# **Laboratório 2: Conhecendo o ambiente JUICE SHOP**

## Objetivo

* Navegar pela aplicação seguindo o fluxo normal de uso, sem explorar vulnerabilidades.
* Conhecer as funcionalidades básicas do OWASP Juice Shop: cadastro, login, navegação, compra, e logout.
* Familiarizar-se com o funcionamento esperado da aplicação para subsidiar futuras análises de segurança.
* Estimular a observação crítica dos aspectos funcionais e potenciais fragilidades do sistema.

***Obs: ao longo da navegação anote informações sobre possíveis vulnerabilidades básicas de segurança já identificadas durante a “jornada feliz”.***

## Acesso à Aplicação

* Abra o navegador e acesse a página inicial do Juice Shop (http://localhost:3000).
* Observar a tela inicial com os produtos listados.

**Questões:**

* O site solicita autenticação logo na tela inicial? Por quê?

Não, pois não precisa estar logado para olhar os produtos da loja.

* Quais elementos no layout indicam que este é um site de e-commerce?

Produtos, preços, página do carrinho.

* A comunicação indica ser criptografada? Justifique.

Não está em https

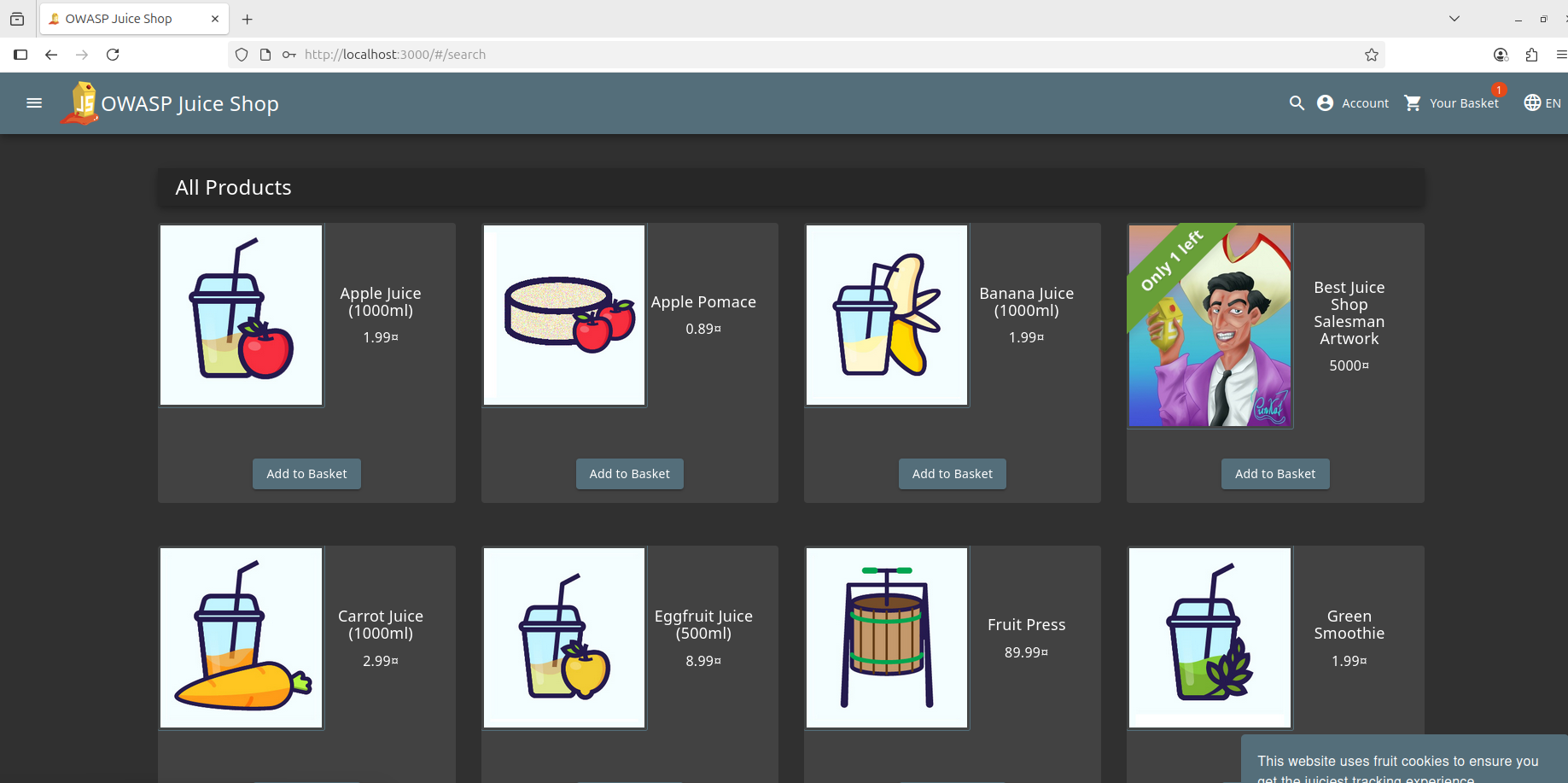
* Que mecanismos de autenticação estão disponíveis? Você identificou se há autenticação multifator?

Cadastro por email e senha, e não há autenticação multifator

* A aplicação protege adequadamente as credenciais do usuário em trânsito e em armazenamento?

Não, pois o email aparece para todos os usuários quando é feita uma review de um produto.

**→ Tarefa:** Faça uma captura de tela da página inicial visitada.



## Explorando Produtos

* Navegue entre as páginas de produtos.
* Use a barra de busca para localizar produtos específicos.
* Visualize detalhes e avaliações clicando no ícone de “olho” ao lado do preço.

**Questões:**

* Quais as categorias disponíveis? Existem filtros além da busca por texto?

Não há filtros. As categorias são sucos, artes, vestimentas, colecionáveis.

* Os preços, imagens e descrições são exibidos corretamente em todas as páginas?

Sim

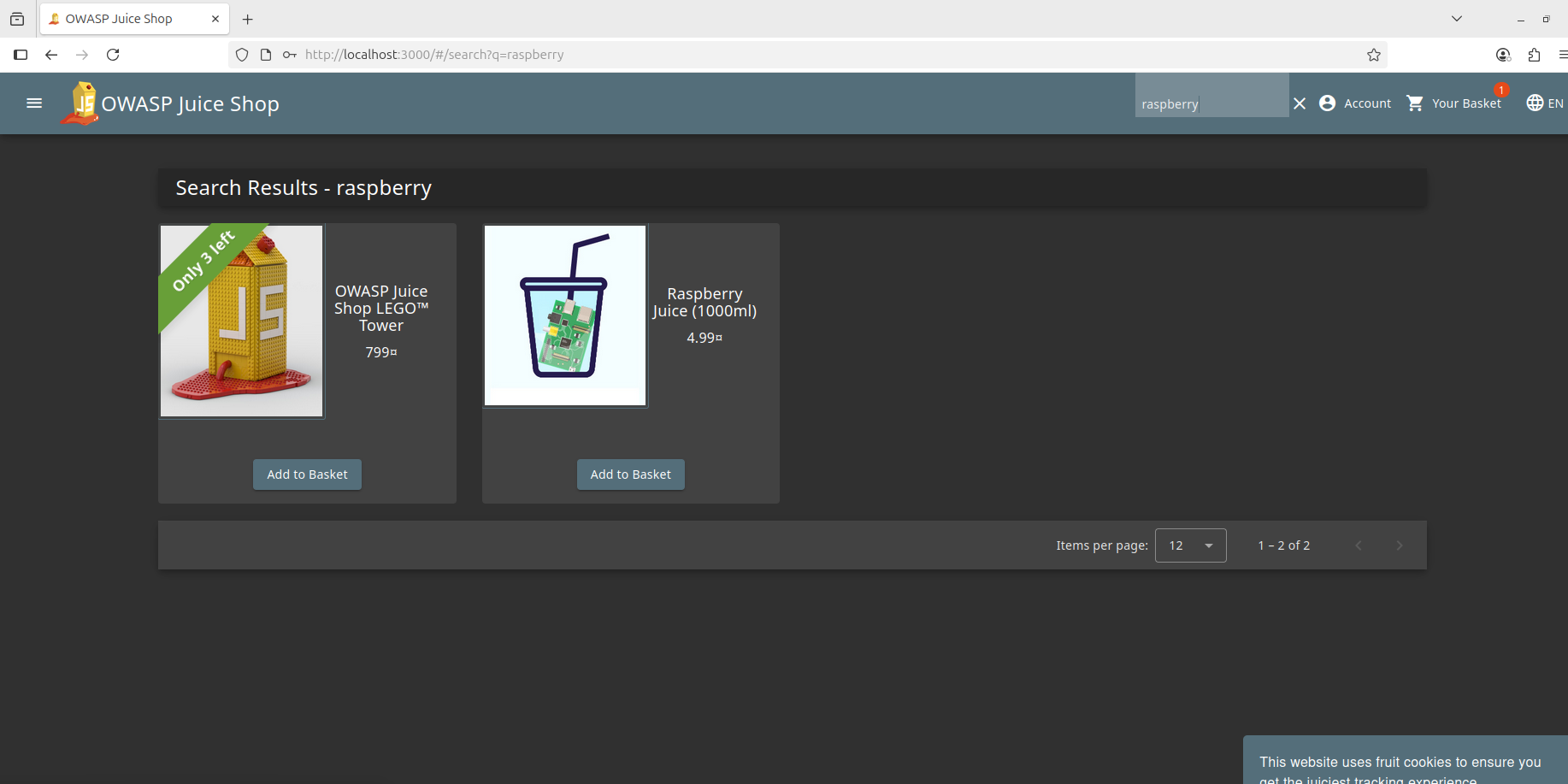
* Os dados exibidos (descrição, preços, avaliações) parecem estar protegidos contra exposição indevida para usuários não autenticados?

Não, pois é possível ver os produtos sem realizar o login

* Você percebeu indícios de controle de acesso baseado em função para limitar o que cada usuário pode ver?

Apenas usuários autenticados podem acessar a página de pagamentos

**→ Tarefa:** Insira uma captura de tela navegando pelos produtos e usando a barra de busca.



## Cadastro de Usuário

* Clique em “Login” e depois em “Não tem uma conta? Registre-se agora.”
* Preencha o formulário de registro **com dados fictícios**.
* Realize o login com a conta criada.

**Questões:**

* Quais campos o sistema exige para cadastro? Algum é opcional?

Email, senha e repetir a senha, pergunta e resposta de segurança. Todos são obrigatórios

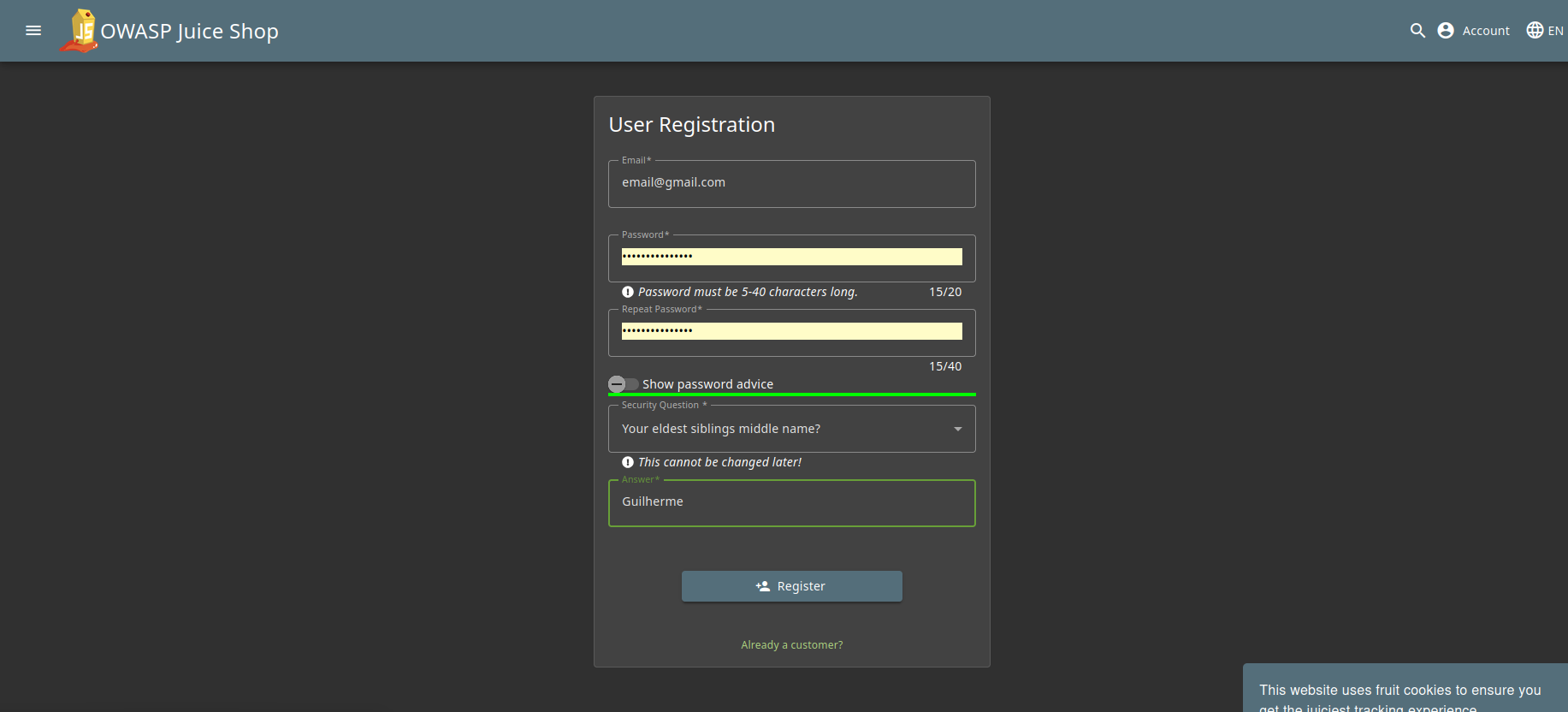
* O site permite cadastro com e-mail repetido? Como ele reage?

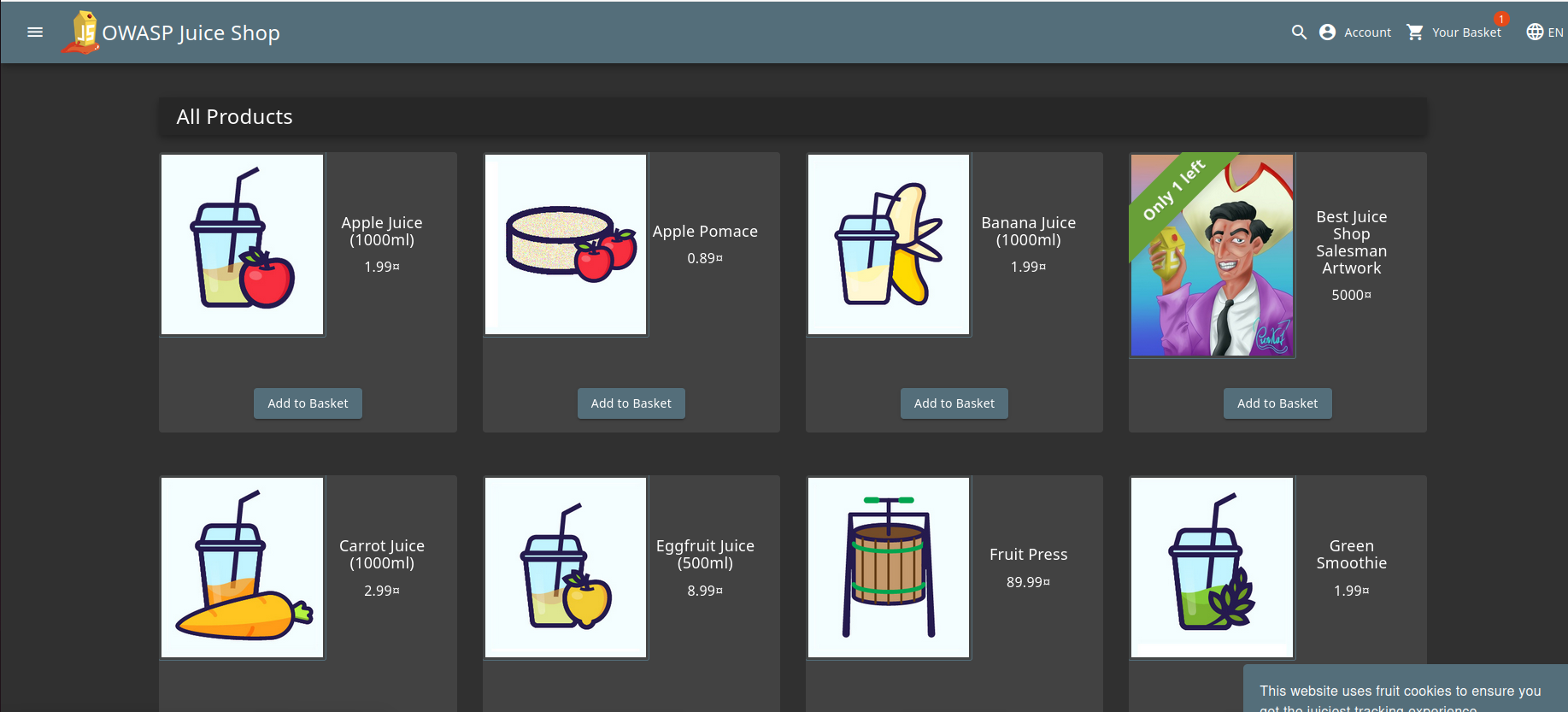
Não, ele exige validação de email e mostra um erro

* Há política de requisitos para a senha (tamanho, complexidade)? Ela é suficiente para proteção? (Faça uma breve pesquisa)

Sim, é necessário ter entre 5 e 40 caracteres. É recomendável pelo menos 1 letra minúscula, 1 maiúscula, 1 número e 1 caractere especial.

**→ Tarefa:** Adicione uma captura: tela de cadastro preenchida e, em seguida, uma com o login realizado.





## Adicionando Produtos ao Carrinho

* Adicione um ou mais produtos ao carrinho através do ícone.
* Acesse o carrinho pelo menu superior e confira os itens.

**Questões:**

* O que acontece visualmente ao adicionar um produto?

O ícone carrinho aparece a quantidade de produtos

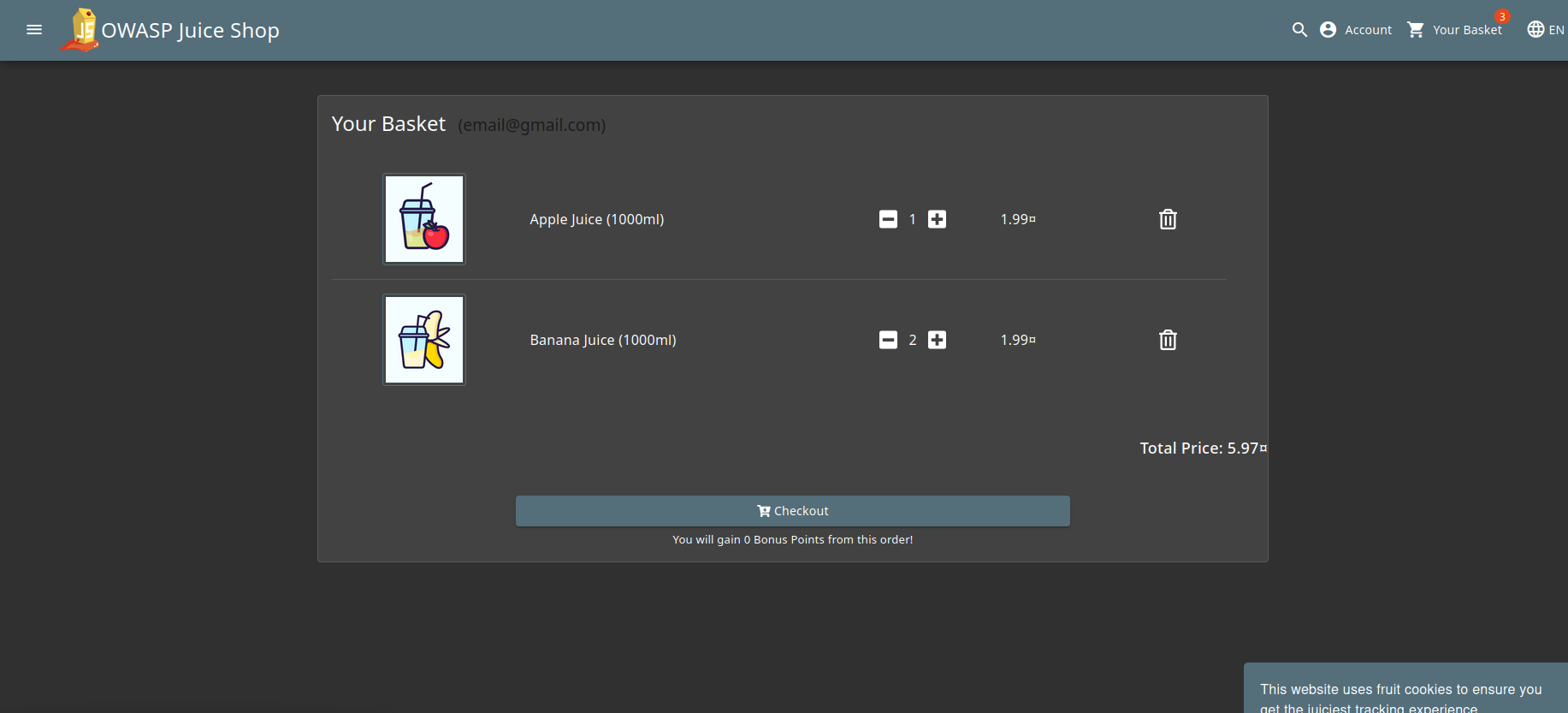
* É possível adicionar múltiplas unidades do mesmo produto? Como é exibida a quantidade?

Sim, aparece ao lado do produto com botões para adicionar e remover

* Existe alguma confirmação após a adição?

Não

**→ Tarefa:** Anexe uma captura mostrando o carrinho com produtos adicionados.



## Finalizando a Compra (Checkout)

* Clique em “Checkout” no carrinho.
* Preencha informações fictícias de endereço, método de envio e pagamento.
* Finalize o pedido.

**Questões:**

* Quais dados são solicitados para endereço e pagamento? Há validação?

Endereço, telefone, cep. Não há validação

* O sistema aceita qualquer cartão fictício? O que acontece se campos obrigatórios estiverem vazios?

Sim, apenas exige que o número do cartão tenha 16 números

* Após o pedido, o resumo mostra informações completas?

Sim

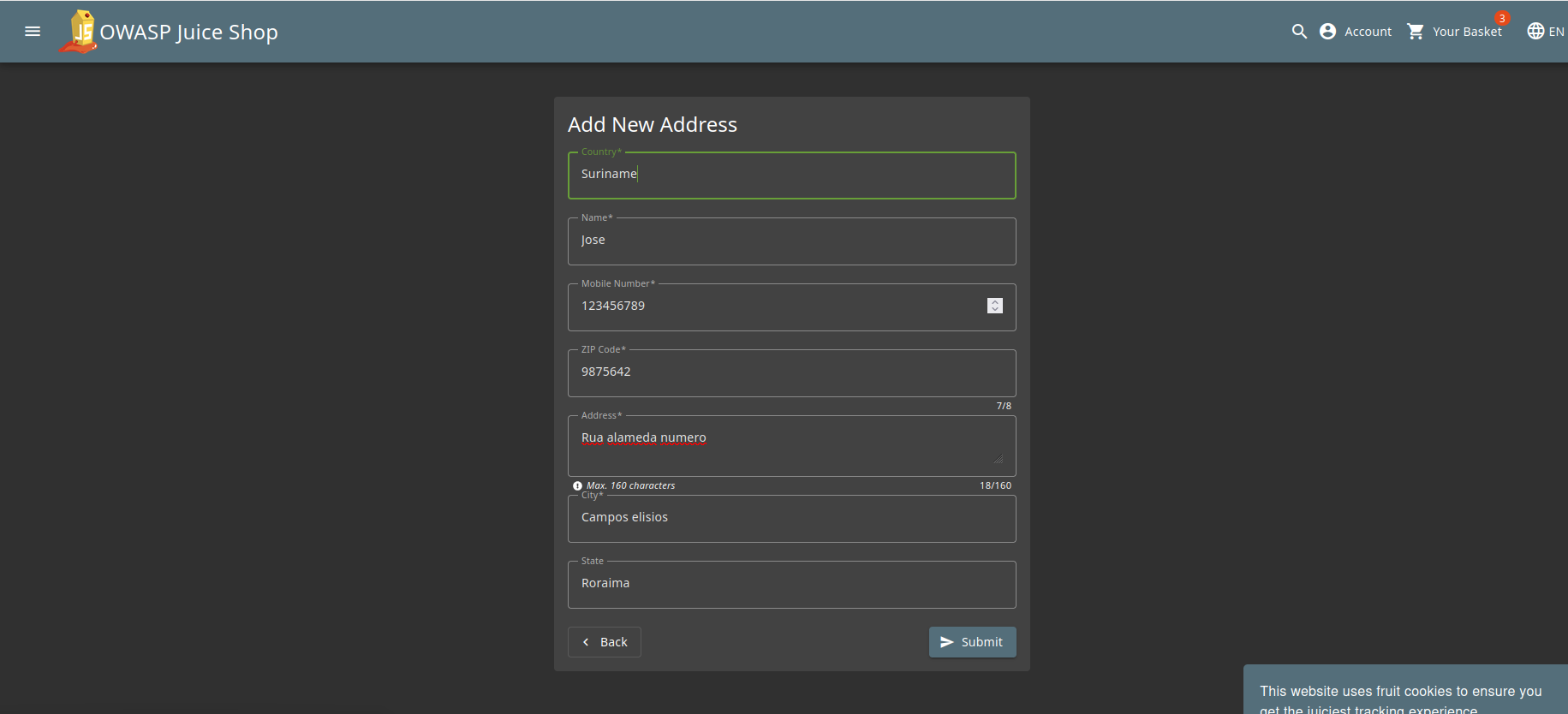
* O sistema valida as informações de pagamento antes de aceitar? Há algum tipo de criptografia das informações transmitidas?

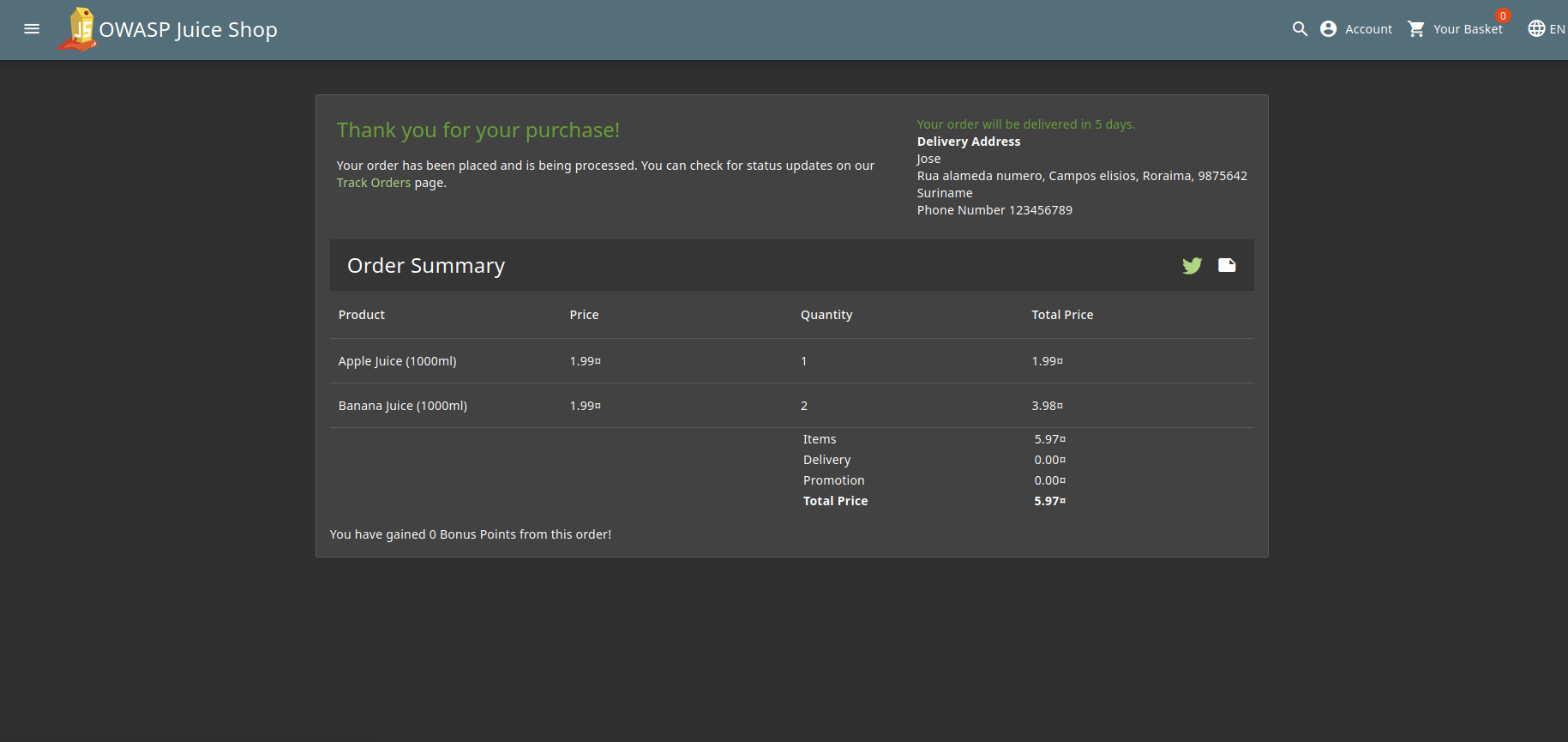
Não

* Que controles poderiam ser adotados para evitar fraudes durante o checkout?

Validações de cartão e endereço

**→ Tarefa:** Inclua uma captura da tela de checkout preenchida e uma do resumo da compra/pedido finalizado.





## Acompanhando o Pedido

* Visualize a página de confirmação com resumo do pedido.
* Explore opções para salvar ou imprimir o comprovante.

**Questões:**

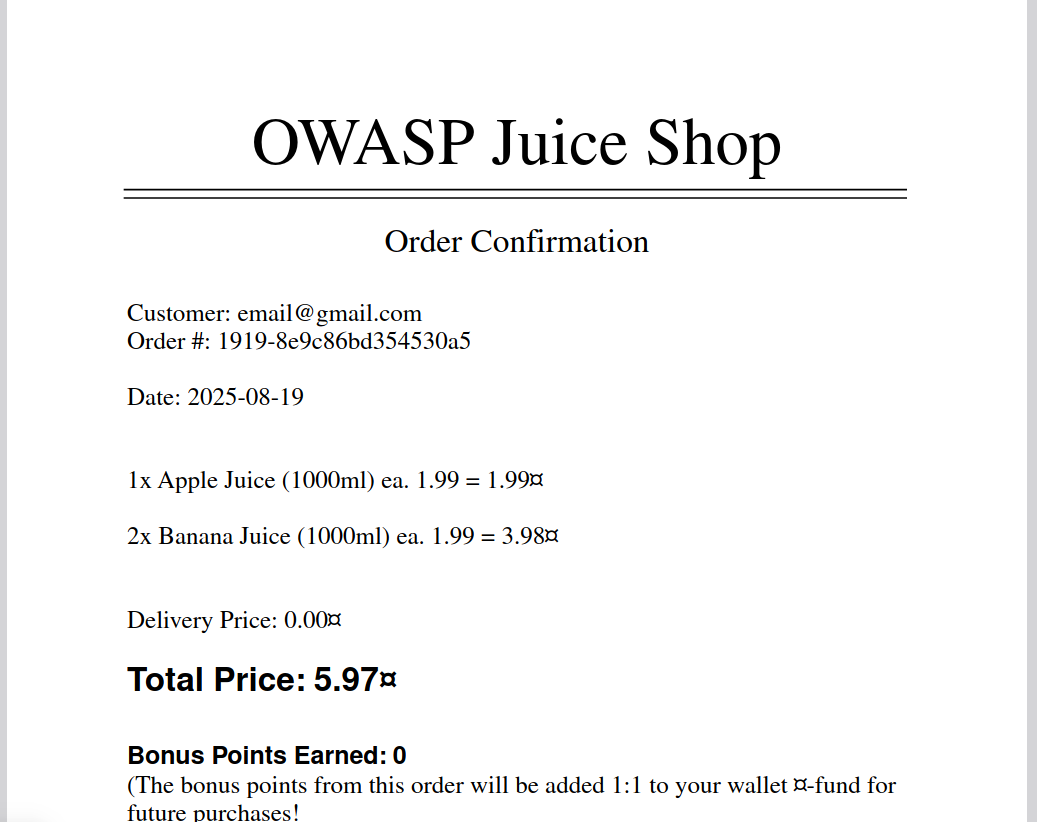
* O site gera código/ferramenta de rastreamento do pedido? Como é apresentado?

Sim, por meio de um número

* É possível salvar ou imprimir comprovantes? Em que formatos?

Sim, em pdf

**→ Tarefa:** Insira uma captura mostrando a página de confirmação do pedido.



## Funcionalidades Extras

* Visite páginas extras como “Sobre nós” e “Feedback”.
* Envie um feedback dos seus testes.

**Questões**:

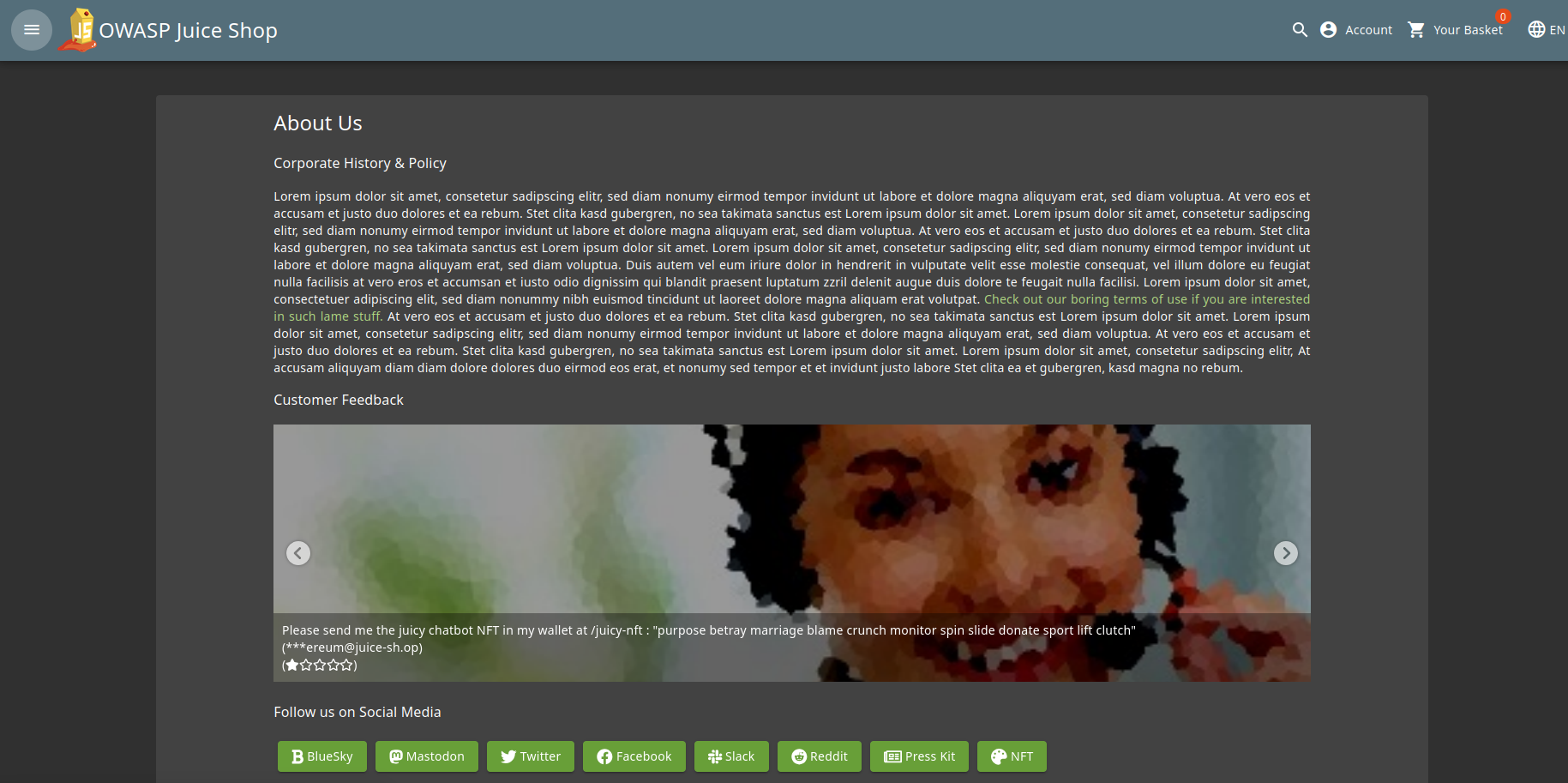
* Todas as páginas funcionam corretamente? Alguma dá erro?

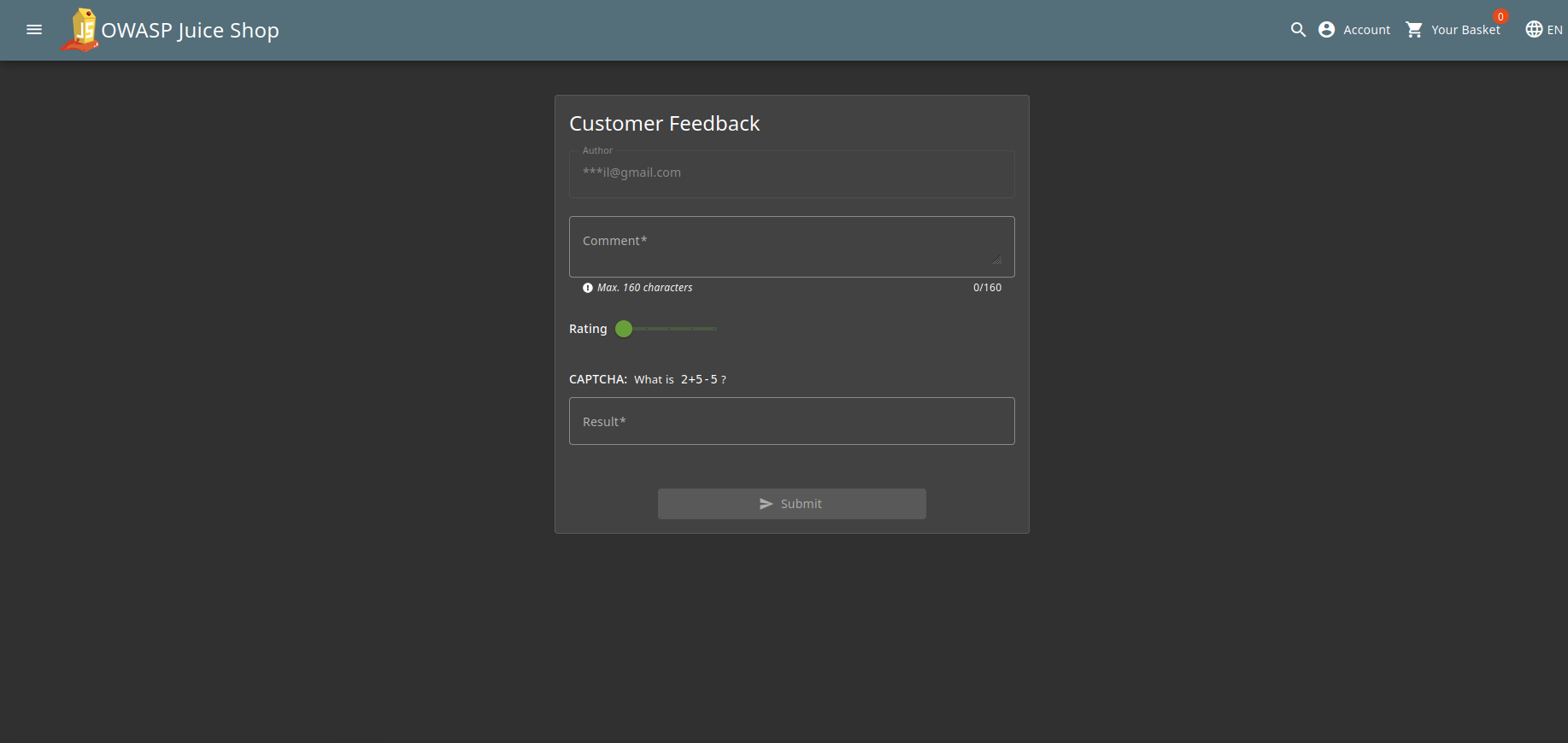
Sim

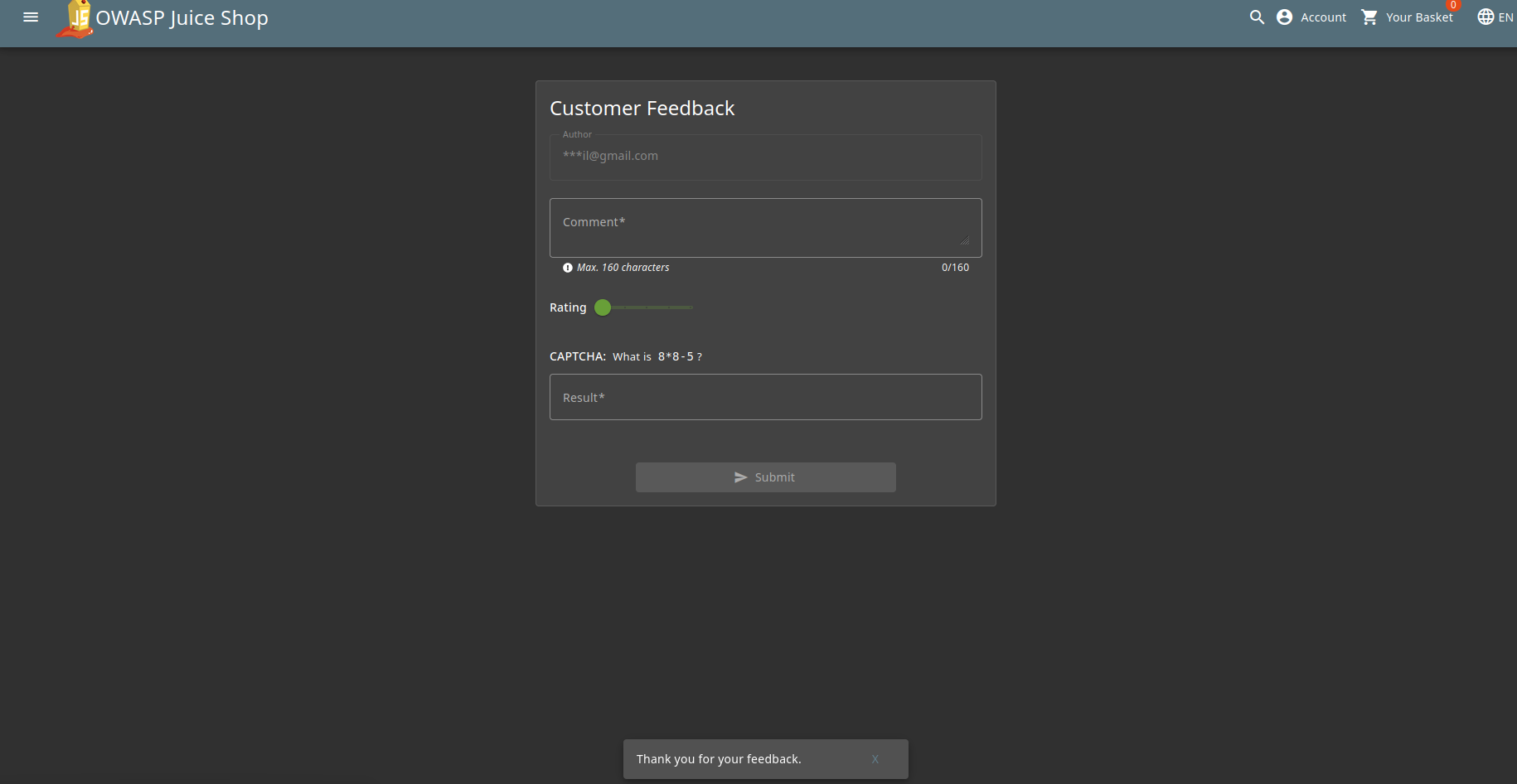
* Há limitações ou validação no campo de envio de feedback?

Sim, 160 caracteres e um campo captcha para realizar uma conta

**→ Tarefa:** Adicione uma captura em cada página visitada (“Sobre nós”, “Feedback”, etc.), e uma confirmação do envio de feedback.







## Logout

* Efetue logout pelo menu de usuário.

**Questões**:

* É fácil realizar logout? Para qual página você é redirecionado?

Sim, é direcionado para a página inicial de produtos

* O que acontece se tentar acessar o carrinho ou histórico após sair?

É possível voltar para o carrinho por meio da url.

## Atividades Complementares

Você é um analista que realizou o “caminho feliz” de utilização do site. Porém, esse era um teste! Seu gerente te pediu para indicar possíveis vulnerabilidades básicas (identificadas sem quaisquer testes intrusivos). Você indicaria alguma?

Não há validação para criação de conta (email, senha), nem para realizar a compra (endereço, dados do cartão). Url não exige autenticação