Universidade Federal de Uberlândia
Faculdade de Computação – Prof. Daniel A. Furtado
8º Trabalho de Desenvolvimento Web II
Cookies, Sessões, Login e CSRF

Instruções Gerais

- Esta atividade deve ser realizada **individualmente**;
- Tecnologias permitidas: HTML5, CSS, JavaScript, PHP, MySQL;
- 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

https://furtado.prof.ufu.br/site/teaching/DW2/DW2-Modulo5-Cookies-Sessao-CSRF.pdf

Exercício 1

Leia os slides de aula do PDF acima e descompacte os exemplos do arquivo https://furtado.prof.ufu.br/site/teaching/DW2/Exemplos-Trab8.zip. Siga os passos a seguir:

1. Modifique o arquivo conexaoMysql.php dos exemplos **e1**, **e2** e **e3**, conforme o seu banco de dados MySQL no infinityfree;
2. Dentro de sua conta existente no infinityfree, crie uma nova **conta de hospedagem** (Hosting Accounts) com um novo subdomínio seguindo o formato site1xxxx.infinityfreeapp.com (substitua o xxxx por 4 letras de sua escolha);
3. Coloque os exemplos **e1**, **e2** e **e3** online utilizando essa nova conta. Utilize o script **sql-tabelas.sql** dentro de **e1** para criar a tabela **cliente** no banco de dados;
4. Copie para o servidor o arquivo **index.html** da raiz, contendo os links para abertura dos três exemplos;
5. Acesse o primeiro exemplo, **e1**, e cadastre 3 clientes;

6. Ainda no primeiro exemplo, faça login com uma das contas criadas e observe a listagem dos dados. Experimente excluir um dos clientes cadastrados;
7. Abra os arquivos do exemplo **e1** no VS Code e analise os códigos, especialmente em:
    a. Index.html
    b. login.php
    c. home.php
    d. exclui-cliente-get.php
    e. logout.php
8. Explique o funcionamento do mecanismo de login utilizando cookie de sessão. Inclua na explicação aspectos relacionados ao protocolo HTTP;
9. Explique o funcionamento da função **session_start** do PHP. Inclua na explicação aspectos relacionados ao protocolo HTTP;
10. Estando logado no exemplo e1, acesse o ambiente de desenvolvimento do navegador (F12) e exclua o cookie de sessão do PHP (F12 → Application → Storage (no painel esquerdo) → Cookies → PHPSESSID → Botão direito → Delete);
11. Recarregue a página **home.php** (F5) e observe o resultado;
12. Faça login novamente no exemplo **e1** e mantenha-se logado;
13. Crie mais uma conta de hospedagem no infinityfree com um novo subdomínio seguindo o formato site2xxxx.infinityfreeapp.com (substitua o xxxx por 4 letras de sua escolha);
14. Abra o arquivo **index.html** da pasta **site-2-atacante** e modifique o primeiro link **<a>** substituindo o domínio (conforme seu site1xxxx) e o **X** de i**d=X** para o id de um dos clientes que se encontra cadastrado no seu exemplo **e1**. Coloque os arquivos da pasta **site-2-atacante** online utilizando a conta recém-criada (site2xxxx.);
15. Mantenha-se logado no exercício **e1** do site1xxxx, abra uma nova aba no navegador e visite o site2xxxx;
16. Clique no primeiro link da página (Testar A T A Q - C S R F – Exclusão) e observe o resultado. Se os passos anteriores foram executados corretamente, esta ação deve excluir o respectivo cliente no site1xxxx. Responda as seguintes questões:
    a. Explique, em detalhes, porque exatamente a exclusão foi realizada, considerando que o link foi acessado a partir de outro site (site2, e não site1);
    b. Quais fatores contribuíram para o sucesso da ação?
    c. Caso, no site2xxx, houvesse uma imagem no formato <img src="https://site1xxxx.infinityfreeapp.com/e1/exclui-cliente-get.php?id=X"> (ao invés do link), a ação de exclusão teria sido executada? Por quê?
    d. Qual seria uma forma simples e rápida de corrigir o exemplo **e1** para evitar essa vulnerabilidade? Qual efeito colateral ela teria?
17. Abra os arquivos do exemplo **e2** no VS Code e analise os códigos, especialmente em:
    a. Index.html
    b. login.php
    c. home.php
    d. altera-senha-form.html
    e. altera-senha.php
18. Abra o arquivo **ataq-rf-altera-senha.html** da pasta **site-2-atacante** e atualize o atributo **action** do <**form**> para corresponder ao seu nome de domínio (site1xxxx). Envie o arquivo atualizado para o site2xxxx;
19. Mantenha-se logado no exercício **e2** do site1xxxx, abra uma nova aba no navegador e visite novamente o site2xxxx;

20. Clique no segundo link da página (Testar A T A Q - C S R F - Mudança de Senha) e observe o resultado. Se os passos anteriores foram executados corretamente, esta ação deve alterar a senha do usuário logado no site1xxxx para 123456. Responda as seguintes questões:
    a. Explique, em detalhes, porque exatamente a senha foi realizada, considerando que o link foi acessado a partir de outro site (site2, e não site1);
    b. Qual fator crítico permitiu o sucesso dessa ação?
    c. Essa ação teria tido sucesso se o login tivesse sido realizado da mesma forma que no exemplo **e1**? Por quê?
    d. Qual seria uma forma simples e rápida de corrigir o exemplo **e2** para evitar essa vulnerabilidade? Qual efeito colateral ela teria?
21. Abra os arquivos do exemplo **e3** no VS Code e analise os códigos, especialmente em:
    a. login.php
    b. altera-senha-form.html
    c. altera-senha.php
22. Explique o mecanismo de proteção contra ataques CSRF utilizando um token CSRF, conforme ilustrado no exemplo **e3**. Qual a vantagem desse método quando comparado ao uso de SameSite=Strict?

Entrega

As respostas das questões devem ser entregues (em arquivo zip) pelo Sistema Acadêmico de Aplicação de Testes (SAAT) até a data limite indicada pelo professor em sala de aula. Os arquivos dos exemplos devem ser disponibilizados online utilizando sua conta de hospedagem. O arquivo zip deve incluir um arquivo de nome **link.txt** contendo as URLs de acesso dos exemplos online.

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**.