

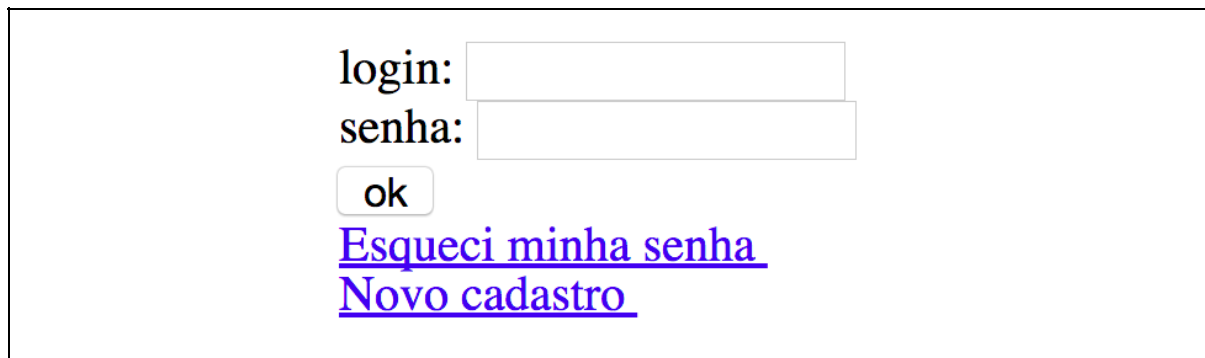
## Disciplina: Programação II

1º Semestre de 2015

## Gabarito

**Utilizando PHP e MySQL implemente o sistema descrito a seguir.**

Suponha um sistema web em PHP no qual uma página de login regula o acesso a informações pessoais.



login:

senha:

[Esqueci minha senha](#)

[Novo cadastro](#)

*Figura 1 - Página de Login*

**(2.0 pontos:)**

A página de login (ver Figura 1) apresenta um formulário para serem digitados o login do usuário e sua senha, um botão de enviar e ainda dois links para tratarem os casos "Esqueci minha senha" (a ser tratado pelo script 'recuperarSenha.php') e ainda o caso "Novo usuário" (a ser tratado pelo script 'cadastro.php').

Caso digite login e senha e selecione o botão 'Ok' você deve conferir os dados do usuário e enviá-lo para uma página produzida pelo script 'usuarioJaLogado.php' onde está escrito 'Bem vindo' seguido do nome do usuário, ou ainda 'Dados inválidos' caso não confirmem com os registrados no banco.

Atenção, sua solução deve prevenir-se de usuários mal intencionados que tentem burlar o login deste sistema digitando diretamente na barra de endereço do navegador a URL correspondente ao arquivo 'usuarioJaLogado.php'.

**(2.0 pontos:)**

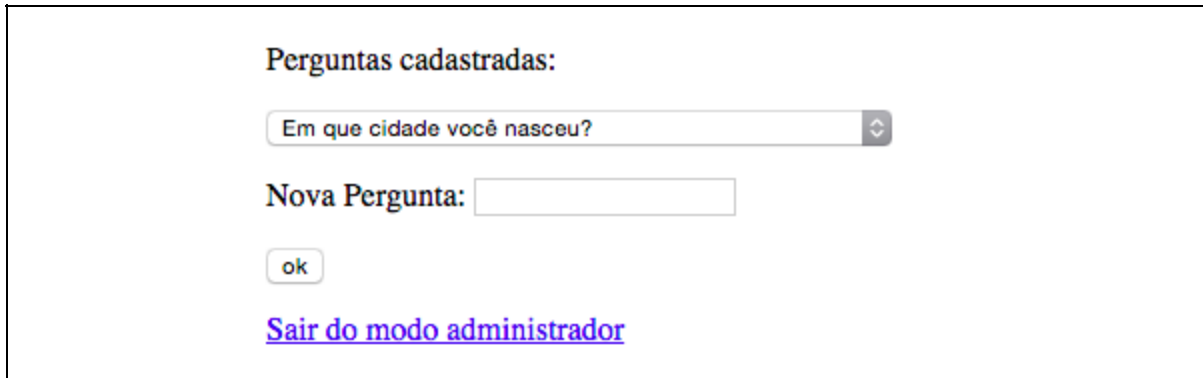
Este sistema armazena um banco de perguntas, para oferecer como mecanismo de recuperação de senha esquecida como por exemplo as perguntas:

- "Em que cidade você nasceu?";
- "Qual a sua cor preferida?";
- "Qual o nome do seu primeiro animal de estimação";
- entre outras;

Para isso, considere a possibilidade de um login especial utilizando o usuário

'admin' como um caso de tratamento especial, a ser direcionado para o script 'cadastroPerguntas.php'.

Uma vez logado, o administrador tem acesso ao cadastro de novas perguntas (Figura 2) onde pode rever as perguntas já cadastradas, e acrescentar uma nova pergunta ao banco de dados com até 128 caracteres. Deve ainda poder sair do sistema, ou seja, fazer *log out*.



Perguntas cadastradas:

Em que cidade você nasceu?

Nova Pergunta:

ok

[Sair do modo administrador](#)

*Figura 2 - Cadastro de perguntas*

### **(3 pontos:)**

Um usuário regular, ao se registrar pela primeira vez (a ser implementado pelo script 'cadastro.php'), deve escolher uma entre as perguntas previamente cadastradas pelo administrador do banco de dados, e digitar uma resposta não nula para a pergunta escolhida (string de até 128 caracteres).

Durante o cadastro deve também escolher um nome de login, uma senha e um email. Você deve registrar e conferir que:

- o nome não é nulo e possui mais de 3 caracteres;
- o login não foi previamente utilizado no banco de dados;
- a senha escolhida possui pelo menos 8 caracteres incluindo letras maiúsculas, minúsculas e números;
- o email fornecido é válido e também ainda não foi previamente cadastrado no sistema.

Para recuperar a senha escolha entre receber nova senha ou responder a pergunta secreta cadastrada.

email:

Pergunta secreta:

email ou login:

  
  
resposta:  

*Figura 3 - Página para recuperar senha*

**(3 pontos:)**

Caso o usuário esteja na página de login e tenha esquecido a senha e siga para o arquivo 'recuperarSenha.php', deve visualizar uma página oferecendo um campo para digitar o email previamente cadastrado para resgate de uma nova senha ou ainda responder uma pergunta secreta (veja figura 3).

Caso o usuário escolha digitar o email, implemente um script no arquivo 'recuperarSenha.php', que verifica se o email está de fato cadastrado no banco e gere uma senha aleatória de 8 dígitos (números e letras) e envie para o email correspondente.

Caso escolha a pergunta secreta, recupere do banco de dados a pergunta escolhida para o login do usuário, e confira se a resposta está correta.

## **GABARITO:**

### **Arquivo index.php:**

```
<html>
<head>
<title>Sistema de Login</title>
<?php
session_start();
session_destroy();
?>
</head>
<body>
    <h1>Sistema de Login</h1>
    <form action="./usuarioJaLogado.php" method="get">
        <label for="login">Login:</label>
        <input type="text" name="login" />
        <br />
        <label for="senha">Senha:</label>
        <input type="password" name="senha" />
        <br />
        <input type="submit" value="ok" />
    </form>
    <a href="./recuperarSenha.php">Esqueci minha senha</a>
    <br />
    <a href="./cadastro.php">Novo Cadastro</a>
</body>
</html>
```

### Arquivo usuarioJaLogado.php:

```
<html>
<head>
<title>Sistema de Login</title>
<?php
session_start();
require_once 'util.php';

if (verificaGetValido('login')
    && verificaGetValido('senha')) {

    $login = $_GET['login'];
    $senha = $_GET['senha'];

    $_SESSION['usuarioLogado'] = autenticaUsuario($login, $senha);

    if(verificaSessionTrue('usuarioLogado')) {
        $_SESSION['admin'] = usuarioAdmin($login);
        $nomeUsuario = carregaNomeUsuario($login);
    }
} else {
    $_SESSION['usuarioLogado'] = false;
}
?>
</head>
<body>
    <h1>
    <?php if (verificaSessionTrue('usuarioLogado')) {
        echo "Bem vindo, $nomeUsuario.";
    } else {
        echo "Dados inválidos!";
    }
    ?>
    </h1>
    <a href="./index.php">Voltar</a>
</body>
</html>
```

## Arquivo cadastra.php

```
<html>
<head>
<title>Sistema de Login</title>
<?php
session_start();
require_once 'util.php';

$cadastro = false;
$submit = false;

if (isset($_GET) && !empty($_GET)) {
    $submit = true;

    $nome = $_GET['nome'];
    $email = $_GET['email'];
    $login = $_GET['login'];
    $senha = $_GET['senha'];
    $pergunta = $_GET['pergunta'];
    $resposta = $_GET['resposta'];

    $cadastro = validaCadastro($nome, $email, $login, $senha, $pergunta, $resposta)
        && cadastra($nome, $email, $login, $senha, $pergunta,
$resposta);

    unset($_GET);
}

if (!$cadastro) $perguntas = recuperaPerguntas();
?>
</head>
<body>
<?php if ($submit && $cadastro) {?>
    <h1>Cadastro efetuado com sucesso.</h1>
    <a href="./index.php">Voltar</a> para tela inicial.
<?php } else { ?>
    <?php if ($submit) { ?>
    <span>Erro ao efetuar cadastro</span>
    <?php } ?>
    <h1>Cadastro</h1>
    <form action="./cadastro.php" method="get">
        <label for="nome">Nome:</label><input type="text" name="nome" /><br />
        <label for="email">Email:</label><input type="text" name="email" /><br />
        <label for="login">Login:</label><input type="text" name="login" /><br />
        <label for="senha">Senha:</label><input type="password" name="senha"
/><br />
```

```
<label for="pergunta">Pergunta:</label>
<select name="pergunta">
  <?php foreach($perguntas as $key => $value) { ?>
    <option value="<?php echo $key;?>"><?php echo
$value;?></option>
  <?php } ?>
</select>
<br />
<label for="resposta">Resposta:</label>
<input type="text" name="resposta" /><br />
<input type="submit" value="ok" />
</form>
<?php } ?>
</body>
</html>
```

### Arquivo cadastraPerguntas.php

```
<html>
<head>
<title>Sistema de Login</title>
<?php
session_start();
require_once 'util.php';

$cadastro = false;
$submit = false;

if (isset($_GET) && !empty($_GET)) {
    $submit = true;

    $pergunta = $_GET['nova'];

    $cadastro = cadastraPergunta($pergunta);
    unset($_GET);
}

$perguntas = recuperaPerguntas();
?>
</head>
<body>
<?php if ($submit && $cadastro) {?>
    <span>Pergunta cadastrada com sucesso.</span>
<?php } else if ($submit) { ?>
    <span>Erro ao cadastrar pergunta.</span>
<?php } ?>

<?php if (verificaSessionTrue('usuarioLogado') && verificaSessionTrue('admin')) { ?>
    <h1>Cadastro</h1>
    <label for="pergunta">Perguntas cadastradas:</label><br />
    <select name="pergunta">
        <?php foreach($perguntas as $key => $value) { ?>
            <option value="<?php echo $key;?>"><?php echo $value;?></option>
        <?php } ?>
    </select>
    <br />

    <form action="./cadastroPerguntas.php" method="get">
        <label for="nova">Nova pergunta:</label><input type="text" name="nova"
/><br />
        <input type="submit" value="ok" />
    </form>
```



```
        <a href="./index.php">Sair do modo administrador</a>
<?php } else { ?>
    <h1>Erro</h1>
    <a href="./index.php">Voltar</a> ao login.
<?php } ?>
</body>
</html>
```

### Arquivo recuperarSenha.php

```
<html>
<head>
<title>Sistema de Login</title>
<?php
session_start();
require_once 'util.php';

$submit = false;
$envioEmail = false;
$envioResposta = false;

if (verificaGetValido("email")) {
    $email = $_GET("email");

    if (verificaEmailExistente($email)) {
        enviaSenhaEmail($email);
        $envioEmail = true;
    }
    $submit = true;
} else if (verificaGetValido("emailLogin")) {
    $id = $_GET("emailLogin");
    $pergunta = $_GET("pergunta");
    $resposta = $_GET("resposta");

    if (verificaEmailExistente($id)
        && validaPerguntaRespostaSecretaEmail($id, $pergunta,
$resposta)) {

        $senha = recuperaSenhaEmail($id);
        $envioResposta = true;
    } else if (verificaLoginExistente($id)
        && validaPerguntaRespostaSecretaLogin($id, $pergunta,
$resposta)) {

        $senha = recuperaSenhaLogin($id);
        $envioResposta = true;
    } else {
        $envioResposta = false;
    }
    $submit = true;
}

$perguntas = recuperaPerguntas();
?>
</head>
```

```

<body>
<?php if ($submit && $envioEmail) { ?>
    <h1>Email enviado com sucesso.</h1>
<?php } else if ($submit && $envioResposta) { ?>
    <h1>Sua senha: <?php echo $senha; ?>.</h1>
<?php } else if ($submit) { ?>
    <h1>Erro ao recuperar senha.</h1>
    <a href="./recuperarSenha.php">Voltar</a>
<?php } else { ?>
    <h1>Para recuperar a senha, escolha entre receber nova
    senha ou responder a pergunta secreta cadastrada</h1>

    <form action="./recuperarSenha.php" method="get">
        <label for="email">email:</label>
        <br />
        <input type="text" name="email" />
        <br />
        <input type="submit" value="enviar nova senha" />
    </form>

    <h2>Pergunta secreta:</h2>

    <form action="./recuperarSenha.php" method="get">
        <label for="emailLogin">email ou login:</label>
        <br />
        <input type="text" name="emailLogin" />
        <br />
        <select name="pergunta">
            <?php foreach($perguntas as $key => $value) { ?>
                <option value="<?php echo $key;?>"><?php echo
$value;?></option>
            <?php } ?>
        </select>
        <label for="resposta">resposta:</label>
        <br />
        <input type="text" name="resposta" />
        <br />
        <input type="submit" value="ok" />
    </form>

    <a href="./index.php">Voltar</a>
<?php } ?>
</body>
</html>

```

## Arquivo util.php

```
<?php
function validaCadastro($nome, $email, $login, $senha, $pergunta, $resposta) {
    if ($nome == null || strlen($nome) < 3) {
        return false;
    }

    if (verificaLoginExistente($login)) {
        return false;
    }

    if (!preg_match("/[a-z]/", $senha)
        || !preg_match("/[A-Z]/", $senha)
        || !preg_match("/[0-9]/", $senha)) {

        return false;
    }

    if (verificaEmailExistente($email)) {
        return false;
    }

    return true;
}

function enviaSenhaEmail($email) {
    mail($email,"Recuperar senha",geraSenha());
}

function geraSenha($tamanho = 10) {
    $letras =
'0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
    $tamLetras = strlen($letras);
    $senha = "";
    for ($i = 0; $i < $tamanho; $i++) {
        $senha .= $letras[rand(0, $tamLetras-1)];
    }
    return $senha;
}

function validaPerguntaRespostaSecretoLogin($login, $pergunta, $resposta) {
    $sql = "SELECT login FROM usuario WHERE login = '$login' AND pergunta =
'$pergunta' AND resposta = '$resposta'";

    return consultaSingular($sql);
}
```

```

function validaPerguntaRespostaSecretaEmail($email, $pergunta, $resposta) {
    $sql = "SELECT email FROM usuario WHERE email = '$email' AND pergunta =
'pergunta' AND resposta = '$resposta'";

    return consultaSingular($sql);
}

function recuperaSenhaLogin($login) {
    return "senha";
}

function recuperaSenhaEmail($email) {
    return "email";
}

function verificaSessionTrue($nome) {
    return isset($_SESSION) && isset($_SESSION[$nome]) && $_SESSION[$nome]
== true;
}

function verificaGetValido($nome) {
    return isset($_GET) && isset($_GET[$nome]) && $_GET[$nome] != "";
}

function verificaLoginExistente($login) {
    $sql = "SELECT login FROM usuario WHERE login = '$login'";

    return consultaSingular($sql);
}

function verificaEmailExistente($email) {
    $sql = "SELECT email FROM usuario WHERE email = '$email'";

    return consultaSingular($sql);
}

function autenticaUsuario($login, $senha) {
    $sql = "SELECT login FROM usuario WHERE login = '$login' AND senha =
'$senha'";

    return consultaSingular($sql);
}

function usuarioAdmin($login) {
    $sql = "SELECT login FROM usuario WHERE login = '$login' AND level = 'admin'";

```

```

        return consultaSingular($sql);
    }

function carregaNomeUsuario($login) {
    $conecta = mysql_connect("localhost", "admin", "admin");
    mysql_select_db("login", $conecta) or print(mysql_error());

    $sql = "SELECT nome FROM usuario WHERE login = '$login'";
    $result = mysql_query($sql, $conecta);

    $resposta = "";
    if ($consulta = mysql_fetch_array($result)) {
        $resposta = $consulta['nome'];
    }

    mysql_free_result($result);

    mysql_close($conecta);

    return $resposta;
}

function cadastra($nome, $email, $login, $senha, $pergunta, $resposta) {
    $sql = "INSERT INTO usuario VALUES (DEFAULT, '$nome', '$email', '$login',
'$senha', '$pergunta', '$resposta')";

    return consultaSingular($sql);
}

function recuperaPerguntas() {
    $conecta = mysql_connect("localhost", "admin", "admin");
    mysql_select_db("login", $conecta) or print(mysql_error());

    $sql = "SELECT id, pergunta FROM pergunta";
    $result = mysql_query($sql, $conecta);

    $resposta = array();
    if ($consulta = mysql_fetch_array($result)) {
        $resposta[$consulta['id']] = $consulta['pergunta'];
    }

    mysql_free_result($result);

    mysql_close($conecta);
}

```

```

        return $resposta;
    }

function cadastraPergunta($pergunta) {
    $sql = "INSERT INTO pergunta VALUES (DEFAULT, '$pergunta')";

    return consultaSingular($sql);
}

function consultaSingular($sql) {
    $conecta = mysql_connect("localhost", "admin", "admin");
    mysql_select_db("login", $conecta) or print(mysql_error());

    $result = mysql_query($sql, $conecta);

    $resposta = false;
    if ($consulta = mysql_fetch_array($result)) {
        $resposta = true;
    }

    mysql_free_result($result);

    mysql_close($conecta);

    return $resposta;
}
?>

```