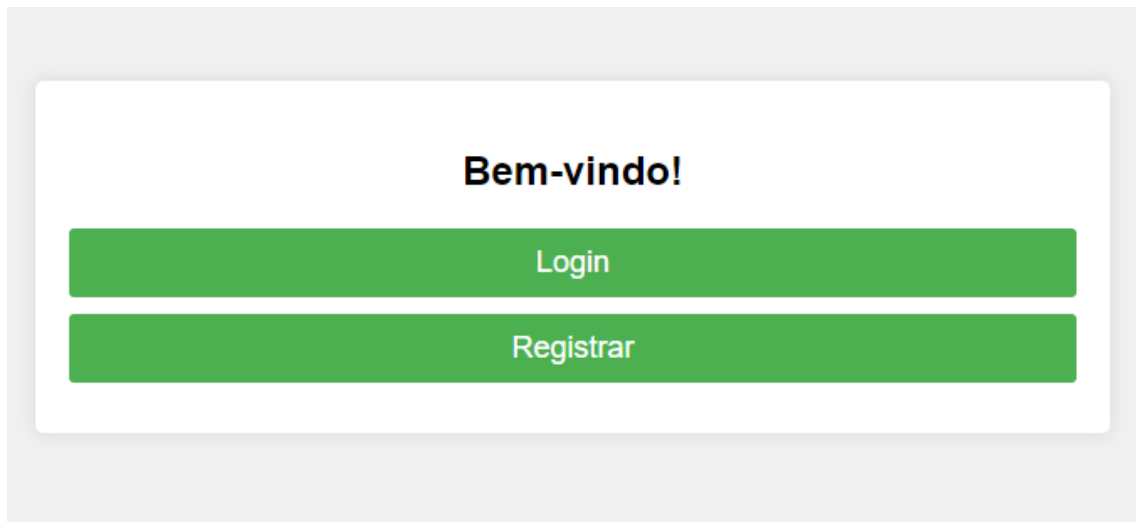


PAGINA INICIAL

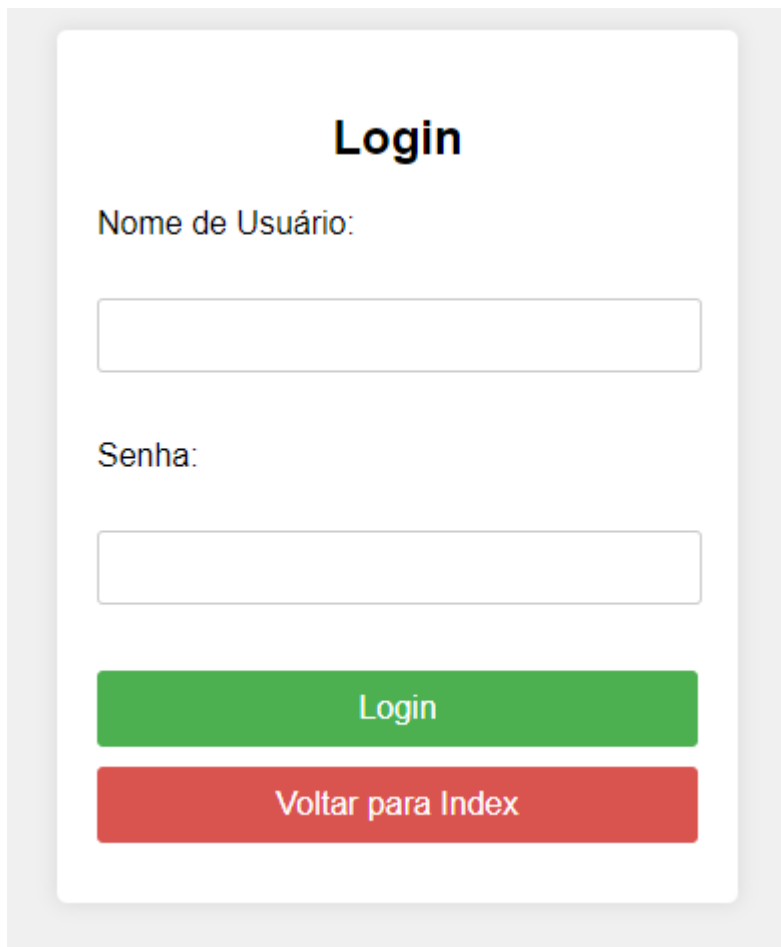
Pagina de login e registro.



The image shows a light gray rectangular area representing a page. Inside this area is a white rounded rectangle. At the top of the white rectangle, the text "Bem-vindo!" is centered in a bold black font. Below this text are two green rectangular buttons stacked vertically. The top button contains the text "Login" in white, and the bottom button contains the text "Registrar" in white.

TELA DE LOGIN

Possui nome de usuário e sua senha:



The image shows a light gray rectangular area representing a page. Inside this area is a white rounded rectangle. At the top of the white rectangle, the text "Login" is centered in a bold black font. Below this text, the label "Nome de Usuário:" is followed by a white rectangular input field with a thin gray border. Below the first input field, the label "Senha:" is followed by another white rectangular input field with a thin gray border. At the bottom of the white rectangle are two buttons stacked vertically. The top button is green with the text "Login" in white. The bottom button is red with the text "Voltar para Index" in white.

VERIFICAÇÃO DE DUAS ETAPAS (HABILIDATO)

Tela aonde pede para o usuário digitar o código de verificação.

Autenticação em Duas Etapas

Um código de autenticação foi enviado para você. Por favor, insira o código abaixo:

Código de Autenticação:

Verificar CódigoMostrar Código de Autenticação

TELA DE DASHBOARD

Tela para criar um backup ou fazer logout.

Dashboard

Bem-vindo ao dashboard, prof!

Criar Backup

Logout

TELA DE BACKUP

Tela para criar backup ou voltar ao dashboard

Criar Backup

Criar Backup

Voltar ao Dashboard

TELA DE REGISTRO DO USUARIO

Tela que pede informações como email, nome de usuário, senha(forte) e se o usuário vai querer uma verificação de duas etapas.

Registro de Usuário

Nome de Usuário:

E-mail:

Senha:

Confirme a Senha:

☐

Habilitar Autenticação em Duas Etapas

Registrar

Voltar para Index

LINHAS DE CODIGO

Linhas do htaccess

```
# Ativar o X-Frame-Options para proteção contra clickjacking
Header always append X-Frame-Options SAMEORIGIN

# Impedir Clickjacking
Header set X-Frame-Options "DENY"

# Limitação de taxa de requisições (mod_evasive)
<IfModule mod_evasive20.c>
    DOSHashTableSize 3097
    DOSPageCount 2
    DOSSiteCount 50
    DOSPageInterval 1
    DOSSiteInterval 1
    DOSBlockingPeriod 10
    DOSEmailNotify admin@example.com
    DOSLogDir "/var/log/mod_evasive"
    DOSWhitelist 127.0.0.1
</IfModule>

# Bloqueio de IPs maliciosos
<RequireAll>
    Require all granted
    # Bloquear IPs específicos
    Require not ip 192.168.1.100
    Require not ip 10.0.0.0/8
</RequireAll>

# Configuração de cache e compactação
<IfModule mod_deflate.c>
    AddOutputFilterByType DEFLATE text/html text/plain text/xml
</IfModule>
```

LINHA DE CODIGO DO LOGIN DO USUARIO

```
$stmt = $mysqli->prepare("SELECT id, senha, autenticacao_habilitada FROM usuarios WHERE username=?");
$stmt->bind_param("s", $username);
$stmt->execute();
$result = $stmt->get_result();

if ($result->num_rows == 1) {
    $user = $result->fetch_assoc();

    if (password_verify($password, $user['senha'])) {
        $_SESSION['userid'] = $user['id'];
        $_SESSION['username'] = $username;
    }
}
```

LINHA DO CODIGO DE LOGOUT

```
<?php
session_start();
session_unset();
session_destroy();
header('Location: index.php');
exit();
?>
```

ANALISE BASEADA A METEDOLOGIA STRIDE

De acordo com a Metodologia STRIDE, duas vulnerabilidades principais foram identificadas no sistema analisado.

Falta de Criptografia em Alguns Campos do Banco de Dados (Threat: Information Disclosure):

Resumo da Vulnerabilidade: A ausência de criptografia em certos campos do banco de dados pode levar à exposição não autorizada de informações sensíveis.

Impacto: Caso um atacante obtenha acesso ao banco de dados, ele pode visualizar e utilizar informações confidenciais, comprometendo a integridade e privacidade dos dados.

Mitigação: Implementar criptografia robusta para todos os campos sensíveis no banco de dados, assegurando que mesmo em caso de acesso indevido, os dados permaneçam inacessíveis e protegidos.

Limitar o Número de Tentativas para Logar (Threat: Denial of Service):

Resumo da Vulnerabilidade: A ausência de restrição no número de tentativas de login pode facilitar ataques de força bruta, onde um atacante tenta várias combinações de senhas até conseguir acesso.

Impacto: Além do risco de comprometimento de contas de usuários, esse tipo de ataque pode levar a uma sobrecarga do sistema, causando indisponibilidade de serviços.

Mitigação: Implementar uma política de limitação de tentativas de login, como bloqueio temporário da conta após um número específico de tentativas falhas, uso de CAPTCHA após múltiplas tentativas, e monitoramento de atividades suspeitas de login.

Conclusão Geral: A aplicação da Metodologia STRIDE permitiu identificar e propor soluções para duas vulnerabilidades críticas no sistema. A adoção de criptografia para campos sensíveis e a implementação de limites de tentativas de login são medidas essenciais para aumentar a segurança e a resiliência do sistema contra ataques maliciosos.