de Autenticação)

- Inicialmente, ele verifica se o usuário está autenticado e se a autenticação em duas etapas já está ativa, redirecionando-o para a página principal se necessário. A página exibe uma pergunta de segurança com base nas informações do usuário armazenadas no banco de dados. A pergunta é escolhida aleatoriamente entre três opções: CEP do endereço, nome da mãe e data de nascimento. O usuário fornece uma resposta, e dependendo da pergunta, a resposta é validada. Se a resposta estiver correta, a autenticação em duas etapas é ativada, e o usuário é redirecionado para a página principal. Caso contrário, ocorre o encerramento da sessão e o usuário é redirecionado para a página de login. A página HTML exibe a pergunta, solicita a resposta do usuário e fornece a opção de confirmar a resposta.

* Tela Principal (Main)

- Este código cria a página principal de um sistema após a autenticação do usuário. Inicialmente, verifica se o usuário está autenticado e se a autenticação em duas etapas está ativa. Se não estiver, redireciona para uma página de erro. A página principal inclui uma barra de navegação, um cabeçalho com uma imagem de logo e um efeito de ondas. O conteúdo principal varia com base no tipo de usuário (Master ou Comum). Para usuários Master, são exibidas mensagens de boas-vindas personalizadas, com links para acessar serviços adicionais e consultas. Para usuários Comuns, a mensagem destaca o acesso aos serviços e incentiva a explorar promoções no site. A página também oferece um link para visualizar o modelo Entidade-Relacionamento (ER) do sistema. O rodapé é incluído no final da página.

- Um detalhe interessante é que o footer e a navbar são criados nesse projeto como elementos, assim, os podendo chamar no projeto quando necessário. Fizemos dessa maneira para melhor manutenção.

* Consulta

- Este código cria uma página de administração de usuários apenas para usuário(s) Master. Ele inicia a sessão, verifica a autenticação do usuário e se a autenticação em duas etapas está ativa. Se o usuário não estiver autenticado ou for do tipo Comum, é redirecionado para páginas de erro correspondentes. A página exibe uma tabela de usuários recuperada do banco de dados, apresentando informações como login, nome, idade, CPF, telefone fixo, tipo de usuário e status. Além disso, fornece funcionalidades para ativar, desativar ou deletar usuários, dependendo do status atual. Há também um campo de pesquisa que permite filtrar os usuários na tabela.

* Modelo

- Este código cria uma página que exibe um modelo Entidade-Relacionamento (ER) do site. Antes de mostrar o modelo, verifica se o usuário está autenticado e se a autenticação em duas etapas está ativa. Caso contrário, redireciona para uma página de erro. A página apresenta uma imagem do modelo ER centralizada e uma breve mensagem explicativa abaixo.

* Serviços

- Esse código cria uma página de serviços (fictícios) que oferece planos de internet para casa e planos de celular com bônus de internet. Antes de exibir os serviços, ele verifica se o usuário está autenticado e se a autenticação em duas etapas está ativa; caso contrário, redireciona para uma página de erro. A página é estilizada, apresentando os planos de internet e celular em cards com informações detalhadas, incluindo preço e opção para contratação via WhatsApp.

* Sobre

- Esse código cria uma página "Sobre Nós" que destaca as fundadoras da empresa "Claro". A página exibe informações sobre três figuras-chave da empresa, Morgana, Syndra e Evelynn, com imagens e detalhes sobre seus papéis na organização. É bom ressaltar que são figuras fictícias e não há nenhum vínculo entre a empresa Riot e a Claro. O layout responsivo utiliza CSS para apresentar essas informações em cards, ajustando-se de acordo com o tamanho da tela. O código também inclui verificações de sessão para garantir que o usuário esteja autenticado antes de acessar a página.

* Elementos: Navbar e Footer

- Os códigos apresentados são componentes modulares para construir uma página web. O Footer define um rodapé com links sociais, menu e informações de direitos autorais, adaptando-se dinamicamente ao tipo de usuário. O Navbar cria uma barra de navegação responsiva com marca, links dinâmicos e animação de ícone para telas menores. Ambos são projetados para inclusão em várias páginas, promovendo a reutilização e facilitando a manutenção do site. Ambos componentes deixam explícitos pro usuário os links para acesso a outras telas, sendo que o link para acesso a tela de Consulta seja acessível e exposta apenas para o usuário Master logado. O mesmo acontece com a página de alteração de senha, onde apenas usuários comuns podem acessar e realizar a alteração, deixando também o link inacessível. Vale ressaltar que na navbar, fica exposto o nome do usuário logado. Assim como na tela principal.

* Alteração de Senha

- Este código constitui uma página de alteração de senha para usuários autenticados. A primeira parte (PHP) verifica a autenticação do usuário, proíbe o acesso indevido (Proíbe o usuário Master) e processa a alteração da senha se o formulário for enviado corretamente. A segunda parte (HTML) apresenta o formulário de alteração de senha, com campos para a nova senha e sua confirmação.O script JavaScript valida se as senhas inseridas correspondem antes de enviar o formulário. A página possui um design responsivo e inclui links para outras páginas relevantes do sistema.

* Telas de Erro

As telas de erro são separadas em três arquivos:

Erro para acesso ao login, Erro para reativação de conta, Erro para voltar para a página onde o usuário estava:

1. Erro para acesso ao login:

Este código representa uma página de erro de autenticação. Caso ocorra uma falha na autenticação do usuário, esta página é exibida. Ela apresenta uma mensagem de erro centralizada, indicando que houve um problema na autenticação e incentivando o usuário a verificar suas credenciais. Além disso, oferece um botão "Login" que redireciona o usuário à página de login principal. O design inclui estilos para proporcionar uma experiência visual coerente com a identidade visual da aplicação.

1. Erro para reativação de conta:

Este código representa uma página de erro de login projetada para o caso em que o usuário tenta fazer login em uma conta desativada. A página exibe uma mensagem de erro indicando que ocorreu um problema no login e informa ao usuário que a conta foi desativada. Fornece uma opção de reativação por meio de um link de contato, que redireciona para o WhatsApp com uma mensagem pré-configurada para reativar a conta. Além disso, há um botão "Voltar" que permite ao usuário retornar à página anterior. O design inclui estilos para uma apresentação visual coesa com a identidade visual da aplicação.

1. Erro para voltar:

Este código representa uma página de erro que é exibida quando um usuário tenta acessar uma página restrita, como a de alteração de senha, sem as permissões adequadas. A página exibe uma mensagem indicando que ocorreu um erro ao tentar acessar a página desejada. Sugere que o usuário entre em contato com o suporte para obter assistência e fornece um link para contato via WhatsApp. Além disso, há um botão "Voltar" que permite ao usuário retornar à página anterior. O design da página segue a identidade visual da aplicação.

* Arquivo Logout

- O arquivo "logout.php" é utilizado como um ponto de encerramento de sessão em uma aplicação web. Quando chamado, ele inicia a sessão, a encerra usando session\_destroy(), exibe um alerta informando que o usuário saiu da conta e redireciona o navegador para o login. Essa funcionalidade é comumente utilizada como âncora nos elementos de navegação da aplicação, como o botão de logout na barra de navegação e no rodapé da página. Ao clicar nesses botões, o arquivo "logout.php" é chamado, resultando na destruição da sessão e no redirecionamento do usuário para a página inicial. Isso proporciona uma maneira eficaz e segura para que os usuários encerrem suas sessões e saiam de suas contas.