

Universidade dos Açores
Ano letivo 2018/2019

Plataforma Web para uma empresa de turismo:
Paradise Guide



Paulo Cunha (20170017) e Júlio Furtado (20170007)
Desenvolvimento de Aplicações Web

Descrição geral do projeto

No âmbito da unidade curricular de Segurança Web, foi proposto o desenvolvimento de uma plataforma web para uma empresa de turismo, que tem como objetivo reservar atividades como whale watching, trilhos, entre outras. Neste projeto, foi-nos pedida a implementação de várias funcionalidades, de modo a proteger a plataforma contra diversos tipos de ataques e falhas, entre os quais, como exemplos:

- Cross-site Scripting (XSS);
- SQL Injection;
- Não implementação de protocolos;
- Haver a necessidade de encriptar e desencriptar os dados.

As funcionalidades que nos foram pedidas e conseguimos com sucesso implementar na plataforma foram as seguintes:

FRONT END

1. O cliente pode visualizar uma lista de todas as atividades;
2. Pesquisar atividades pelo nome e localização geográfica (tanto havendo sessão iniciada como não estando);
3. Reservar atividades: A reserva é feita mediante disponibilização dos dados de cartão de crédito, guardados de forma encriptada;
4. O cliente pode ver a sua lista de atividades reservadas;
5. Inserir comentários às atividades já realizadas.

BACK END

1. O admin (no nosso caso, dois) pode listar as suas atividades;
2. O vendedor pode filtrar as suas atividades pelo nome;
3. Também é possível criar, atualizar (editar) e eliminar atividades.
4. Visualizar uma lista de reservas de atividades efetuadas por cada cliente.
5. Marcar reservas como realizadas adiadas ou canceladas.

Pode anunciar-se desde já que cada medida de prevenção tomada e demonstrada em seguida foi tomada ao longo de toda a aplicação e não só nos exemplos

demonstrados. Sendo este facto passível de ser confirmado observando o código do projeto. Muitas mais medidas foram tomadas e serão com certeza mencionadas aquando da apresentação e visualização geral do próprio projeto.

O cliente

Utilizadores não registados e registados conseguem, tal como já referido, pesquisar atividades por:

- Localização geográfica;
- Tipo de atividade.

Obviamente apenas utilizadores com conta registada conseguem reservar as atividades. Além disso, conseguem ver os comentários das mesmas e também efetuá-los. Um utilizador registado consegue reservar atividades, tendo como meio de pagamento o cartão de crédito. Ao reservar uma atividade, é obrigatório o preenchimento de um formulário com alguns dados pessoais (o próprio número de cartão de crédito, a data de expiração deste e o nome tal como presente no cartão).


No registo do cliente existe formulário com os seguintes campos:

TORNA-SE JÁ NUM NOVO MEMBRO

Nome de utilizador




Endereço de email



Palavra-passe



Confirmação da palavra-passe



REGISTAR-SE!

Medidas de prevenção tomadas:

- Cross-site scripting;
- Encriptação de dados;
- Prepared statements de modo a evitar SQL injection

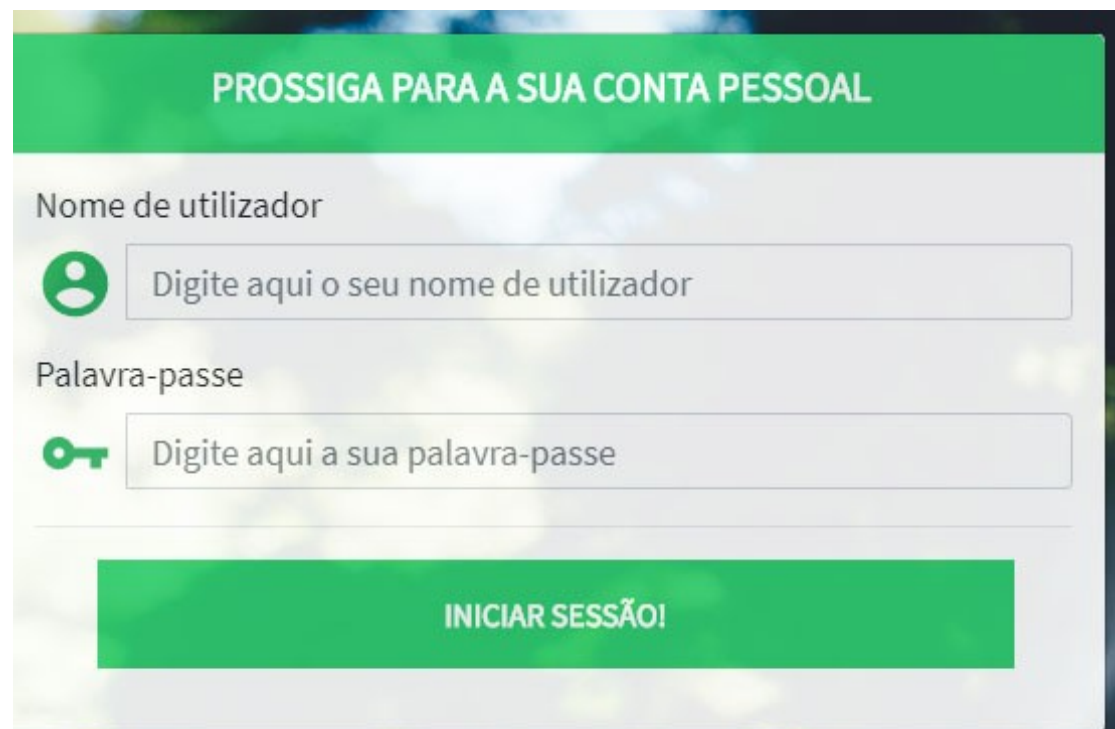
```
# Proteção contra XSS (Cross-Site Scripting)
$username = htmlspecialchars($username, ENT_QUOTES, 'UTF-8');
$email = htmlspecialchars($email, ENT_QUOTES, 'UTF-8');
$password = htmlspecialchars($password, ENT_QUOTES, 'UTF-8');
$password_rewrite = htmlspecialchars($password_rewrite, ENT_QUOTES, 'UTF-8');

# Encriptação da palavra-passe
$password_hash = password_hash($password, PASSWORD_BCRYPT, array("cost" => 12));
```

```
# Inserir campos na base de dados
$sql = "INSERT INTO users(username, email, password) ";
$sql .= "VALUES(:username, :email, :password)";
$stmt = $pdo->prepare($sql);

# Executar o statement
$stmt->execute([":username" => $username, ":email" => $email,
":password" => $password_hash]);
```

Login de cliente



The image shows a login form with a green header bar containing the text "PROSSIGA PARA A SUA CONTA PESSOAL". Below the header, there are two input fields. The first is labeled "Nome de utilizador" and has a green user icon to its left; the input text is "Digite aqui o seu nome de utilizador". The second is labeled "Palavra-passe" and has a green key icon to its left; the input text is "Digite aqui a sua palavra-passe". At the bottom of the form is a large green button with the text "INICIAR SESSÃO!" in white capital letters.

As medidas utilizadas foram:

- Proteção contra Cross-site scripting (XSS);
- Proteção contra SQL Injection;
- Descriptação

```
# Verificação do formulário de login
if(isset($_POST["login_submit"])) {

    # Aceder aos campos do formulário
    $username = $_POST["username"];
    $password_attempt = $_POST["password"];

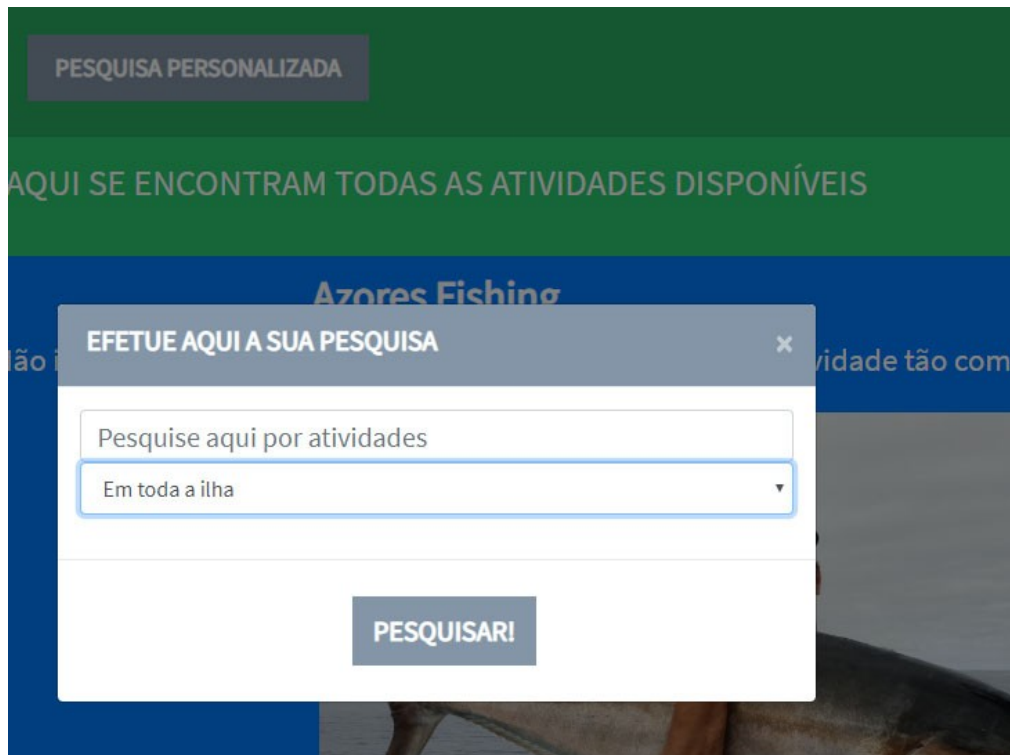
    # Verificar que os campos não se encontram vazios
    if (!empty($username) && !empty($password_attempt)) {

        # Eliminar os espaços dos campos de username e password
        $username = trim($username);
        $password_attempt = trim($password_attempt);

        # Proteção contra XSS (Cross-Site Scripting)
        $username = htmlspecialchars($username, ENT_QUOTES, 'UTF-8');
        $password_attempt = htmlspecialchars($password_attempt, ENT_QUOTES, 'UTF-8');

        // Descriptar a palavra-passe
        # Query que retorna os dados do utilizador pretendido
        $check_user_sql = "SELECT idUser, username, password FROM users ";
        $check_user_sql .= "WHERE username = :username";
        $check_user_stmt = $pdo->prepare($check_user_sql);
        $check_user_stmt->execute([":username" => $username]);
```

Cada cliente pode pesquisar atividades utilizando a “pesquisa avançada”:



A pesquisa pode ser por localização geográfica, ou seja, por concelho da ilha:

```
# Query de pesquisa
$filtero_sql = "SELECT * FROM atividades WHERE nomeAtividade LIKE :nomeAtividade";

# Definir o prepared statement
$filtero_stmt = $pdo->prepare($filtero_sql);

# Executar o prepared statement
$filtero_stmt->execute(["nomeAtividade" => "%" . $termoPesquisa . "%"]);
} else {

# Query de pesquisa
$filtero_sql = "SELECT * FROM atividades WHERE nomeAtividade LIKE :nomeAtividade ";
$filtero_sql .= "AND zonaAtividade LIKE :zonaAtividade";

# Definir o prepared statement
$filtero_stmt = $pdo->prepare($filtero_sql);

# Executar o prepared statement
$filtero_stmt->execute(["nomeAtividade" => "%" . $termoPesquisa . "%", "zonaAtividade" => $zonaAtividade]);
}
```


O utilizador ao iniciar sessão, consegue visualizar a lista de atividades turísticas, conseguindo ver a descrição da mesma, preços. Pode efetuar comentários (exemplo de um destes abaixo) e também ver as suas reservas já feitas.

Miradouro do Pico do Ferro

Explore 7 Cidades e Vista do Rei, os mais famosos mirantes de Sete Cidades, Portugal. Passe meio dia admirando a cratera, a costa sul da ilha e os famosos lagos azul e verde.

Zona: Sete Cidades

Duração média: Aprox 4h

Preço: 25€



Comentários à atividade

Título do comentário: Fantástico

Comentário: A atividade foi simplesmente incrível!

Autor: Paulo

Para comentar uma atividade, o utilizador teve a necessidade de reservar previamente a atividade.


Logo abaixo da listagem de atividades, os utilizadores podem reservar as mesmas, preenchendo o seguinte formulário representado na imagem abaixo:

Atividades de pesca do mais alto nível na ilha de São Miguel. Não irá querer perder este evento se possuir gosto por esta atividade tão comum na ilha.

Zona: Vila Franca do Campo

Duração média: 02:00h

Preço: Desde 30€



Deseja reservar esta atividade? Proceda ao preenchimento do formulário abaixo!

Número do cartão de crédito

Data de expiração

Nome presente no cartão

RESERVAR ATIVIDADE!

Nesta zona, há que ter em conta a inserção do cartão de crédito e, sendo este um dado sensível, devemos ter em atenção a segurança deste formulário.

Ao encriptar um dado tão sensível, é necessário efetuar uma encriptação “ultra-segura”, apesar de dúvidas quanto à inserção deste dado na base de dados (exclarecidas atempadamente).

```
# Obter o número do cartão de crédito
$cartaoCredito = $_POST["credit_card"];
$idAtividade = $_POST["idAtividade"];

if (!empty($cartaoCredito)) {


    /* Eliminar todo o "whitespace" em branco do campo que contém o número
    de cartão de crédito */
    $cartaoCredito = trim(preg_replace("/\s+/", "", $cartaoCredito));

    # Proteção contra XSS (Cross-Site Scripting)
    $cartaoCredito = htmlspecialchars($cartaoCredito, ENT_QUOTES, 'UTF-8');

    # Encriptação do cartão de crédito
    $bytes = openssl_random_pseudo_bytes(8, $strong);
    $key = bin2hex($bytes);
    $plaintext = $cartaoCredito;
    $cipher = "aes-128-gcm";

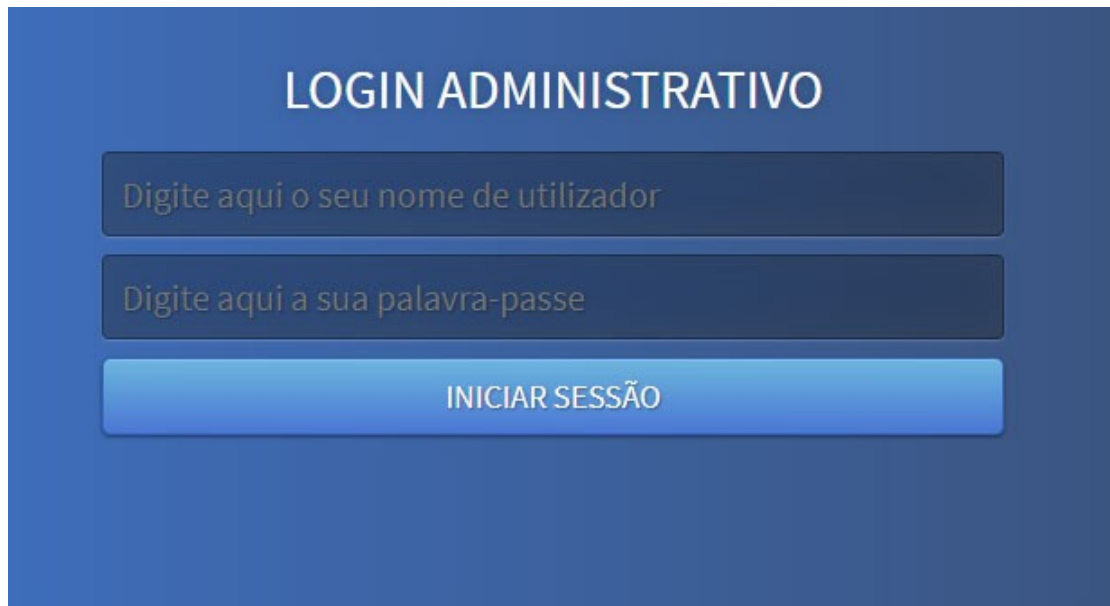
    if (in_array($cipher, openssl_get_cipher_methods())) {
        $ivlen = openssl_cipher_iv_length($cipher);
        $iv = openssl_random_pseudo_bytes($ivlen);
        $cipherCartaoCredito = openssl_encrypt($plaintext, $cipher, $key, $options=0, $iv, $tag);
    }
}
```

Os utilizadores registados, estando com sessão iniciada, conseguem ver todas as suas reservas, deste modo, conseguindo ver o estado da mesma: Podendo estar marcada, adiada. Pode até mesmo cancelar a reserva.

NOME DA ATIVIDADE	DESCRIÇÃO DA ATIVIDADE	ZONA	DURAÇÃO MÉDIA	IMAGEM	PREÇO	ESTADO	DESMARCAR ATIVIDADE
EXCURSÃO DE DIA INTEIRO ENTRE BALEIAS E VULCÕES	MERGULHE NA BELEZA NATURAL DE AÇORES NESTA EXCURSÃO DE DIA INTEIRO COM UMA EXCURSÃO PARA OBSERVAR BALEIAS E VULCÕES. OBSERVE VÁRIAS ESPÉCIES DE BALEIAS EM SEU HABITAT NATURAL E PROCURE POR GOLFINHOS SALTANDO NA ÁGUA. VIAJE DE BARCO PELO LITORAL RUMO A LAGOA DO FOGO E CALDEIRA VELHA, DESFRUTANDO DE UM DELICIOSO ALMOÇO AO LONGO DO CAMINHO. VISITE UM VULCÃO ATIVO E APRENDA COMO OS CIENTISTAS ESTÃO UTILIZANDO SUA ENERGIA PARA PRODUZIR ELETRICIDADE. NÃO PERCA ESTA OPORTUNIDADE DE CONHECER A VERDADEIRA BELEZA DE AÇORES, SUA AVENTURA NA VISTA DE BALEIAS E VULCÕES DE AÇORES COMEÇA AO ENCONTRAR O SIMPÁTICO GUIA LOCAL. DEPOIS DE OUVIR BREVES INSTRUÇÕES, PARTA RUMO A AÇORES PELO LITORAL ATÉ A MARINA DE PONTA DELGADA. AO LONGO DO CAMINHO, PROCURE POR UMA GRANDE VARIEDADE DE VIDA SELVAGEM, INCLUINDO BALEIAS-CACHALOTES, BALEIAS-AZUIS, BALEIAS-JUBARTES, BALEIAS-FRANCAS-PIGMEIAS, BALEIAS-BICUDAS, GOLFINHOS, TARTARUGAS, PEIXES-VOADORES E AVES OCEÂNICAS.	MARINA DE PONTA DELGADA	DIA INTEIRO		100€	MARCADA	<input type="button" value="CANCELAR"/>

O administrador

A zona administrativa também possui um login, para vendedores.

A screenshot of a web form titled "LOGIN ADMINISTRATIVO" on a blue background. The form contains two input fields: the first is labeled "Digite aqui o seu nome de utilizador" and the second is labeled "Digite aqui a sua palavra-passe". Below these fields is a large blue button with the text "INICIAR SESSÃO" in white capital letters.

Protegemos o mesmo contra Cross-site scripting (XSS) e SQL Injection:

```
# Proteção contra XSS (Cross-Site Scripting)
$usernameAdmin = htmlspecialchars($usernameAdmin, ENT_QUOTES, 'UTF-8');
$passwordAdmin = htmlspecialchars($passwordAdmin, ENT_QUOTES, 'UTF-8');

# Query que retorna os dados do utilizador pretendido
$check_user_sql = "SELECT COUNT(idAdmin) FROM admin_users WHERE ";
$check_user_sql .= "usernameAdmin = :usernameAdmin ";
$check_user_sql .= "AND passwordAdmin = :passwordAdmin";

# Preparar e executar a query
$check_admin_stmt = $pdo->prepare($check_user_sql);
$check_admin_stmt->execute(["usernameAdmin" => $usernameAdmin,
":passwordAdmin" => $passwordAdmin]);

# Fetch efetuado para mais tarde verificar se o username existe na base de dados
$count = $check_admin_stmt->fetchColumn();
```

Dentro da área de gestão, o vendedor consegue primeiramente ver todas as atividades que estão inseridas por si no sistema. Posto isto, o admin consegue inserir novas atividades na plataforma, editar as mesmas, visualizar as atividades reservadas pelos seus clientes e também alterar o estado destas reservas, cancelando as mesmas, marcando-as como realizadas ou adiá-las. Os vendedores também possuem uma “search bar”, para filtrarem as suas atividades por nome, tal como pedido no enunciado:



Como está descrito acima, os vendedores podem eliminar atividades e editar as mesmas, sendo isto demonstrado pelo “screenshot” seguinte:

Miradouro do Pico do Ferro



Explore 7 Cidades e Vista do Rei, os mais famosos mirantes de Sete Cidades, Portugal. Passe meio dia admirando a cratera, a costa sul da ilha e os famosos lagos azul e verde.

Zona: Sete Cidades

Duração média: Aprox 4h

Preço: 25€

[EDITAR ESTA ATIVIDADE](#)

[ELIMINAR ATIVIDADE](#)

Clicar no botão de eliminar, executa a “query de delete”, e elimina a atividade da base de dados.

O vendedor também pode editar as suas atividades, tanto através da área própria como de um “shortcut” existente após filtragem. Página de edição individual, sendo que uma de grupo também é existente, na aba própria:

Insira aqui um novo título para a atividade

Miradouro do Pico do Ferro

Substituir imagem de destaque



Escolher ficheiro Nenhum ficheiro selecionado

Insira aqui uma nova descrição para a atividade

Explore 7 Cidades e Vista do Rei, os mais famosos mirantes de Sete Cidades, Portugal. Passe meio dia admirando a cratera, a costa sul da ilha e os famosos lagos azul e verde.

Modifique a zona da atividade:

Sete Cidades

Modifique a duração da atividade:

Aprox 4h

Modifique o preço da atividade:

25

CONCLUIR EDIÇÃO DA ATIVIDADE


Cada vendedor pode, como já foi referido, inserir novas atividades através do preenchimento do formulário respetivo:

ÁREA DE CRIAÇÃO DE ATIVIDADES

Nome da atividade



Descrição da atividade




Descreva aqui de forma concisa e explicativa de que se trata a atividade em questão

Zona da atividade




Ex: Sete Cidades

Duração média



Ex: Aprox 2h

Preço base da atividade



Ex: Desde 30€

Upload da imagem de destaque da atividade

Escolher ficheiro

Nenhum ficheiro selecionado

INSERIR NOVA ATIVIDADE

PÁGINA 14

Mais sobre a segurança

Uma das medidas a ter atenção no “back-end”, é fazer com que users “mal-intencionadas” não tentem aceder às páginas utilizando endereços de URL, isto é, entrar nas páginas sem conta de cliente ou vendedor/gestor, portanto adicionamos restrições de página que verificam se existe alguma sessão iniciada. Ao verificar que não existem sessões ligadas, redireciona automaticamente o user para a página de index. Se existirem sessões iniciadas, não é permitido que um utilizador consulte páginas que não lhe são destinadas (um cliente na área administrativa, por exemplo) e estes utilizadores são reencaminhados para as suas páginas respetivas. “Screenshot” elucidativo encontra-se abaixo:

```
<!-- Iniciar a sessão -->
<?php session_start(); ?>
You, a few seconds ago • Uncommitted changes
<?php

/* Um cliente não poderá ter acesso à área administrativa (é redirecionado para a
área de cliente) */
if (isset($_SESSION["client"])) {header("Location:../area_cliente.php");}

/* Um administrador com sessão iniciada é reencaminhado para a área de gestão */
if (isset($_SESSION["admin"])) {header("Location:area_gestao.php");}

?>
```


Conclusão

Com o projeto elaborado tomamos sem dúvida conta das medidas de segurança que necessitamos tomar ao construir uma aplicação web. Uma “skill” essencial para o curso que frequentamos e para qualquer trabalho que podemos vir a desempenhar.

Temas como a “sanitization”, a encriptação de dados, a proteção contra SQL Injection ou Sross-site scripting são sem dúvida importantes para o nosso melhor entendimento de como a segurança pode influenciar o mundo digital e real em que vivemos.

Tiramos um enorme proveito ao realizar o trabalho e consideramos a cadeira na sua globalidade útil para uma melhor prevenção e medidas de segurança a executar na construção dos nossos projetos futuros, bem como ver os erros que podemos ter cometido em projetos passados.

Dados de acesso

Lado do cliente:

Username: paulo

Palavra-passe: 12345678

Username: henrique

Palavra-passe: 12345678

Username: julio

Palavra-passe: 12345678

Lado administrativo:

Username: vendedor1

Palavra-passe: admin123

Username: vendedor2

Palavra-passe: admin123