Universidade Federal de Uberlândia
Faculdade de Computação - Prof. Daniel A. Furtado
11º Trabalho de Programação para Internet – Gestão da Informação
Desenvolvimento Web com BD, Prepared Statements e Transações

## Instruções Gerais

- Esta atividade deve ser realizada individualmente;
- Utilize apenas as tecnologias HTML5, CSS, JavaScript, Bootstrap 5, PHP e MySQL;
- Sintaxe da XHTML como <img/> ou <br/> 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 (**jamais utilize** dados pessoais como seu nome, CPF, endereço, e-mail etc.);
- Esteja atento às **observações sobre plágio** apresentadas no final desde 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 à 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.

https://furtado.prof.ufu.br/site/teaching/PPI/PPI-Modulo7-Banco-de-Dados.pdf

## Exercício 1

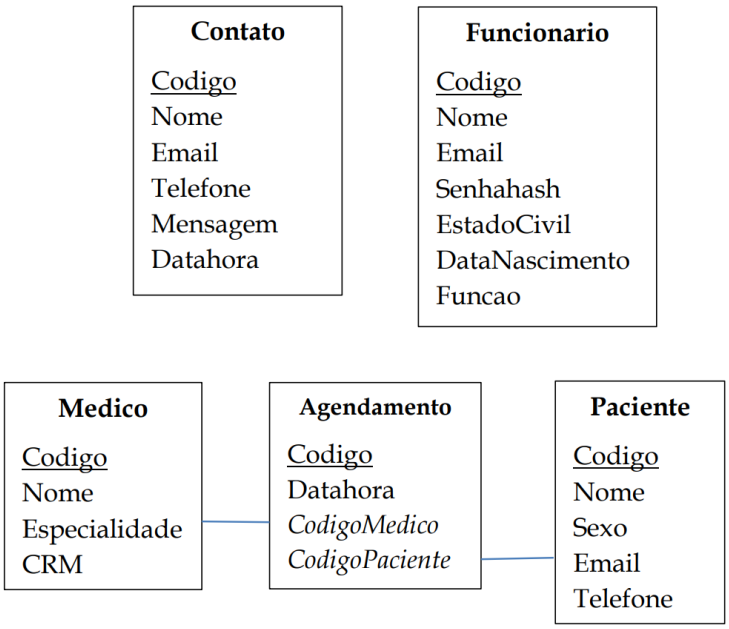
Faça uma cópia do **Trabalho10** / **Exercício 2** e altere o exemplo para que os dados do aluno sejam inseridos na tabela de forma segura utilizando **prepared statements**. Simule novamente o ataque de injeção de SQL e verifique o resultado.

## Exercício 2

Faça uma cópia do **Trabalho10** / **Exercício 3** e altere o exemplo para que os dados do funcionário sejam inseridos na tabela de forma segura utilizando **prepared statements**.

## Exercício 3

a) Crie um novo banco de dados no infinityfree para ser utilizado no projeto final da disciplina (clínica médica). Em seguida crie tabelas de acordo com o diagrama a seguir. Observe a necessidade de chaves primárias e estrangeiras.




b) Insira manualmente dois registros na tabela **Medico**;

c) Crie um formulário simplificado que permita o cadastro de um novo agendamento médico. O formulário deve ter um campo do tipo Data/Hora (datetime) para que o usuário informe a data/hora do agendamento, um campo para inserção do **código do médico** que prestará o atendimento e campos para inserção dos dados do paciente que terá a consulta agendada (Nome, Sexo, Email e Telefone). **OBS**: neste momento será necessário que o usuário informe o código do médico diretamente no formulário. Porém, isso será alterado posteriormente quando a técnica Ajax for abordada;

d) Crie um script PHP que receba o formulário anterior e faça a devida inserção dos dados nas tabelas **Agendamento** e **Paciente**. Utilize o conceito de *prepared statements* e transação. Como referência, utilize o exemplo **Ex4-transacao** disponibilizado em https://furtado.prof.ufu.br/site/teaching/PPI/Exemplos-Mysql.zip)

## Exercício 4

Crie um script PHP para listar os dados cadastrados no exercício anterior. O script deve produzir uma página HTML dinâmica contendo uma tabela conforme exemplo a seguir. Aspectos de segurança devem ser considerados para evitar ataques do tipo XSS. A consulta SQL deve fazer um inner JOIN envolvendo as tabelas **Medico**, **Agendamento** e **Paciente**.

| **DataHora do Agendamento** | **Nome Médico** | **Nome Paciente** | **Sexo Paciente** | **Email Paciente** | **Telefone Paciente** |
|---|---|---|---|---|---|
| ... | ... | ... | ... | ... | ... |
| ... | ... | ... | ... | ... | ... |

## 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**.