AI Test Results from testers.ai

D+

The 'AccnSpark' app's HOME page presents a concerning picture of quality. Several security vulnerabilities, such as insecure transmission of credentials due to the lack of HTTPS and insecure password management (missing 'autocomplete' attribute for new password), are critical. Accessibility is also a major concern, with missing labels for form fields and WCAG violations. Furthermore, usability is hampered by issues like a broken 'Forgot Password?' link, a missing email validation, and lack of password visibility toggle. Performance issues, such as redundant requests for the logo image, add to the app's woes.

Best Aspects

It at least loads something, which is more than can be said for apps that crash immediately.

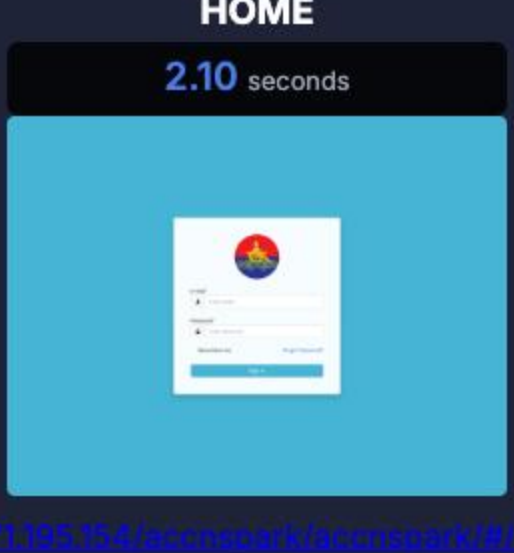
Areas for Improvement

The egregious security vulnerabilities and accessibility issues are appalling.

Quality Summary

HOME

2.10 seconds



http://167.71.195.154/accnspark/accnspark/#/dashboard

Detailed Analysis

The 'AccnSpark' app's HOME page is riddled with problems spanning security, accessibility, performance, and usability. From a security standpoint, the absence of HTTPS for credential transmission is a glaring red flag, potentially exposing user data. The insecure password management, with missing 'autocomplete' attributes, further amplifies this risk. Accessibility is severely compromised by missing labels for form fields and general WCAG violations. Usability is also undermined by a broken 'Forgot Password?' link, lack of password visibility, and missing email validation, making the user experience frustrating. Performance bottlenecks, such as redundant logo image requests, also exist. The missing privacy policy is a legal concern.

Key Suggestions

- Prioritize security fixes: Implement HTTPS immediately and address insecure password management practices.
- Address accessibility violations: Ensure all form fields have proper labels for screen readers.
- Improve usability: Fix the 'Forgot Password?' link, add email validation, and provide a password visibility toggle.
- Optimize performance: Eliminate redundant logo image requests.
- Add a link to a valid Privacy Policy

Priority Improvements

1. Implement HTTPS to encrypt all data transmissions, especially credentials, on the HOME page.
2. Add the 'autocomplete="new-password"' attribute to the new password input field to improve secure password management.
3. Implement server-side email validation to prevent users from submitting invalid or malicious email addresses.
4. Implement a password visibility toggle on all password input fields.
5. Remove the redundant requests for the logo image to improve the page loading speed.

Issues Found by AI Testers

HOME

Pete — Privacy and Security Tester

Insecure Transmission of Credentials due to Lack of HTTPS

Priority: 8/10 | Confidence: 9/10

Security | GDPR | OWASP

Why is this a bug?
The page is served over HTTP, as evidenced by the network call `http://167.71.195.154/accnspark/accnspark/`. This means that the email and password submitted through the login form are transmitted in plaintext, making them vulnerable to interception by malicious actors. This directly violates the GDPR's requirement for secure handling of personal data and is a major security risk.

Suggested Fix
Implement HTTPS by obtaining an SSL/TLS certificate and configuring the web server to serve the page over HTTPS. Redirect all HTTP traffic to HTTPS.

Why Fix This?
Failure to encrypt data in transit leaves user credentials exposed, potentially leading to unauthorized access and data breaches. This violates privacy regulations like GDPR and damages user trust.

Route To
Security Engineer, DevOps Engineer

Relevant Network Call
`http://167.71.195.154/accnspark/accnspark/`

Sharon — API and Networking Tester

Redundant Requests for Logo Image

Priority: 7/10 | Confidence: 9/10

performance | network efficiency

Why is this a bug?
The network traffic shows multiple requests for the same logo image ('http://167.71.195.154/accnspark/accnspark/as within a short period (approximately 0.01 seconds). This indicates a lack of proper caching, leading to unnecessary bandwidth consumption and increased load times. The timestamp on the requests are: 1744643272.999778 and 1744643273.203603

Suggested Fix
Implement browser caching for the logo image by setting appropriate cache headers (e.g., Cache-Control, Expires) on the server serving the image. Also, investigate the client-side code to ensure that the image is not being re-requested unnecessarily.

Why Fix This?
Resolving this issue reduces bandwidth usage, speeds up page load times, and lowers server load, improving the overall user experience.

Route To
Frontend Engineer and Backend Engineer

Relevant Network Call
`http://167.71.195.154/accnspark/accnspark/assets/logo.e34a61bf.png`

Pete — Privacy and Security Tester

Missing Privacy Policy

Priority: 7/10 | Confidence: 8/10

GDPR | General Privacy

Why is this a bug?
A privacy policy is not visibly linked or present on the login page. The GDPR mandates that users must be informed about how their data is collected, used, and protected. The absence of a privacy policy violates this requirement.

Suggested Fix
Create a comprehensive privacy policy that outlines data collection practices, usage, and protection measures. Add a visible link to the privacy policy in the footer of the page, or near the login form.

Why Fix This?
Lack of a privacy policy violates GDPR and other privacy regulations, leading to potential legal issues and loss of user trust.

Route To
Legal, Front-end Engineer

Isabella — Usability Tester

Missing Labels for Form Fields

Priority: 7/10 | Confidence: 9/10

WCAG | accessibility

Why is this a bug?
The form fields for 'E-mail' and 'Password' do not have properly associated `<label>` elements. While there is text visually indicating what the fields are for, this text is not programmatically connected to the input fields. This lack of proper labels makes the form inaccessible to screen reader users, violating WCAG 2.1 success criterion 1.3.1 (Info and Relationships).

Suggested Fix
Use the `<label>` element with the 'for' attribute to associate each label with its corresponding input field by matching the 'id' of the input. E.g., `<label for="email">E-mail* </label>` and `<input type="email" id="email" ...>`.

Why Fix This?
Essential for accessibility compliance, improving user experience for people using screen readers and other assistive technologies.

Route To
Frontend Engineer

Relevant Network Call
N/A

Aisha — Tester for Missing Aspects

Missing Email Validation

Priority: 7/10 | Confidence: 9/10

general | usability

Why is this a bug?
The email input field lacks client-side validation. Without it, users might submit incorrectly formatted email addresses, which will only be caught server-side (if at all). This leads to a poor user experience due to delayed error feedback.

Suggested Fix
Implement client-side email validation using HTML5 input type='email' and/or JavaScript to check for a valid email format (e.g., using a regular expression).

Why Fix This?
Improved user experience, reduced server load, and immediate feedback for users.

Route To
Frontend Engineer

Isabella — Usability Tester

Broken 'Forgot Password?' Link

Priority: 7/10 | Confidence: 9/10

general | accessibility

Why is this a bug?
The 'Forgot Password?' link has an `href` value of '#', indicating it's a placeholder and not functional. Clicking it won't lead to a password reset page, frustrating users attempting to recover their accounts.

Suggested Fix
Implement a functional password reset mechanism and update the `href` attribute to point to the appropriate reset page.

Why Fix This?
Essential for account recovery, improving user experience and security.

Route To
Backend Engineer

Relevant Network Call
N/A

Abdul — Privacy and Security Tester

Insecure HTTP Request

Priority: 7/10 | Confidence: 8/10

OWASP | Sensitive Data Exposure

Why is this a bug?
The initial request to the website `http://167.71.195.154/accnspark/accnspark/` is made over HTTP. This is insecure because any data transmitted during this initial request, including any potential redirects that might expose sensitive information, is vulnerable to interception by malicious actors. This can lead to man-in-the-middle attacks, where attackers can eavesdrop on the communication, steal sensitive data, or even inject malicious content into the webpage. Even if subsequent requests are made over HTTPS, the initial HTTP request creates a window of vulnerability.

Suggested Fix
Implement a server-side redirect to enforce HTTPS for all requests to the website. This can be done by configuring the web server to redirect HTTP requests to the HTTPS equivalent. Additionally, ensure that the HTTP Strict Transport Security (HSTS) header is configured to instruct browsers to always use HTTPS when accessing the site.

Why Fix This?
Fixing this vulnerability is critical to ensure the confidentiality and integrity of data transmitted between the user and the website. By enforcing HTTPS, you protect against eavesdropping, data tampering, and man-in-the-middle attacks, enhancing the overall security posture of the website and protecting user information.

Route To
DevOps/Backend Engineer

Relevant Network Call
`http://167.71.195.154/accnspark/accnspark/`

AI Generated Functional Test Results

Start Page: HOME

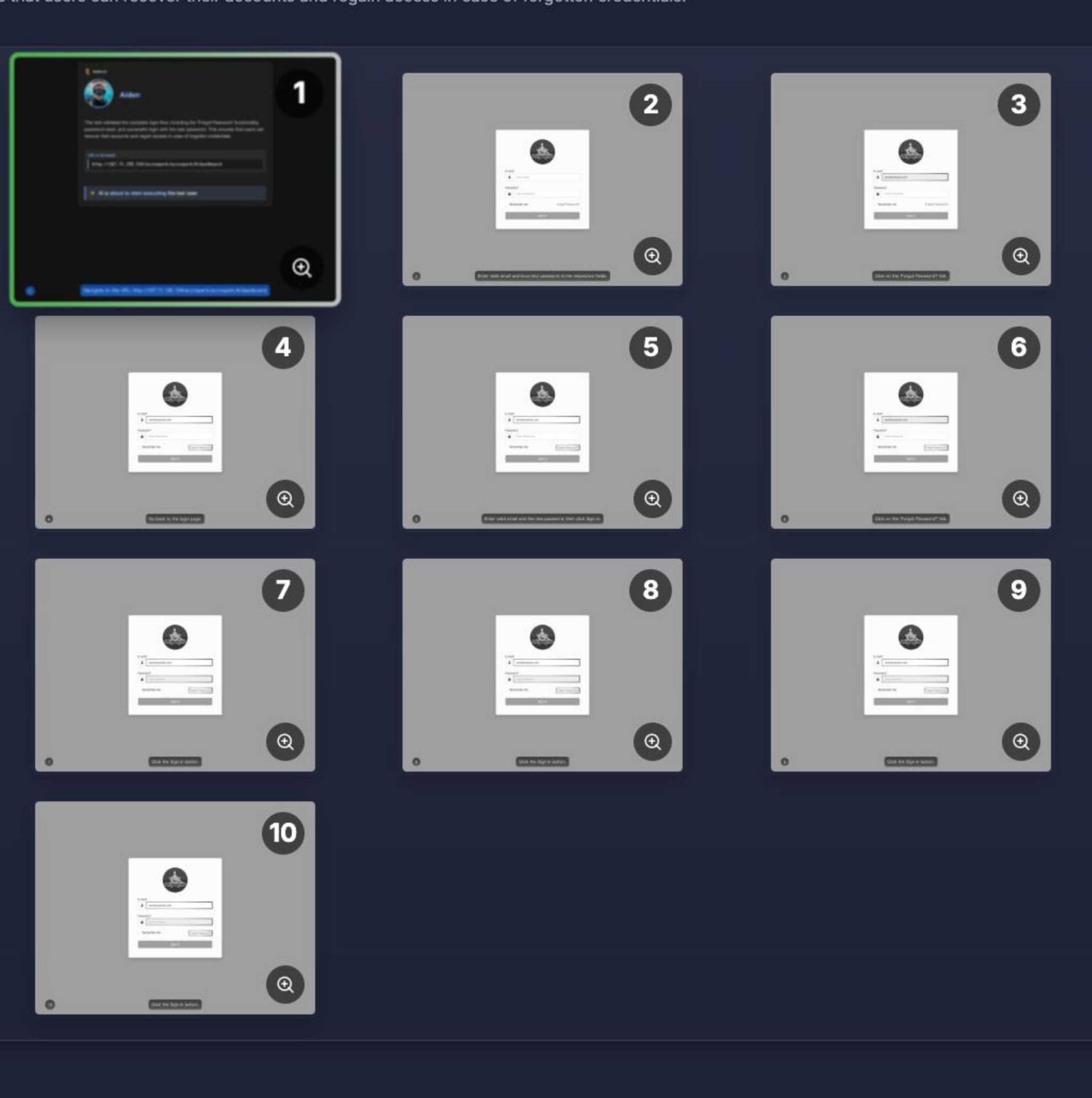
Aiden
Demo_Tests

✓ Login with valid email and password

This test verifies that a user can successfully log in with a valid email and password. This ensures the core login functionality is working as expected.

Valid login flow after password reset

This test validates the complete login flow, including the 'Forgot Password' functionality, password reset, and successful login with the new password. This ensures that users can recover their accounts and regain access in case of forgotten credentials.



✓ Verify 'Forgot Password?' link navigates to password reset page

This test verifies that the 'Forgot Password?' link functions correctly and redirects the user to the appropriate password reset page. This ensures users can recover their accounts if they forget their passwords.

User Persona Feedback Summary

HOME

The purpose of the webpage is to provide a login portal for users to access a dashboard, likely for an application or service named 'accnspark'.

Overall Score ★★★☆☆
The page is functional for its intended purpose, but has some minor issues regarding usability and visual design that could be improved. The password reset option is good, but needs to be better featured.

Visual Design ★★★☆☆
The overall visual presentation could be improved, especially with more attention to contrast and modern design.

Usability ★★★☆☆
The usability is decent, as the form is straightforward to use. However, the 'Forgot Password?' link could be more prominent.

Content Quality ★★★★☆
The content is minimal but effective for its purpose. The email and password fields are clearly labeled, and the 'Remember me' option is present.

Individual User Persona Feedback

Aisha Khan, 28

Persona:Aisha is a software developer with 5 years of experience. She works remotely and is always looking for efficient tools to manage her workflow. She often uses multiple applications and needs seamless login experiences.

Overall Rating ★★★☆☆

As a software developer, I appreciate the simplicity of the login page. However, I expect more robust security features and a smoother user experience.

Actions Performed
- Enter email and password
- Click 'Sign in'

Suggestions
- Implement a more modern and visually appealing design.
- Add two-factor authentication for enhanced security.
- Make the 'Forgot Password?' link more prominent and easier to find.
- Ensure the page is fully accessible with proper ARIA attributes and keyboard navigation.

David Lee, 35

Persona:David is a seasoned IT professional who works as a systems administrator. He is highly skilled in identifying security vulnerabilities and ensuring system integrity. He values robust authentication mechanisms.

Overall Rating ★★☆☆☆

As a systems administrator, I'm immediately concerned about the security aspects. This login page is very basic and lacks essential security features.

Actions Performed
- Enter email and password
- Examine the security features

Suggestions
- Implement mandatory two-factor authentication.
- Add a captcha or other bot protection to prevent brute-force attacks.
- Include a password strength meter to encourage strong passwords.
- Provide security audit information for transparency.

Emily Carter, 45

Persona:Emily is a small business owner who struggles with technology. She often finds complicated login processes frustrating. She needs a simple, straightforward way to access her account.

Overall Rating ★★★☆☆

I just want to log in and get my work done. This page is simple enough, but I always worry about forgetting my password.

Actions Performed
- Enter email and password
- Look for customer support

Suggestions
- Make the 'Forgot Password?' link more visible.
- Provide easy access to customer support in case I get stuck.

Print Report