Universidade Federal de Uberlândia
Faculdade de Computação – Prof. Daniel A. Furtado
3º Trabalho de Desenvolvimento Web II
Aspectos de Segurança no Acesso à Banco de Dados 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
 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**.

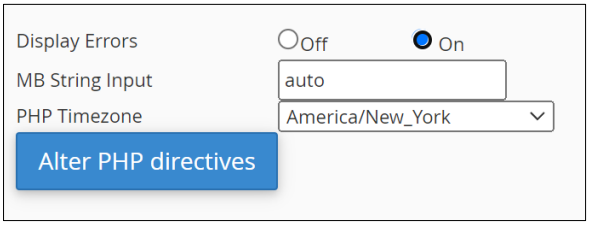
Material de Apoio e Dicas Gerais

https://furtado.prof.ufu.br/site/teaching/DW2/DW2-Modulo3-Aspectos-Seguranca-BD.pdf

Exercício 1

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

Accounts →if0_xxx → Control Painel → Software → Alter PHP Config → Alter PHP Directives → Display Errors → ON, como na figura a seguir:



1. Descompacte o arquivo https://furtado.prof.ufu.br/site/teaching/DW2/Exemplos-Trab3.zip e coloque os exemplos online seguindo os próximos passos;
2. Crie um banco de dados no **infinityfree** conforme instruções do final do material de aula;
3. Siga os passos do **slide 27** para executar o código SQL disponibilizado no arquivo **sql-tabelas.sql** (disponível na arquivo .zip);
4. Abra o arquivo **conexaoMysql.php** da pasta raiz e altere os dados de conexão inserindo os dados do seu banco de dados (veja figura do **slide 26**);
5. Copie a pasta raiz contendo todos os exemplos para o servidor. O exemplo deve ficar disponível no endereço **seudominio.com/trab3.** Neste trabalho não é necessário criar subpastas para cada exercício;
6. Digite **seudominio.com/trab3** no navegador para abrir a página contendo o menu de opções. Acesse o **Exemplo 1 – Mostrar Alunos** e verifique se os dados dos alunos inseridos no código SQL estão sendo listados adequadamente.

Exercício 2

1. Acesse o **Exemplo 1 – Cadastrar aluno** e cadastre dois novos alunos. Liste os dados;
2. O código PHP do exemplo está vulnerável a ataques do tipo **SQL Injection**. Simule um ataque cadastrando um novo aluno e inserindo a string a seguir no campo **telefone** do formulário:

   tolo'); DELETE FROM aluno; -- comment

3. Acrescente comentários no código PHP do arquivo **cadastro-vulneravel.php** explicando o motivo da vulnerabilidade. Não utilize explicitamente na explicação as palavras Injeção, Injection, Ataques, XSS etc.;
4. Coloque o código vulnerável dentro de um **comentário de bloco** e acrescente o código adequado utilizando **prepared statements** para corrigir a vulnerabilidade. Em seguida, cadastre novos alunos e repita o ataque de injeção para verificar se o problema foi resolvido.

Exercício 3

1. Acesse o **Exemplo 2 – Cadastro em duas tabelas** no navegador e observe o formulário HTML;
2. Abra novamente o arquivo **sql-tabelas.sql** e analise o código SQL que cria as tabelas correlacionadas **cliente** e **enderecoCliente**.
3. Abra o exemplo no **VS Code** e analise o código dos arquivos:
   a. index.html
   b. controlador.php
   c. cliente.php -> método Create
   d. cliente.php -> método GetFirst30
   e. clientes.html (analisar apenas superficialmente)
4. Complete o código PHP no método **Create** (do arquivo **cliente.php**) para que os dados dos parâmetros sejam inseridos adequadamente nas tabelas **cliente** e **enderecoCliente** do banco de dados. Utilize como base o exemplo de transação disponibilizado no slide 18.
5. Adicione comentários no código PHP do arquivo **controlador.php** explicando as operações.
6. Adicione comentários no código PHP do arquivo **cliente.php** explicando as operações.

Disponibilização Online

O trabalho deve entregue pelo sistema SAAT e disponibilizado online utilizando o subdomínio gratuito registrado em site de hospedagem. Como este trabalho consiste em modificações dos

arquivos de exemplo, não é necessário criar subpastas para cada exercício. Ao acessar o endereço a seguir, deverá abrir a página contendo o **menu de opções**:

seusubdominio.com/**trab3**

Entrega

Além da disponibilização online, a pasta raiz 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**.