Bug Detection

Prepared by: Simran Shaikh  
Role: QA lead   
Date: 06 October 2025  
Project: AB Testing Platform (App.vwo.com)

This document presents a professional-level analysis of potential defects, risk areas, and quality vulnerabilities across the App.vwo.com web application based on the reviewed requirement and test plan documentation. The assessment combines predictive QA insights, experience-based risk evaluation, and requirement traceability analysis to identify likely points of failure before actual execution.

## Login & Authentication

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Functional Area | Potential Defect / Observation | Impact | Category | Risk Level |
| Email Validation | Improper email format accepted without client/server validation. | Incorrect user records, login failures | Functional | Medium |
| Password Policy Enforcement | Weak passwords accepted; missing complexity rules. | Security vulnerability and data breach exposure | Security | High |
| Session Timeout Handling | Session persists after inactivity. | Potential unauthorized access | Security | High |
| Forgot Password Flow | Reset link token not invalidated after use. | Reusability risk, potential account takeover | Security | High |
| Brute Force Mitigation | No account lockout after multiple failed attempts. | Exposure to brute-force attacks | Security | Critical |

## Dashboard Module

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Functional Area | Potential Defect / Observation | Impact | Category | Risk Level |
| Data Accuracy | KPI metrics not updating dynamically post campaign change. | Incorrect business analytics | Functional | High |
| API Performance | Dashboard APIs delay under high load (>5s). | Performance degradation | Performance | High |
| UI Persistence | Sort/filter state resets on refresh. | Workflow interruption | Usability | Medium |
| Cross-Device Responsiveness | Dashboard misaligned on mobile viewports. | Reduced usability on smaller devices | UI | Medium |

## Campaign Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Functional Area | Potential Defect / Observation | Impact | Category | Risk Level |
| Variant Validation | Campaign creation proceeds without all required variants. | Invalid A/B setup | Functional | High |
| Traffic Distribution Logic | Traffic allocation inconsistent with defined ratio. | Incorrect experiment results | Logic | High |
| Campaign Deletion | No delete confirmation modal. | Accidental data loss | Usability | High |
| Duplicate Entry | Rapid multiple clicks on ‘Create’ cause duplication. | DB redundancy, inconsistent reports | Functional | Medium |

## A/B Variant Execution

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Functional Area | Potential Defect / Observation | Impact | Category | Risk Level |
| Visitor Assignment | Same visitor served different variants on reload. | Skewed experiment results | Functional | Critical |
| Tracking Accuracy | Conversion events misattributed to incorrect variant. | Incorrect decision analytics | Data Integrity | High |
| Cookie Persistence | Variant cookie resets upon logout. | User tracking inconsistency | Functional | Medium |

## Conversion Tracking & Reporting

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Functional Area | Potential Defect / Observation | Impact | Category | Risk Level |
| Event Capture | Inconsistent event firing under network delays. | Missing conversion data | Functional | High |
| Duplicate Event Logging | Multiple events logged for single action. | Inflated KPIs, incorrect reporting | Logic | High |
| Data Export | CSV exports missing key columns or timestamps. | Incomplete analytics data | Functional | Medium |

## Security & Compliance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Functional Area | Potential Defect / Observation | Impact | Category | Risk Level |
| SSL/TLS Enforcement | HTTP endpoints still active alongside HTTPS. | Man-in-the-middle vulnerability | Security | Critical |
| Cross-Site Scripting (XSS) | Unescaped user input fields. | JavaScript injection risk | Security | Critical |
| CSRF Tokens | Missing CSRF tokens in key POST requests. | Session hijacking risk | Security | High |
| Cookie Security Flags | Session cookies missing HttpOnly/Secure flags. | Token theft risk | Security | High |

## Performance & Scalability

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Functional Area | Potential Defect / Observation | Impact | Category | Risk Level |
| Concurrent User Load | Application unstable beyond 500 users. | System unavailability | Performance | High |
| DB Optimization | High query response time for reporting. | Slower report generation | Backend | Medium |
| Memory Management | Memory leak during campaign refresh. | Crash risk on prolonged use | Performance | High |

## Usability & Accessibility

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Functional Area | Potential Defect / Observation | Impact | Category | Risk Level |
| Keyboard Navigation | Non-interactive elements receive focus. | Accessibility non-compliance | Accessibility | Medium |
| Color Contrast | Low contrast between chart lines and background. | Poor readability | UI | Low |
| Tooltip Guidance | Missing or unclear tooltips for dashboard metrics. | Increased user confusion | Usability | Medium |

## Defect Risk Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Category | High/Critical | Medium | Low |
| Functional | 9 | 3 | 1 |
| Security | 6 | 0 | 0 |
| Performance | 3 | 1 | 0 |
| Usability/Accessibility | 0 | 3 | 1 |

## Strategic Recommendations

* Implement a formal static code analysis process to catch early functional and security issues.
* Integrate continuous API monitoring and automated regression suite in CI/CD pipelines.
* Enforce OWASP Top 10 compliance with periodic penetration testing.
* Adopt environment parity between staging and production for performance validation.
* Introduce accessibility audits (WCAG 2.1 AA) before every major release.
* Apply performance baselining for concurrent users (>1000) to ensure scalability.
* Introduce risk-based prioritization to testing sprints to ensure focus on high-impact defects.

## Conclusion

Based on predictive analysis and cross-verification with the provided requirement and test strategy documents, critical vulnerabilities predominantly exist in authentication flows, data consistency between campaign modules, and performance stability under load. Addressing these high-priority areas will ensure improved system reliability, data accuracy, and overall user trust in the AB testing ecosystem.