



Universidade Federal de Uberlândia

Faculdade de Computação

10º Trabalho de Programação para Internet – Prof. Daniel A. Furtado

Trabalho Individual – Desenvolvimento Web com Banco de Dados

Instruções Gerais

- Esta atividade deve ser realizada individualmente;
- Utilize apenas as tecnologias HTML5, CSS, JavaScript, Bootstrap 5, PHP e MySQL;
- Sintaxe da XHTML como ou
 não é permitida (anulará o trabalho);
- O website deve ser hospedado e disponibilizado online, conforme orientações disponíveis no final deste documento;
- Ao construir o website, utilize dados fictícios (**jamaís utilize** dados pessoais como seu nome, CPF, endereço, e-mail etc.);
- Esteja atento às **observações sobre plágio** apresentadas no final deste documento;
- Trabalhos com implementações utilizando trechos de códigos retirados de sites da Internet ou de trabalhos de semestres anteriores serão anulados;
- As páginas web não devem conter qualquer conteúdo de caráter imoral, desrespeitoso, pornográfico, discurso de ódio, desacato etc.;
- O website deve ser validado utilizando as ferramentas disponíveis nos endereços **validator.w3.org** e **jigsaw.w3.org/css-validator** (não deve conter nenhum erro ou *warning*);
- O trabalho deve ser entregue até a data/hora definida pelo professor. Não deixe para enviar o trabalho nos últimos instantes, pois eventuais problemas relacionados a eventos adversos como instabilidade de conexão, congestionamento de rede etc., não serão aceitos como motivos para entrega da atividade por outras formas ou em outras datas;
- Este trabalho deve ser feito **mantendo os trabalhos anteriores intactos**, ou seja, os trabalhos anteriores devem permanecer online conforme foram entregues;
- Trabalhos enviados por e-mail ou pelo MS Teams **não serão considerados**.

Leia os slides de aula disponibilizados no endereço a seguir e resolva os exercícios seguintes.

<http://www.furtado.prof.ufu.br/site/teaching/PPI/PPI-Modulo6-MySQL-PHP.pdf>

OBS: Para visualizar eventuais erros do MySQL, acesse sua conta do infinityfree e configure:

Control Painel → Software → Alter PHP Config → Alter PHP Directives → Display Errors → ON

The image shows a control panel for PHP configuration. It includes three settings: 'Display Errors' with radio buttons for 'Off' and 'On' (where 'On' is selected), 'MB String Input' with a text box containing 'auto', and 'PHP Timezone' with a dropdown menu showing 'America/New_York'. Below these settings is a blue button labeled 'Alter PHP directives'.

Exercício 1

Abra o arquivo <http://www.furtado.prof.ufu.br/site/teaching/PPI/Exemplos-Mysql.zip> e observe o código HTML e os scripts PHP dos cinco exemplos. Utilize o arquivo **sql-tabelas.sql** para criar as tabelas do banco de dados sua conta do infinityfree. Coloque os exemplos online e teste-os.

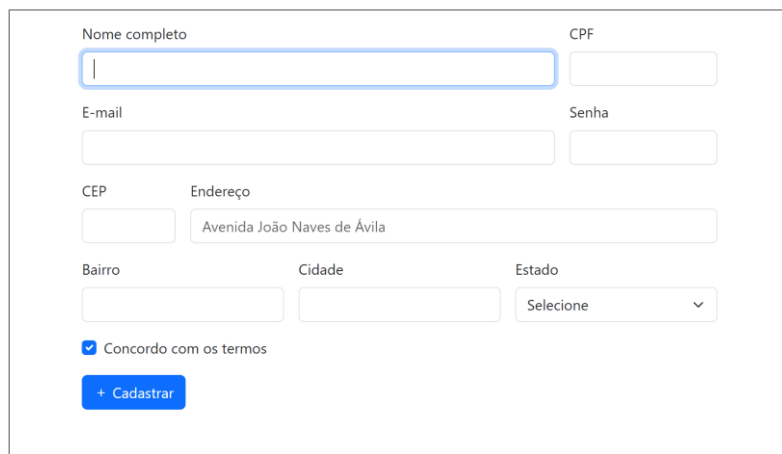
Em seguida, crie uma página HTML simples, de nome **index.html**, descrevendo, de forma sucinta, as principais funcionalidades de cada exemplo.

Exercício 2

- a) Crie uma página HTML simples contendo um formulário para cadastro de contatos. Deve haver os seguintes campos: Nome, E-mail e Mensagem.
- b) Crie um script PHP que receba o formulário pelo método POST e insira os dados em uma tabela do MySQL de nome **Contato** (a tabela deve ser criada). O script deve fazer a inserção na tabela utilizando o método **exec**. Não utilize a função **htmlspecialchars** neste momento;
- a) Crie um segundo script para produzir uma página HTML dinâmica completa listando todos os dados da tabela **Contato**. Os dados devem ser listados em uma tabela HTML. Não utilize a função **htmlspecialchars**. Altere o script de cadastro para que o usuário seja redirecionado para o script de listagem de dados assim que a inserção na tabela for efetuada;
- b) Simule um ataque XSS inserindo código HTML de sua escolha nos campos do formulário (por exemplo, `<h1 style='color: red'>Ataque XSS</h1>`). Observe o resultado na listagem dos dados;
- c) Simule um ataque XSS inserindo código JavaScript nos campos do formulário capaz de redirecionar o usuário para uma página externa quando o script de listagem de dados for requisitado;
- d) Simule um ataque de injeção de SQL para excluir todo o conteúdo da tabela **Contato**.

Exercício 3

- a) Crie uma página HTML contendo um formulário que se apresente como na figura a seguir (Trabalho6 / Exercício 1);
- b) Crie duas tabelas no banco de dados: uma com o nome **Cliente** para armazenar os dados individuais da pessoa (Código, Nome, CPF, E-mail e **hash** da senha) e outra de nome **ClienteEndereco** para armazenar os dados do endereço da pessoa (CEP, Endereço, Bairro, Cidade e Estado). As duas tabelas devem ser vinculadas adequadamente por meio de chave estrangeira. O campo para armazenar o **hash** da senha deve ter um tamanho de pelo menos 60 caracteres;
- c) Crie um script PHP que receba o formulário HTML e faça a devida inserção dos dados nas duas tabelas utilizando o conceito de **transação** e **prepared statements**. Em caso de sucesso, o script deve direcionar o usuário para outro script PHP capaz de produzir uma página HTML dinâmica listando todos os dados das duas tabelas (pessoas e respectivos endereços, sem códigos/ids). Aspectos de segurança devem ser considerados para evitar ataques XSS;
- d) Simule novamente o ataque XSS realizado no exercício anterior. Simule também o ataque de injeção de SQL e analise os resultados.



Formulário de cadastro de cliente:

- Nome completo:
- CPF:
- E-mail:
- Senha:
- CEP:
- Endereço:
- Bairro:
- Cidade:
- Estado:
- ☒ Concordo com os termos
-

e) Crie um arquivo **index.html** que apresente links para executar as seguintes ações:

1. Cadastrar novo cliente
2. Listar clientes cadastrados
3. Testar login de cliente

Os links 1 e 2 devem apenas redirecionar o usuário para as páginas solicitadas no item c) anterior. O link 3 deve permitir ao usuário fazer um teste de login usando os dados cadastrados anteriormente. Utilize como base o exemplo **Ex4-login** disponibilizado no **Exercício 1** deste trabalho.

Disponibilização Online

As páginas dos exercícios devem ser disponibilizadas online utilizando o subdomínio gratuito registrado anteriormente, porém em pasta própria (isto é, seusubdominio.com/trabalhoX/ex1, seusubdominio.com/trabalhoX/ex2, etc.). Não altere ou exclua as pastas dos trabalhos anteriores.

Acrescente um arquivo de nome **index.html** na pasta raiz do trabalho contendo links para as páginas dos exercícios.

Entrega

Além da disponibilização online, a pasta raiz contendo as subpastas dos exercícios deve ser compactada no formato zip e enviada pelo Sistema Acadêmico de Aplicação de Testes (SAAT) até a data limite indicada pelo professor em sala de aula.

Adicione também um arquivo de nome **link.txt**, na pasta raiz, contendo a URL do trabalho online (para a pasta raiz do trabalho).

Sobre Eventuais Plágios

Este é um trabalho individual. Os alunos envolvidos em qualquer tipo de plágio, total ou parcial, seja entre equipes ou de trabalhos de semestres anteriores ou de materiais disponíveis na Internet (exceto os materiais de aula disponibilizados pelo professor), serão duramente penalizados (art. 196 do Regimento Geral da UFU). Todos os alunos envolvidos terão seus **trabalhos anulados** e receberão **nota zero**.