AI Test Results from testers.ai

C-

The PagerDuty HOME page presents a mixed bag of quality signals. On the one hand, there are significant security concerns such as "Mixed Content Warning - Insecure Frame Request" and "Missing or Misconfigured Content Security Policy (CSP)", indicating a potential vulnerability. There are also multiple performance and network issues reported as "Failed Resource Loads - 404 Not Found" . On the other hand, a large number of accessibility issues have been reported such as "Inadequate link descriptions in "Our Solutions" section", indicating a failure to conform to WCAG standards.

Best Aspects

The app has a well-defined purpose and attempts to provide valuable content, but the technical execution needs improvement to realize its potential.

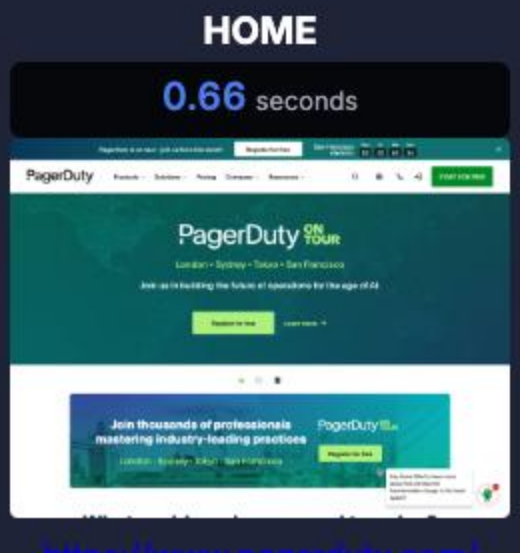
Areas for Improvement

Security vulnerabilities, accessibility violations, and performance bottlenecks are the most glaring weaknesses of the PagerDuty HOME page.

Quality Summary

HOME

0.66 seconds



https://www.pagerduty.com/

Detailed Analysis

The PagerDuty HOME page analysis reveals critical issues demanding immediate attention. The presence of security vulnerabilities like "Mixed Content Warning - Insecure Frame Request" and "Insecure HTTP Request for Iframe" exposes users to potential risks, demanding a thorough security audit. Performance problems, highlighted by "Multiple Failed Resource Loads - Domain Name Not Resolved" and other network-related bugs, impact the user experience and necessitate optimizing resource loading. Moreover, accessibility shortcomings, such as "Missing Context for Links with Identical Text" and "Insufficient Text Contrast in Butter Bar Link", exclude users with disabilities and undermine the app's inclusivity.

Key Suggestions

- Conduct a thorough security audit to identify and remediate all potential vulnerabilities.
- Implement WCAG guidelines to enhance accessibility for all users.
- Optimize resource loading and address network-related issues to improve page performance.
- Establish automated testing procedures to detect and prevent regression of security and accessibility issues.
- Refactor existing components to ensure all links have proper context and descriptions.

Priority Improvements

1. Implement a robust Content Security Policy (CSP) to mitigate the risk of mixed content and other security vulnerabilities.
2. Identify and resolve all instances of insecure HTTP requests, migrating to HTTPS to protect data in transit.
3. Optimize resource loading to eliminate failed resource loads and improve page performance, including addressing DNS resolution issues.
4. Refactor ambiguous and context-lacking link text to comply with WCAG guidelines, ensuring all links are descriptive and accessible.
5. Update outdated JavaScript libraries (like VWO) to ensure security and performance.
6. Review and fix all instances of insufficient text contrast to improve accessibility for users with visual impairments.
7. Remove or remediate third-party tracking via ob.thisgreencolumn.com to ensure GDPR compliance.

Issues Found by AI Testers

HOME

Jason
AI Tester

Mixed Content Warning - Insecure Frame Request

Priority: 7/10 Confidence: 9/10

security content

Why is this a bug?
The page is loaded over HTTPS, but it's attempting to load an insecure frame (HTTP). Browsers block this, leading to a degraded user experience and potential security vulnerabilities.

Suggested Fix
Update the frame URL to use HTTPS to ensure all content is served securely.

Why Fix This?
Resolving mixed content warnings is crucial for security and to avoid browser blocking the content.

Route To
Frontend Engineer

Jason
AI Tester

Multiple Failed Resource Loads - Domain Name Not Resolved

Priority: 7/10 Confidence: 8/10

performance network

Why is this a bug?
Numerous 'net::ERR_NAME_NOT_RESOLVED' errors indicate DNS resolution failures, suggesting a network configuration problem or a temporary outage with the server hosting those resources. This impacts functionality reliant on these resources.

Suggested Fix
Investigate DNS configuration, check server availability, and implement retry mechanisms for resource loading.

Why Fix This?
Unresolved DNS leads to broken functionality and poor user experience.

Route To
Backend Engineer / DevOps

Jason
AI Tester

Refused to execute script due to MIME type

Priority: 7/10 Confidence: 8/10

security network

Why is this a bug?
The server is serving a Javascript file with the wrong MIME type ('text/html'), which is a security risk. This stops the browser from executing the script. This is a high confidence bug because the browser explicitly refuses to execute.

Suggested Fix
The server configuration for `api.company-target.com` must be updated to send Javascript files with the correct MIME type (`application/javascript`).

Why Fix This?
Security best practices for browsers prevent execution of wrong mime types

Route To
Backend Engineer / DevOps

Sophia
Content Tester

Outdated Copyright Year

Priority: 7/10 Confidence: 9/10

General

Why is this a bug?
The copyright notice in the footer displays '© 2024 PagerDuty, Inc. All rights reserved.' The current year is 2025, making this incorrect and unprofessional.

Suggested Fix
Update the copyright notice in the footer to '© 2025 PagerDuty, Inc. All rights reserved.'

Why Fix This?
An outdated copyright year undermines the site's credibility and gives the impression of neglect or abandonment.

Route To
Front-end developer

Sharon
API and Networking Tester

Referencing potentially outdated Visual Website Optimizer (VWO) JavaScript libraries.

Priority: 7/10 Confidence: 8/10

Security Performance

Why is this a bug?
The network traffic includes requests to `dev.visualwebsiteoptimizer.com` for JavaScript resources. The names of these resources (e.g., `va_gq-3c5e403756405f46fc0d721428dbc45cbr.js`, `worker-b31b97f8c2fb7582cde37c6681f5aeadbr.js`) appear to be generated based on hashes, which are potentially associated with specific versions of the VWO library. If these library versions are very old, they might contain known security vulnerabilities or compatibility issues with modern browsers or frameworks. While not definitively *old*, the fact that they are being served from 'dev.visualwebsiteoptimizer.com' implies they might not be production-ready or actively maintained. This raises concerns about security and reliability.

Suggested Fix
Investigate the VWO integration to determine if the loaded library versions are the latest recommended and supported versions. If not, update to the most recent stable versions. Ensure that the VWO setup is using production-ready endpoints rather than 'dev' endpoints.

Why Fix This?
Using outdated JavaScript libraries can expose the website to security vulnerabilities, compatibility issues, and performance degradation. Regularly updating to the latest stable versions is crucial for maintaining a secure and reliable user experience.

Route To
Frontend Engineer / Security Engineer

Relevant Network Call

```
https://dev.visualwebsiteoptimizer.com/j.php?a=753563&u=https%3A%2F%2Fwww.pagerduty.com%2F&vn=2.1&x=true
https://dev.visualwebsiteoptimizer.com/cdn/edrv/worker-b31b97f8c2fb7582cde37c6681f5aeadbr.js
https://dev.visualwebsiteoptimizer.com/cdn/edrv/va_gq-3c5e403756405f46fc0d721428dbc45cbr.js
https://dev.visualwebsiteoptimizer.com/v.gif?cd=0&a=753563&d=pagerduty.com&u=DDB0814ADD775A9D817115D3457D7D6B1&h=5c75b7ea370687a92bb2b8cac15a3ac5&t=false
```

Abdul
Privacy and Security Tester

Missing or Misconfigured Content Security Policy (CSP)

Priority: 7/10 Confidence: 8/10

OWASP General Security

Why is this a bug?
The page lacks a properly configured Content Security Policy (CSP) header. Without a CSP, the browser will load resources from any origin, creating significant vulnerabilities. Specifically, the console output indicates mixed content blocking, suggesting an attempt to load a resource over HTTP from a page served over HTTPS. This can be prevented, along with XSS and other injection attacks, by using a strict CSP.

Suggested Fix
Implement a Content Security Policy (CSP) header. Start with a restrictive policy, allowing only resources from trusted origins. For example: `Content-Security-Policy: default-src 'self'; script-src 'self' https://www.pagerduty.com; style-src 'self' https://www.pagerduty.com; img-src 'self' data: https://www.pagerduty.com;`.

Why Fix This?
Implementing a CSP mitigates various risks, including Cross-Site Scripting (XSS) attacks, clickjacking, and other code injection vulnerabilities. It improves the overall security posture of the website.

Route To
Security Engineer/Frontend Engineer

Relevant Network Call

```
N/A
```

Adeela
Mobile Responsive Tester

Missing Top Banner and Countdown Timer on Mobile

Priority: 7/10 Confidence: 9/10

content layout

Why is this a bug?
The top banner displaying "PagerDuty is on tour - join us for a live event!" and the associated countdown timer are present on the large screen but completely missing in the mobile view. This represents a loss of important information for mobile users and suggests a failure in the responsive design to properly handle or relocate this content.

Suggested Fix
Implement responsive design to ensure the banner and countdown timer either scale down appropriately or are relocated to another prominent position on the mobile view. Alternatively, consider a mobile-specific design for this section, ensuring similar information is conveyed.

Why Fix This?
Losing the 'PagerDuty is on tour' banner and timer degrades the user experience for mobile users and may result in missed opportunities to engage with the live event.

Route To
Frontend Engineer

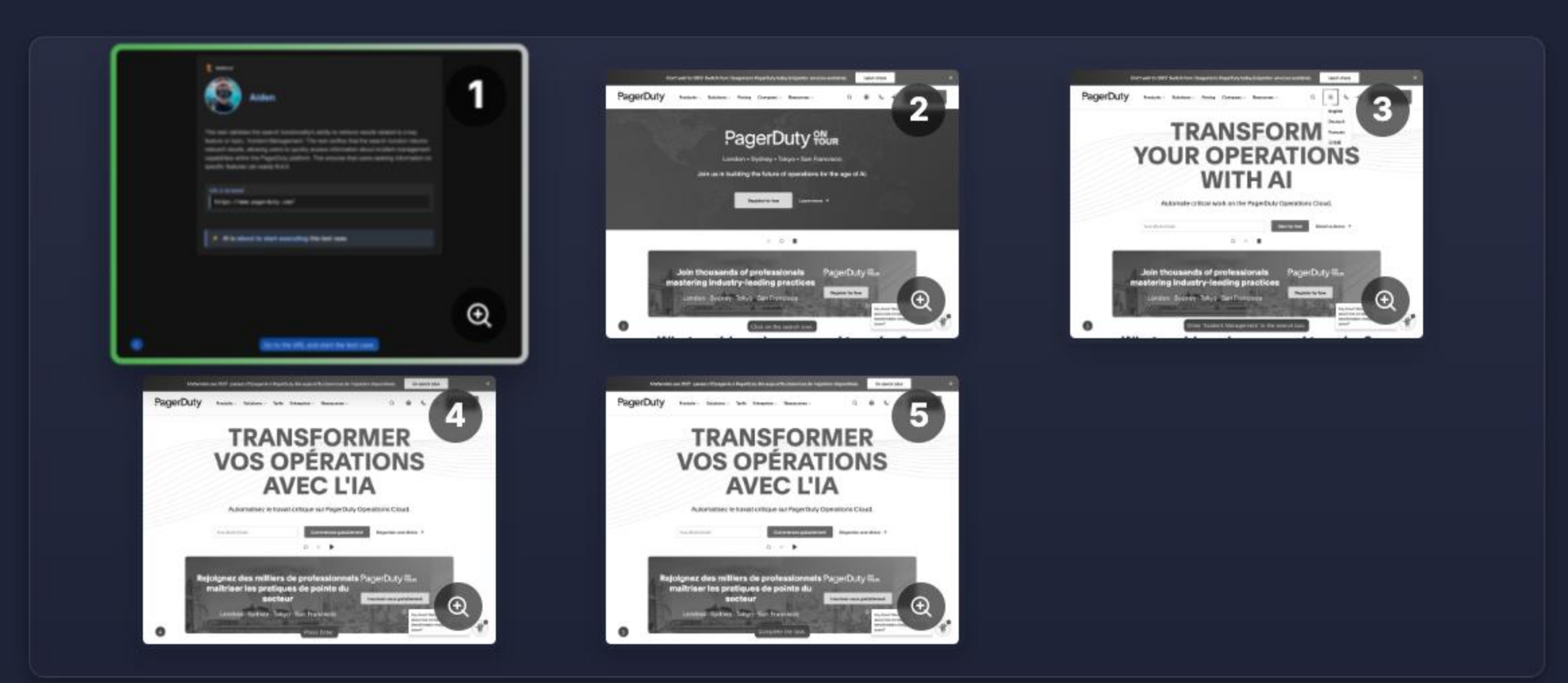
AI Generated Functional Test Results

Start Page: HOME

Aiden
Demo_Tests

✓ Search for 'Incident Management'

This test validates the search functionality's ability to retrieve results related to a key feature or topic, 'Incident Management.' The test verifies that the search function returns relevant results, allowing users to quickly access information about incident management capabilities within the PagerDuty platform. This ensures that users seeking information on specific features can easily find it.



✓ Open Pricing Page from Homepage

This test verifies that the 'Pricing' link in the navigation bar correctly opens the pricing page. It's important to ensure users can easily find and access pricing information. Incorrect routing or a broken link would negatively impact potential customers.

✓ Click See All integrations link

This test verifies that the 'See All integrations link' navigates the user to the appropriate page.

User Persona Feedback Summary

HOME

The primary purpose of the PagerDuty website is to showcase and sell its Operations Cloud platform, which focuses on incident management, automation, and digital operations management.

Overall Score
★★★★☆
The website effectively communicates PagerDuty's value proposition, showcasing its features, customer testimonials, and integration capabilities. The design is modern and engaging, although it could benefit from improved accessibility and clearer calls to action in certain areas.

Visual Design
★★★★☆
The visual design is professional and appealing, but it could benefit from more diverse imagery and better contrast to improve accessibility.

Usability
★★★☆☆
The website is generally easy to navigate, but some users may find the sheer amount of information overwhelming. A more streamlined navigation and clearer calls to action would improve the user experience.

Content Quality
★★★★☆
The content is informative and well-written, showcasing the benefits of PagerDuty's platform. However, some sections could be more concise and focused to better engage the user.

Individual User Persona Feedback

Rajesh Patel, 42

Persona:Rajesh is a DevOps Manager at a mid-sized e-commerce company. He is responsible for ensuring the reliability and performance of the company's infrastructure and applications. He is always looking for ways to improve incident response times and reduce downtime.

Overall Rating
★★★★☆

I'm impressed with the comprehensive features of PagerDuty's incident management platform. The integrations with other DevOps tools are a big plus. However, I'd like to see more detailed documentation and examples of how to integrate with specific tools.

Actions Performed
- Learn more about Incident Management
- Try Incident Management

Suggestions
- Provide more detailed documentation and examples of how to integrate with specific DevOps tools
- Implement a more robust search function to make it easier to find specific information
- Include more detailed use case examples to illustrate the benefits of PagerDuty's platform

Sarah Chen, 30

Persona:Sarah is a Site Reliability Engineer (SRE) at a growing SaaS company. She is responsible for ensuring the availability, performance, and scalability of the company's platform. She is passionate about automation and using technology to solve complex problems.

Overall Rating
★★★★☆

As an SRE, I'm very interested in PagerDuty's automation capabilities. The ability to automate common tasks and remediate incidents automatically is a huge time-saver. I'm particularly impressed with the AI-powered features and the potential to reduce human error.

Actions Performed
- Learn more about Automation
- Try Automation

Suggestions
- Provide more clear and concise technical documentation
- Include more detailed use case examples to illustrate the benefits of PagerDuty's automation platform
- Develop a more robust API to allow for greater integration with other tools

Print Report