



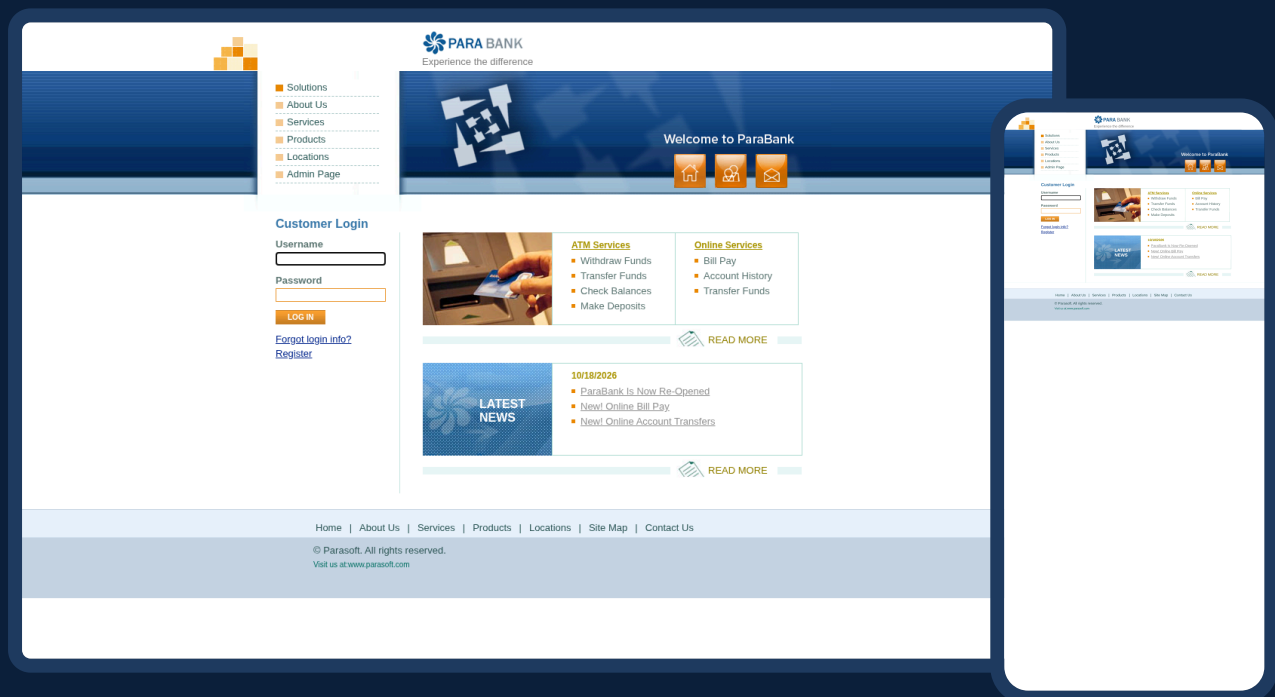
BARROCO
CONSULT

QUALITY DIAGNOSIS

Diagnosis report

ParaBank (public demonstration environment)

Demonstration report



October 18, 2026
Date

12
Pages reviewed

Desktop + Mobile
Devices

Simulated Level 2
demo environment

Executive summary

We tested the demo bank's functional flows (login, sign-up, open account, transfer, bill payment and loan), plus accessibility, performance and security headers. We found serious money business-rule failures: transfers above the balance and with a negative amount complete. There are also form accessibility issues and no mobile adaptation.

Findings by severity



Top risks

- 1 Transfer larger than the balance is accepted** **CRITICAL**
Customers move money they do not have; direct risk of financial loss.
- 2 Negative transfer amount is accepted** **CRITICAL**
Allows pulling money from another account disguised as a transfer.
- 3 Empty or text amount triggers an internal error** **HIGH**
Users cannot tell what went wrong and the team gets what looks like a server failure.
- 4 Session cookie without Secure and SameSite** **HIGH**
Banking sessions are more exposed to hijacking and forged requests.
- 5 Form fields without an accessible label** **HIGH**
Screen reader users cannot log in, sign up or pay bills.

What is already good

- Login rejects invalid credentials and empty fields with a clear message
- Sign-up validates required fields
- Loan denies amounts above available funds and a down payment larger than the amount
- Good load performance on desktop

Measurements

/parabank/index.htm

Metric	Desktop	Mobile	Good up to
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

Lab measurement: real visitor experience may differ.

Findings by category

Performance

0

No findings in this category.

Security headers

2

Session cookie without Secure and SameSite

HIGH

The session cookie is sent with HttpOnly but without the Secure and SameSite attributes.

Business impact: Banking sessions are more exposed to hijacking and forged requests.

Recommendation: Add Secure and SameSite=Lax (or Strict) to the session cookie.

```
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 · Where: /parabank/index.htm (Desktop) · Occurrences: 1 · Effort: Low

HSTS missing

MEDIUM

The response has no Strict-Transport-Security header to force the browser to always use a secure connection.

Business impact: On public networks, raises the risk of intercepting the connection to the bank.

Recommendation: Enable HSTS with a max-age of at least 6 months.

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

SEC-HSTS-MISSING · Where: /parabank/index.htm (Desktop) · Occurrences: 1 · Effort: Low

Accessibility

2

Form fields without an accessible label

HIGH

25 fields across login, sign-up and bill payment have no associated label, including one select list.

Business impact: Screen reader users cannot log in, sign up or pay bills.

Recommendation: Associate a label with every field and select list.

A11Y-FORM-LABEL · Where: index.htm, register.htm, billpay.htm (Desktop) · Occurrences: 25 · Effort: Low · Evidence: login 2, sign-up 13, bill payment 10 (axe: label, select-name)

Page language and contrast

MEDIUM

Pages do not declare a language and several texts are below the recommended minimum contrast.

Business impact: Hurts screen readers and reading on dim screens.

Recommendation: Declare the language in the HTML and adjust text colors to meet minimum contrast.

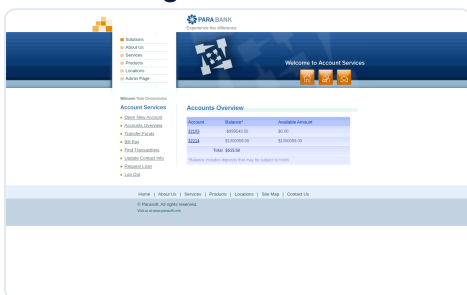
PERF-A11Y-NO-LANG · Where: /parabank/index.htm (Desktop) · Occurrences: 20 · Effort: Low · Evidence: axe html-has-lang; contrast serious on several screens

Visible functional errors

5

Transfer larger than the balance is accepted

CRITICAL



With a US\$ 515.50 balance, a US\$ 999,999.00 transfer completed and the source account ended at -US\$ 999,543.50.

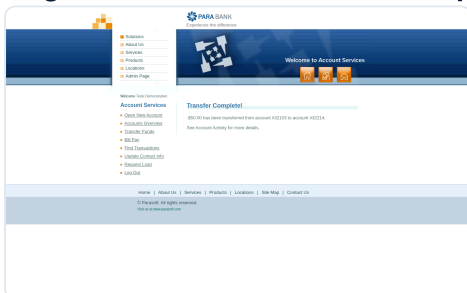
Business impact: Customers move money they do not have; direct risk of financial loss.

Recommendation: Validate balance and limit on the server before completing the transfer and cover it with an automated regression test.

FUNC-TRANSFER-OVERDRAFT · Where: /parabank/transfer.htm (Desktop) · Occurrences: 1 · Effort: Medium · Evidence: final balance -US\$ 999,543.50

Negative transfer amount is accepted

CRITICAL



The amount -50 was accepted and the page confirmed the transfer, reversing the money flow between accounts.

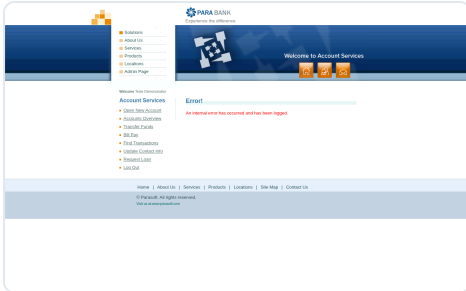
Business impact: Allows pulling money from another account disguised as a transfer.

Recommendation: Reject amounts of zero or less on client and server, with a clear message.

FUNC-TRANSFER-NEGATIVE · Where: /parabank/transfer.htm (Desktop) · Occurrences: 1 · Effort: Low · Evidence: -US\$ 50.00 transferred

Empty or text amount triggers an internal error

HIGH



With an empty or text amount the service returns HTTP 400 "Server timeout" and the page shows "An internal error has occurred", with no guidance.

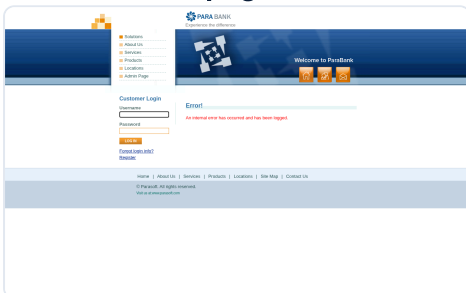
Business impact: Users cannot tell what went wrong and the team gets what looks like a server failure.

Recommendation: Validate the field before sending and return a specific message; fix the misleading service message.

FUNC-TRANSFER-INVALID-AMOUNT · Where: /parabank/transfer.htm (Desktop) · Occurrences: 2 · Effort: Low · Evidence: amount=abc and empty amount → HTTP 400 "Server timeout"

Authenticated page without a session returns an internal error

MEDIUM



After logging out, opening the account overview returns HTTP 500 and an internal error message instead of the login screen.

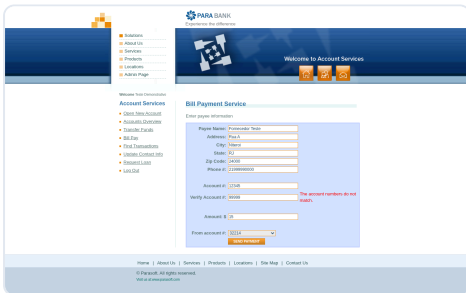
Business impact: Looks unstable and hides the real cause from the user.

Recommendation: Redirect requests without a session to the login page.

FUNC-LOGOUT-500 · Where: /parabank/overview.htm (Desktop) · Occurrences: 1 · Effort: Low · Evidence: GET overview.htm without a session → HTTP 500

Weak account verification on bill payment

MEDIUM



Bill payment only compares "account" and "confirm account"; any matching number passes, with no check that the account exists.

Business impact: Payments can go to non-existent or wrong accounts.

Recommendation: Validate the target account against real data before completing the payment.

FUNC-BILL-VERIFY · Where: /parabank/billpay.htm (Desktop) · Occurrences: 1 · Effort: Low · Evidence: account 12345 vs verification 99999

Basic technical SEO missing

LOW

The home page has no meta description and the pages carry little search markup.

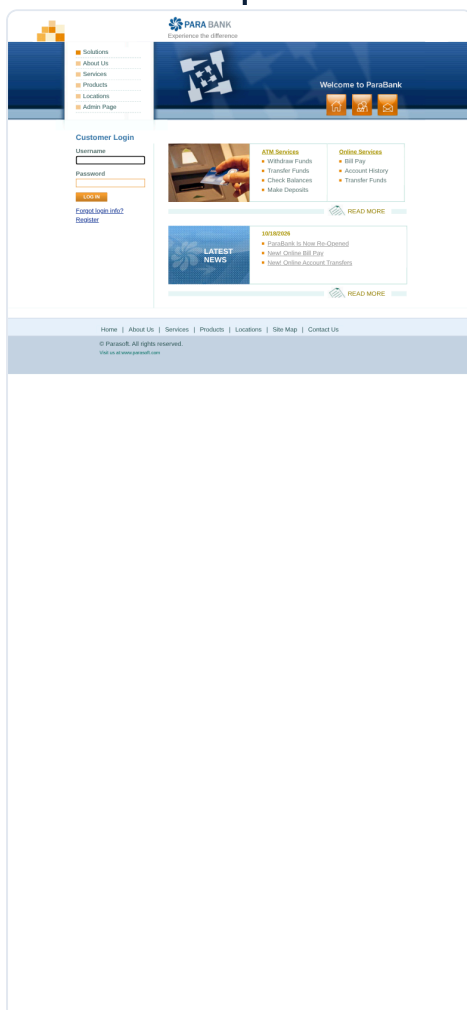
Business impact: Lower visibility in search engines.

Recommendation: Add a unique title and description per page.

SEO-TITLE-DESC · Where: /parabank/index.htm (Desktop) · Occurrences: 1 · Effort: Low · Evidence: no meta description on the home page

Mobile and desktop visuals**Site does not adapt to mobile**

MEDIUM



The page has no viewport meta and renders at 980 px wide on a 390 px screen, forcing zoom and sideways scrolling.

Business impact: Customers on mobile struggle to use the bank.

Recommendation: Add the viewport meta and make the layout responsive.

VIS-MOBILE-OVERFLOW · Where: /parabank/index.htm (Mobile) · Occurrences: 1 · Effort: Medium · Evidence: width 980 px on a 390 px screen; no viewport meta

30-day plan

Week 1 Fix what blocks usage and sales • Transfer larger than the balance is accepted • Negative transfer amount is accepted • Empty or text amount triggers an internal error	Week 2 Close the remaining high risks • Session cookie without Secure and SameSite • Form fields without an accessible label	Week 3 Quality improvements • Authenticated page without a session returns an internal error • Weak account verification on bill payment • Page language and contrast • Site does not adapt to mobile • HSTS missing	Week 4 Prevent regressions • Automated end-to-end tests for the money flows • Server-side validation of balance, limits and amounts • Regression suite running on every release
--	--	--	---

Limitations of this diagnosis

- Tests run on the tool's public demo environment, built for testing, with a fictitious user and no load or attacks
- 12 of 20 flow pages reviewed
- Performance measured in a lab; real experience may differ
- Automated accessibility is not a conformance statement

Next steps

- On a real product, Level 2 requires signed authorization, a test user and an agreed window
- Cover the money flows with automated tests and monitor regressions

Suggested package

160h

hours per month

A bank with a logged-in area and money flows, with critical failures in the transfer rules.
A full-time dedicated QA to cover the critical flows and prevent regressions.
Pricing on request.

Shall we fix these together?

Book a 30-minute call with the Barroco team: we walk you through every finding and build the plan for your product.

barrocoqa.com · contactus@barrocoqa.com

Book a call

Diagnostic produced with AI assistance and validated by a human analyst. Sample report, for public distribution.

