



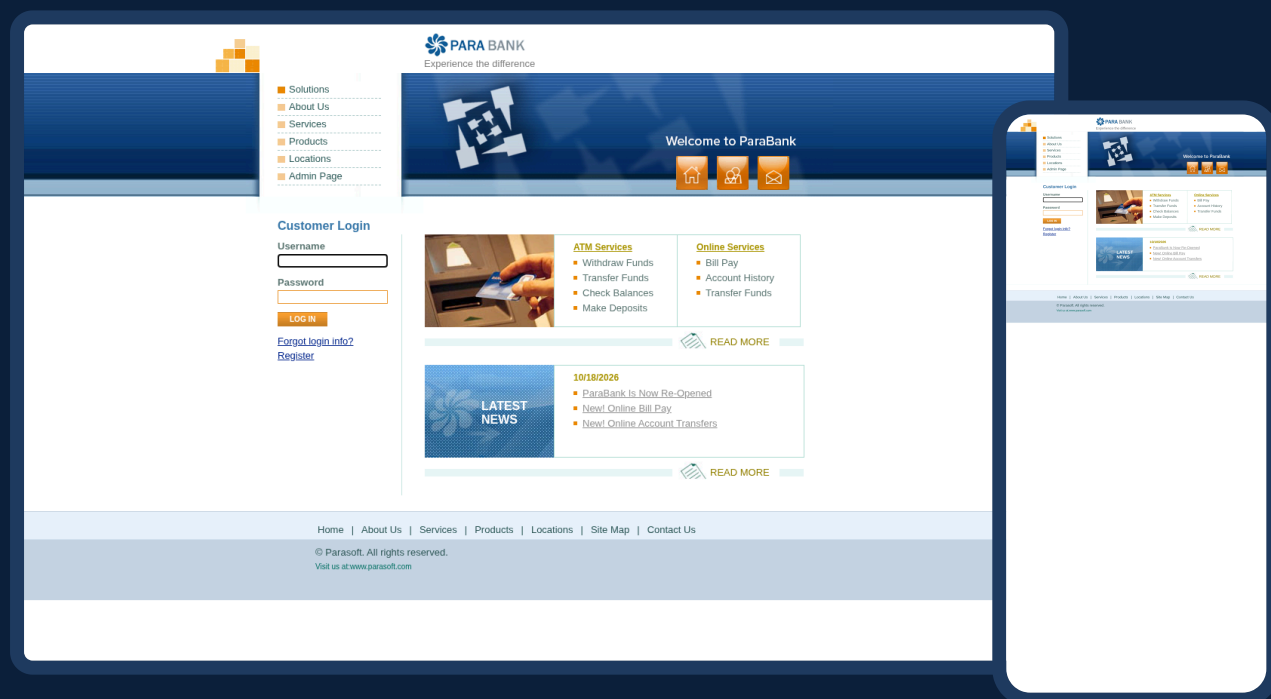
BARROCO
CONSULT

DIAGNÓSTICO DE QUALIDADE

Relatório de diagnóstico

ParaBank (ambiente público de demonstração)

Relatório demonstrativo



18 de outubro de 2026
Data

12
Páginas analisadas

Desktop + Celular
Dispositivos

Nível 2 simulado
ambiente de demonstração

Resumo executivo

Testamos os fluxos funcionais do banco de demonstração (login, cadastro, abertura de conta, transferência, pagamento de contas e empréstimo), além de acessibilidade, performance e cabeçalhos de segurança. Encontramos falhas graves nas regras de negócio de dinheiro: transferências acima do saldo e com valor negativo são concluídas. Também há problemas de acessibilidade em formulários e ausência de adaptação ao celular.

Achados por severidade



Principais riscos

- Transferência maior que o saldo é aceita** **CRÍTICA**
O cliente movimenta dinheiro que não tem; risco direto de perda financeira.
- Transferência com valor negativo é aceita** **CRÍTICA**
Permite puxar dinheiro de outra conta disfarçado de transferência.
- Valor vazio ou com letras gera erro interno** **ALTA**
O usuário não entende o erro e a equipe recebe o que parece falha de servidor.
- Cookie de sessão sem Secure e SameSite** **ALTA**
A sessão de quem acessa o banco fica mais exposta a sequestro e a requisições forjadas.
- Campos de formulário sem rótulo acessível** **ALTA**
Pessoas que usam leitor de tela não conseguem entrar, se cadastrar nem pagar contas.

O que já está bom

- Login rejeita credenciais inválidas e campos vazios com mensagem clara
- Cadastro valida campos obrigatórios
- Empréstimo nega valores acima dos fundos e entrada maior que o valor
- Performance de carregamento boa no desktop

Medições

/parabank/index.htm

Métrica	Desktop	Celular	Bom até
LCP	350 ms	1,5 s	2,5 s
CLS	0	0	0,1
TBT	0 ms	0 ms	200 ms
TTFB	109 ms	299 ms	800 ms

Medição de laboratório: a experiência real dos visitantes pode diferir.

Achados por categoria

Performance

0

Nenhum achado nesta categoria.

Cabeçalhos de segurança

2

Cookie de sessão sem Secure e SameSite

ALTA

O cookie de sessão é enviado com HttpOnly, mas sem os atributos Secure e SameSite.

Impacto no negócio: A sessão de quem acessa o banco fica mais exposta a sequestro e a requisições forjadas.

Recomendação: Adicionar Secure e SameSite=Lax (ou Strict) ao cookie de sessão.

```
HTTP 200 https://parabank.parasoft.com/parabank/index.htm
server: cloudflare
content-type: text/html;charset=ISO-8859-1
set-cookie: JSESSIONID=****; Path=/parabank; HttpOnly
x-content-type-options: nosniff
```

SEC-SESSION-COOKIE · Onde: /parabank/index.htm (Desktop) · Ocorrências: 1 · Esforço: Baixo

HSTS ausente

MÉDIA

A resposta não traz o cabeçalho Strict-Transport-Security, que força o navegador a usar sempre conexão segura.

Impacto no negócio: Em redes públicas, aumenta o risco de interceptação da conexão com o banco.

Recomendação: Ativar HSTS com max-age de pelo menos 6 meses.

```
HTTP 200 https://parabank.parasoft.com/parabank/index.htm
server: cloudflare
strict-transport-security: (ausente)
```

SEC-HSTS-MISSING · Onde: /parabank/index.htm (Desktop) · Ocorrências: 1 · Esforço: Baixo

Acessibilidade

2

Campos de formulário sem rótulo acessível

ALTA

25 campos nos formulários de login, cadastro e pagamento de contas não têm rótulo associado, incluindo uma lista de seleção.

Impacto no negócio: Pessoas que usam leitor de tela não conseguem entrar, se cadastrar nem pagar contas.

Recomendação: Associar um rótulo a cada campo e lista de seleção.

A11Y-FORM-LABEL · Onde: index.htm, register.htm, billpay.htm (Desktop) · Ocorrências: 25 · Esforço: Baixo · Evidência: login 2, cadastro 13, pagamento 10 (axe: label, select-name)

Idioma da página e contraste

MÉDIA

As páginas não declaram o idioma e há vários textos com contraste abaixo do mínimo recomendado.

Impacto no negócio: Dificulta leitores de tela e a leitura em telas com pouco brilho.

Recomendação: Declarar o idioma no HTML e ajustar as cores de texto para o contraste mínimo.

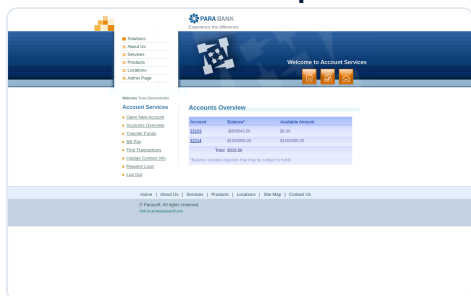
PERF-A11Y-NO-LANG · Onde: /parabank/index.htm (Desktop) · Ocorrências: 20 · Esforço: Baixo · Evidência: axe html-has-lang; c ontraste serious em várias telas

Erros funcionais visíveis

5

Transferência maior que o saldo é aceita

CRÍTICA



Com saldo de US\$ 515,50, uma transferência de US\$ 999.999,00 foi concluída e a conta de origem ficou com saldo de -US\$ 999.543,50.

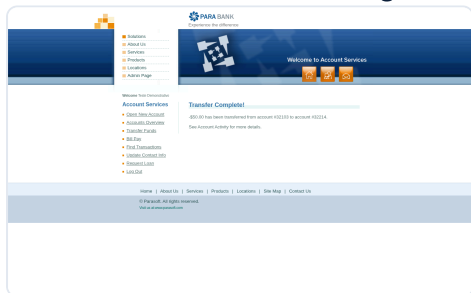
Impacto no negócio: O cliente movimenta dinheiro que não tem; risco direto de perda financeira.

Recomendação: Validar saldo e limite no servidor antes de concluir a transferência e cobrir o caso com teste automatizado de regressão.

FUNC-TRANSFER-OVERDRAFT · Onde: /parabank/transfer.htm (Desktop) · Ocorrências: 1 · Esforço: Médio · Evidência: saldo final -US\$ 999.543,50

Transferência com valor negativo é aceita

CRÍTICA



O valor -50 foi aceito e a tela confirmou a transferência, invertendo o sentido do dinheiro entre as contas.

Impacto no negócio: Permite puxar dinheiro de outra conta disfarçado de transferência.

Recomendação: Rejeitar valores menores ou iguais a zero no cliente e no servidor, com mensagem clara.

FUNC-TRANSFER-NEGATIVE · Onde: /parabank/transfer.htm (Desktop) · Ocorrências: 1 · Esforço: Baixo · Evidência: -US\$ 50,00 transferidos

Valor vazio ou com letras gera erro interno

ALTA



Com o valor vazio ou com letras, o serviço responde HTTP 400 "Server timeout" e a tela mostra "An internal error has occurred", sem orientar o usuário.

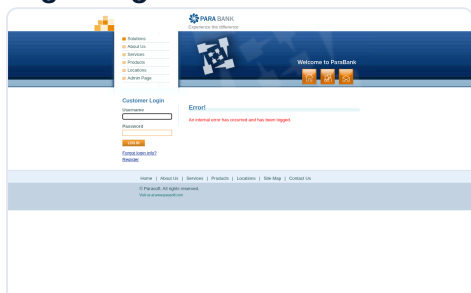
Impacto no negócio: O usuário não entende o erro e a equipe recebe o que parece falha de servidor.

Recomendação: Validar o campo antes do envio e devolver mensagem específica; corrigir a mensagem enganosa do serviço.

FUNC-TRANSFER-INVALID-AMOUNT · Onde: /parabank/transfer.htm (Desktop) · Ocorrências: 2 · Esforço: Baixo · Evidência: amount=abc e amount vazio → HTTP 400 "Server timeout"

Página logada sem sessão devolve erro interno

MÉDIA



Depois de sair, abrir a visão geral de contas retorna HTTP 500 e a mensagem de erro interno, em vez de levar ao login.

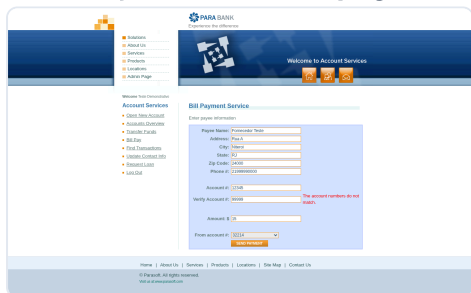
Impacto no negócio: Passa impressão de instabilidade e esconde a causa real do usuário.

Recomendação: Redirecionar requisições sem sessão para a tela de login.

FUNC-LOGOUT-500 · Onde: /parabank/overview.htm (Desktop) · Ocorrências: 1 · Esforço: Baixo · Evidência: GET overview.htm s em sessão → HTTP 500

Verificação de conta no pagamento é frágil

MÉDIA



O pagamento só compara "conta" e "confirmar conta"; qualquer número igual passa, sem checar se a conta existe.

Impacto no negócio: Pagamentos podem ir para contas inexistentes ou erradas.

Recomendação: Validar a conta de destino contra os dados reais antes de concluir o pagamento.

FUNC-BILL-VERIFY · Onde: /parabank/billpay.htm (Desktop) · Ocorrências: 1 · Esforço: Baixo · Evidência: conta 12345 x verificação o 99999

SEO técnico básico ausente

BAIXA

A home não tem meta description e o conjunto de páginas tem pouca marcação para busca.

Impacto no negócio: Menor visibilidade em buscadores.

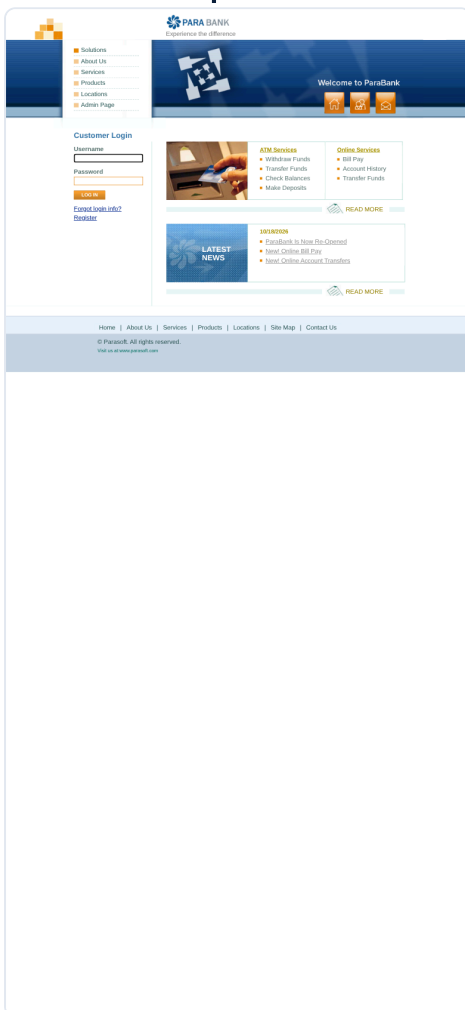
Recomendação: Adicionar título e descrição únicos por página.

SEO-TITLE-DESC · Onde: /parabank/index.htm (Desktop) · Ocorrências: 1 · Esforço: Baixo · Evidência: sem meta description na home

Visual mobile e desktop

Site não se adapta ao celular

MÉDIA



A página não tem meta viewport e renderiza com 980 px de largura numa tela de 390 px, exigindo zoom e rolagem lateral.

Impacto no negócio: Quem acessa o banco pelo celular tem muita dificuldade de usar.

Recomendação: Adicionar a meta viewport e tornar o layout responsivo.

VIS-MOBILE-OVERFLOW · Onde: /parabank/index.htm (Celular) · Ocorrências: 1 · Esforço: Médio · Evidência: largura 980 px em tela de 390 px; sem meta viewport

Plano de 30 dias

Semana 1 Corrigir o que bloqueia uso e vendas • Transferência maior que o saldo é aceita • Transferência com valor negativo é aceita • Valor vazio ou com letras gera erro interno	Semana 2 Fechar os riscos altos restantes • Cookie de sessão sem Secure e SameSite • Campos de formulário sem rótulo acessível	Semana 3 Ajustes de qualidade • Página logada sem sessão devolve erro interno • Verificação de conta no pagamento é frágil • Idioma da página e contraste • Site não se adapta ao celular • HSTS ausente	Semana 4 Prevenir regressões • Testes automatizados de ponta a ponta dos fluxos de dinheiro • Validação de saldo, limites e valores no servidor • Suíte de regressão rodando a cada publicação
--	--	--	--

Limitações deste diagnóstico

- Testes feitos no ambiente público de demonstração da ferramenta, criado para testes, com usuário fictício e sem carga nem ataque
- 12 de 20 páginas do fluxo analisadas
- Performance medida em laboratório; a experiência real pode diferir
- Acessibilidade automática não é declaração de conformidade

Próximos passos

- Em um produto real, o Nível 2 exige autorização assinada, usuário de teste e janela combinada
- Cobrir os fluxos de dinheiro com testes automatizados e monitorar regressões

Pacote sugerido

160h

horas por mês

Banco com área logada e fluxo de dinheiro, com falhas críticas nas regras de transferência.

Um QA dedicado em tempo integral para cobrir os fluxos críticos e evitar regressões.

Valores sob consulta.

Vamos resolver esses pontos juntos?

Agende uma conversa de 30 minutos com a equipe da Barroco: explicamos cada achado e montamos o plano para o seu produto.

barrocoqa.com/pt · contato@barrocoqa.com

Agendar conversa

Diagnóstico gerado com apoio de IA e validado por um analista humano. Relatório demonstrativo, de divulgação pública.

