Trabalho em Sala 12/07/2024

Ariane Paulina e Anthony Vitulo

Documento de Análise de Ameaças Usando o Modelo STRIDE

Aplicação: Sistema de Gerenciamento de Backups

Esta aplicação web permite aos usuários registrar-se, fazer login, autenticar-se, gerenciar backups e acessar um painel administrativo. Desenvolvida em PHP e MySQL, executada em servidor Apache configurado com HTTPS usando XAMPP.

1. Spoofing (Falsificação)

Ameaça: Usuários mal-intencionados podem falsificar identidades para acessar o sistema.

Componentes Afetados:

login.php

autenticacao.php

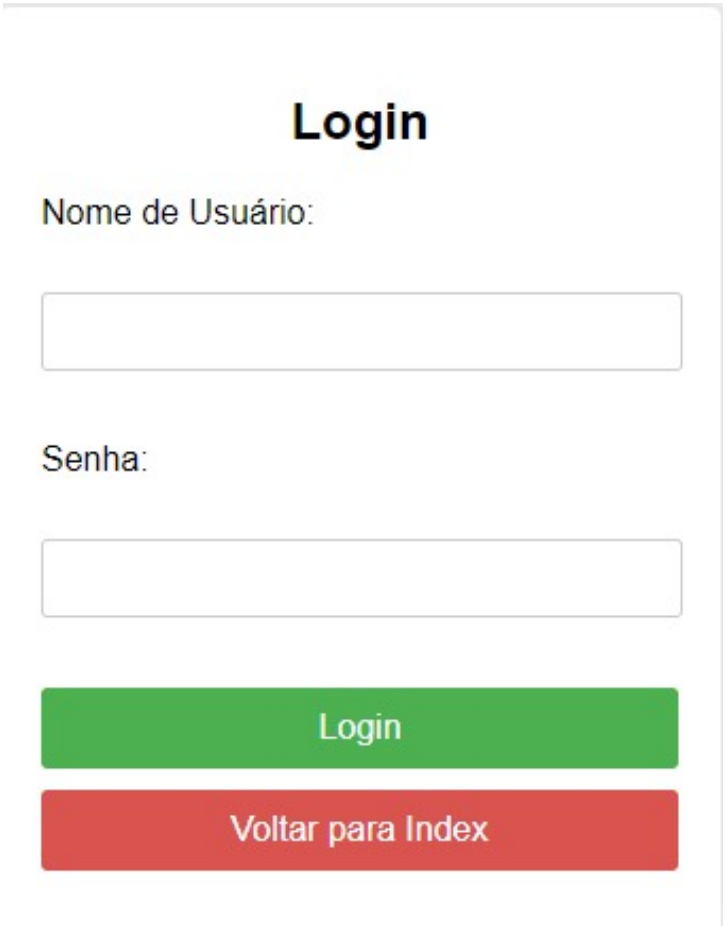
session.php

Medidas Necessárias:

Implementar Autenticação Multifator (MFA).

Usar Tokens de Sessão seguros com expiração.

Aplicar Hashing Seguro de Senhas (bcrypt).



2. Tampering (Adulteração)

Ameaça: Atacantes podem tentar modificar dados para comprometer a integridade.

Componentes Afetados:

register.php

login.php

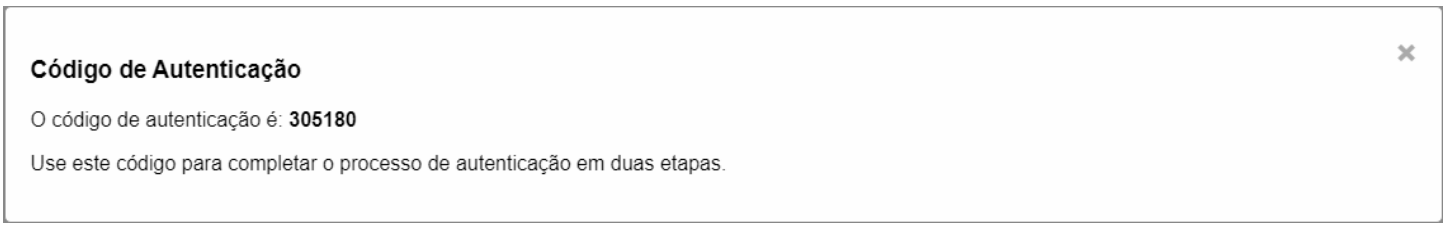
dashboard.php

criar_backup.php

Medidas Necessárias:

Validar e sanitizar todas as entradas de usuário.

Usar Prepared Statements para consultas seguras ao banco de dados.



3. Repudiation (Repúdio)

Ameaça: Usuários podem negar ações realizadas no sistema.

Componentes Afetados:

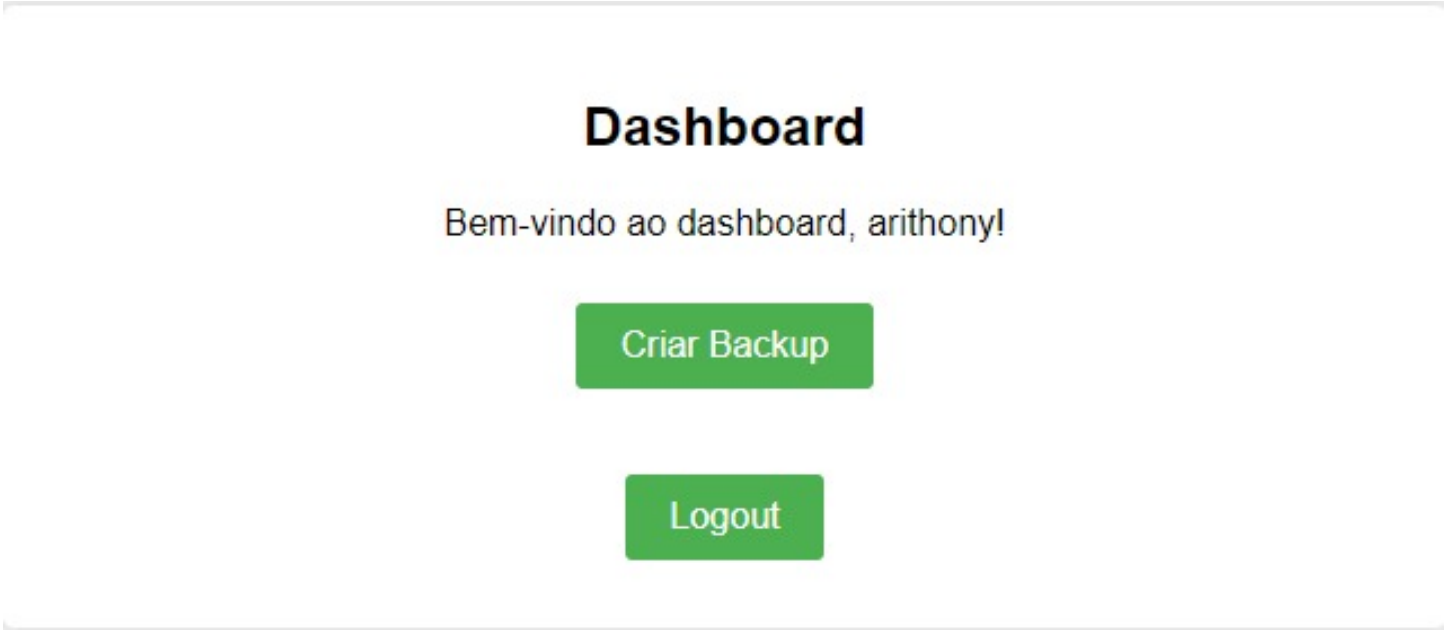
login.php

dashboard.php

Medidas Necessárias:

Manter Logs de Auditoria detalhados.

Utilizar Assinaturas Digitais para garantir a autenticidade dos registros.



4. Information Disclosure (Divulgação de Informações)

Ameaça: Dados sensíveis podem ser expostos.

Componentes Afetados:

db.php

login.php

dashboard.php

verificar_codigo.php

Medidas Necessárias:

Criptografar dados sensíveis em trânsito e em repouso.

Implementar Controles de Acesso rigorosos para proteger informações sensíveis.

5. Denial of Service (Negação de Serviço)

Ameaça: Ataques podem sobrecarregar o sistema, tornando-o inacessível.

Componentes Afetados:

Servidor Web (Apache)

Banco de Dados (MySQL)

Medidas Necessárias:

Implementar Limites de Taxa (Rate Limiting).

Configurar o Apache e MySQL para suportar grandes volumes de tráfego.

6. Elevation of Privilege (Elevação de Privilégio)

Ameaça: Usuários podem tentar obter privilégios não autorizados.

Componentes Afetados:

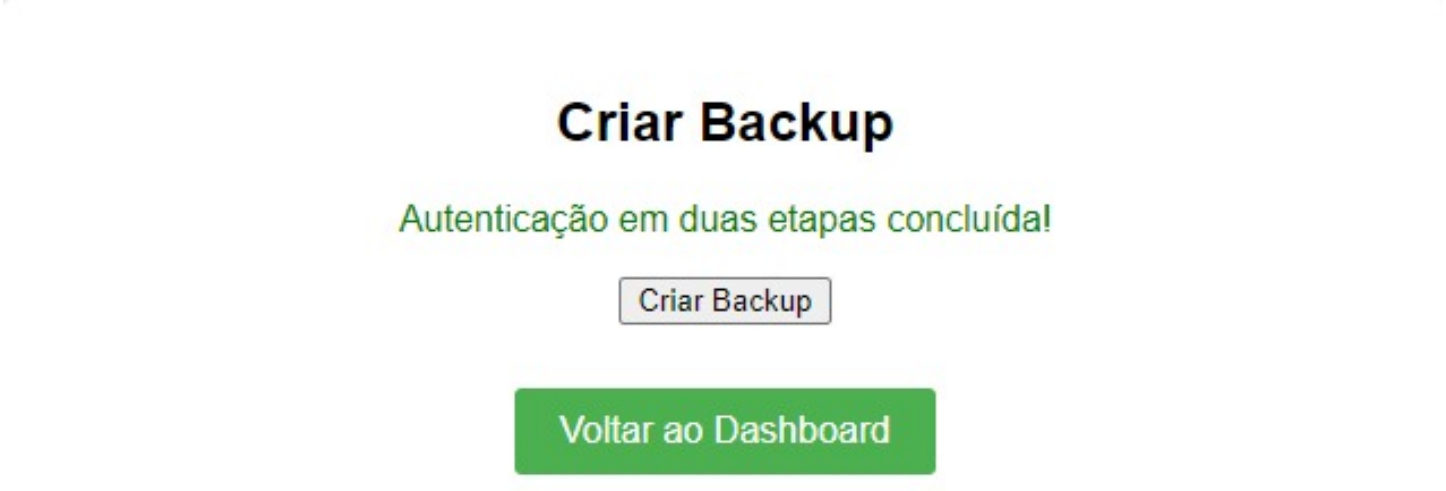
dashboard.php

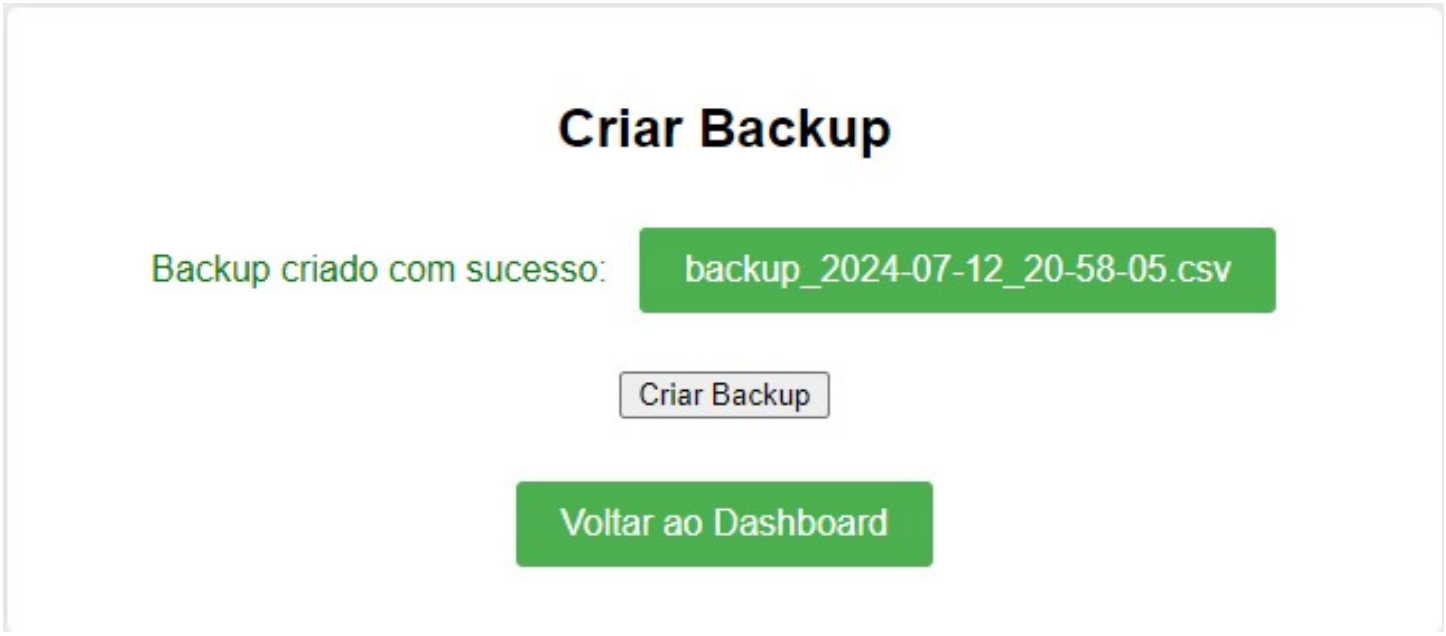
criar_backup.php

Medidas Necessárias:

Implementar Controle de Acesso Baseado em Funções (RBAC).

Aplicar o Princípio do Menor Privilégio para limitar acessos.





Conclusão

Implementar as medidas propostas para cada ameaça identificada utilizando o modelo STRIDE fortalecerá a segurança do sistema de gerenciamento de backups. Isso ajudará a proteger contra uma variedade de ataques potenciais, melhorando a segurança geral da aplicação.