# Code Audit Report

## Redacted iOS Application

**Audit Date:** March 24, 2026

**Audit Tier:** Standard

**Repository:** Redacted Mobile App Repository

**Scope Note:** Project identity, branch, and commit metadata withheld.

**PIXELWRIGHT DIGITAL**

*Security Through Diligence*

Report Version 1.0

# Table of Contents

# Executive Summary

OVERALL RISK RATING

**HIGH**

Risk posture based on identified findings across all severity levels.

## Finding Summary

| CRITICAL | HIGH | MEDIUM |
|---|---|---|
| 0 | 6 | 69 |

| LOW | INFO | TOTAL |
|---|---|---|
| 10 | 0 | 85 |

## Action Priority

| RELEASE BLOCKERS | BEFORE LAUNCH | NEXT SPRINT | BACKLOG |
|---|---|---|---|
| 3 | 5 | 67 | 10 |

This assessment examined the Redacted iOS Application codebase using a combination of automated static-analysis tooling, dependency scanning, and multi-model AI-assisted review to identify security vulnerabilities, code-quality risks, and areas of engineering concern.

The audit identified 0 critical and 6 high-severity findings that warrant prompt attention. The primary risk areas are concentrated in Security (6). Taken together, these findings indicate exploitable weaknesses that could result in unauthorized data access, privilege escalation, or degraded application reliability if left unaddressed.

The most prevalent weakness themes across all severity levels are: Cleartext Storage of Sensitive Information [CWE-312] (5 occurrences); NULL Pointer Dereference [CWE-476] (2 occurrences); CWE-77 [CWE-77] (1 occurrence); CWE-840 [CWE-840] (1 occurrence). Addressing these root-cause patterns systematically will yield the greatest reduction in overall risk surface.

Ship Readiness: This application has 3 release-blocking findings that must be resolved before any production deployment. These represent actively exploitable vulnerabilities or crash-risk conditions. An additional 5 findings

should be addressed before public launch. Pixelwright Digital recommends a focused remediation sprint targeting the release blockers first, followed by the before-launch items.

# Top Findings

### Insecure Storage of Third-Party API Key in UserDefaults

HIGH

Public summary: Insecure Storage of Third-Party API Key in UserDefaults. This public sample represents a validated security finding affecting a production code path.

### Sensitive data stored in UserDefaults. Use Keychain instead.

HIGH

Public summary: Sensitive data stored in UserDefaults. Use Keychain instead.. This public sample represents a validated security finding affecting a production code path.

### Sensitive User Data in Unprotected JSON Files Exposed via Device Backups

MEDIUM

Public summary: Sensitive User Data in Unprotected JSON Files Exposed via Device Backups. This public sample represents a validated security finding affecting a production code path.

See detailed findings section below for complete technical analysis and remediation guidance.

# Findings Overview

The table below provides a consolidated view of all findings identified during this audit, listed by severity. Detailed analysis follows in subsequent sections.

| ID | SEVERITY | PRIORITY | FINDING | CWE | CATEGORY |
|---|---|---|---|---|---|
| PWD-2026-092 | HIGH | RELEASE BLOCKER | Insecure Storage of Third-Party API Key in UserDefaults | CWE-312 | security |
| PWD-2026-093 | HIGH | RELEASE BLOCKER | Sensitive data stored in UserDefaults. Use Keychain instead. | CWE-312 | security |
| PWD-2026-094 | MEDIUM | BEFORE LAUNCH | Sensitive User Data in Unprotected JSON Files Exposed via Device Backups | CWE-312 | security |
| PWD-2026-027 | MEDIUM | BEFORE LAUNCH | Sensitive data stored in UserDefaults. Use Keychain instead. | CWE-312 | security |
| PWD-2026-036 | HIGH | BEFORE LAUNCH | Prompt Injection Via Unsanitized User Content in AI Prompts | CWE-77 | security |

| ID | SEVERITY | PRIORITY | FINDING | CWE | CATEGORY |
|---|---|---|---|---|---|
| PWD-2026-077 | HIGH | BEFORE LAUNCH | Monetization and Quota System Bypassed via User-Accessible "Beta Mode" | CWE-840 | security |
| PWD-2026-078 | HIGH | BEFORE LAUNCH | Subscription Tier and Beta Mode Bypass via UserDefaults Manipulation | CWE-807 | security |
| PWD-2026-023 | MEDIUM | NEXT SPRINT | Force unwrapping should be avoided | CWE-476 | security |

# Scope & Methodology

## What Was Audited

This public sample reflects the structure and depth of a real code audit. Project identity, repository metadata, and implementation-specific evidence have been redacted for external sharing. Full client reports include project-specific references, exact file/line evidence, and any metrics captured during the engagement.

- **Repository:** Redacted Mobile App Repository
- **Audit Tier:** Standard
- **Scan Date:** March 24, 2026
- **Classification:** PUBLIC SAMPLE

## Codebase Metrics

Repository size metrics are intentionally omitted from this public sample to avoid disclosing project scale and internal structure. Full client reports include codebase volume, file counts, and language mix when captured during the assessment.

## Tools & Techniques

The following security analysis tools were used in this audit:

| | |
|---|---|
| scc | v3.7.0 |
| gitleaks | v8.30.0 |
| semgrep | v1.154.0 |
| swiftlint | v0.63.2 |
| trivy | v0.69.3 |

## Methodology

This audit employed a systematic approach to identify security vulnerabilities, code quality issues, and compliance concerns:

- **Static Code Analysis:** Automated scanning for known vulnerabilities and patterns
- **Dependency Analysis:** Identification of vulnerable third-party libraries
- **AI-Assisted Adversarial Review:** Multi-model analysis using large language models to identify cross-module vulnerabilities, architectural risks, and threat vectors not detectable by static tooling alone

- **Automated Scoring & Signal Classification:** Findings are deduplicated, corroborated across tools, and classified by confidence level and signal strength
- **Reference Mapping:** Findings are aligned to published security references such as OWASP guidance, MITRE CWE classifications, and secure-coding practices relevant to the reviewed codebase

## Scope Limitations

- The following tools were not available for this project configuration and their coverage is excluded from this report: binary-analysis, codeql, privacy-manifests.
- The following tools encountered errors during execution: periphery. Related findings may be incomplete.
- Static analysis only: no runtime, dynamic, or penetration testing performed
- Dependency vulnerability data subject to advisory database update timing

**Standard exclusions:** This audit covers static analysis of the source code provided. It does not include: runtime/dynamic analysis, penetration testing, physical device testing, third-party library source code review (only CVE matching), server-side infrastructure, or social engineering assessments. Findings reflect the redacted code snapshot assessed on the date shown above.

# Prioritized Security Findings

This section contains the highest-priority validated security findings selected for the main report body. Lower-priority items are consolidated later under Additional Findings to keep the client-facing report readable.

## High Severity

### Insecure Storage of Third-Party API Key in UserDefaults

HIGH RELEASE BLOCKER PWD-2026-092

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| corroborated | CWE-312 | security |

COMPLIANCE

PCI_DSS_4.0: 3.5.1; HIPAA: 164.312(a)(2)(iv); GDPR: Art.32(1)(a)

LOCATION: `App/Source-07.swift`

DESCRIPTION

Public summary: Insecure Storage of Third-Party API Key in UserDefaults. This public sample represents a validated security finding affecting a production code path.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for near-term remediation because it carries material product or security risk.

REMEDIATION

A targeted security remediation and follow-up verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Sensitive data stored in UserDefaults. Use Keychain instead.

HIGH RELEASE BLOCKER PWD-2026-093

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| corroborated | CWE-312 | security |

COMPLIANCE

PCI_DSS_4.0: 3.5.1; HIPAA: 164.312(a)(2)(iv); GDPR: Art.32(1)(a)

LOCATION: `App/Source-10.swift`

DESCRIPTION

Public summary: Sensitive data stored in UserDefaults. Use Keychain instead.. This public sample represents a validated security finding affecting a production code path.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for near-term remediation because it carries material product or security risk.

REMEDIATION

A targeted security remediation and follow-up verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Prompt Injection Via Unsanitized User Content in AI Prompts

HIGH BEFORE LAUNCH PWD-2026-036

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| ai-assisted | CWE-77 | security |

LOCATION: `App/Source-01.swift`

DESCRIPTION

Public summary: Prompt Injection Via Unsanitized User Content in AI Prompts. This public sample represents a validated security finding affecting a production code path.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for near-term remediation because it carries material product or security risk.

REMEDIATION

A targeted security remediation and follow-up verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Monetization and Quota System Bypassed via User-Accessible "Beta Mode"

HIGH BEFORE LAUNCH PWD-2026-077

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| ai-assisted | CWE-840 | security |

LOCATION: `App/Source-14.swift`

DESCRIPTION

Public summary: Monetization and Quota System Bypassed via User-Accessible "Beta Mode". This public sample represents a validated security finding affecting a production code path.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for near-term remediation because it carries material product or security risk.

REMEDIATION

A targeted security remediation and follow-up verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Subscription Tier and Beta Mode Bypass via UserDefaults Manipulation

HIGH BEFORE LAUNCH PWD-2026-078

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| ai-assisted | CWE-807 | security |

LOCATION: `App/Source-14.swift`

DESCRIPTION

Public summary: Subscription Tier and Beta Mode Bypass via UserDefaults Manipulation. This public sample represents a validated security finding affecting a production code path.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for near-term remediation because it carries material product or security risk.

REMEDIATION

A targeted security remediation and follow-up verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Medium Severity

### Sensitive User Data in Unprotected JSON Files Exposed via Device Backups

MEDIUM BEFORE LAUNCH PWD-2026-094

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| corroborated | CWE-312 | security |

COMPLIANCE

PCI_DSS_4.0: 3.5.1; HIPAA: 164.312(a)(2)(iv); GDPR: Art.32(1)(a)

---

LOCATION: `App/Source-03.swift`

DESCRIPTION

Public summary: Sensitive User Data in Unprotected JSON Files Exposed via Device Backups. This public sample represents a validated security finding affecting a production code path.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted security remediation and follow-up verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Sensitive data stored in UserDefaults. Use Keychain instead.

**MEDIUM** **BEFORE LAUNCH** PWD-2026-027

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| corroborated | CWE-312 | security |

COMPLIANCE

PCI_DSS_4.0: 3.5.1; HIPAA: 164.312(a)(2)(iv); GDPR: Art.32(1)(a)

---

LOCATION: `App/Source-10.swift`

DESCRIPTION

Public summary: Sensitive data stored in UserDefaults. Use Keychain instead.. This public sample represents a validated security finding affecting a production code path.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted security remediation and follow-up verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Force unwrapping should be avoided

**MEDIUM** **NEXT SPRINT** PWD-2026-023

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| tool | CWE-476 | security |

LOCATION: `App/Source-07.swift`

DESCRIPTION

Public summary: Force unwrapping should be avoided. This public sample represents a validated security finding affecting a production code path.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted security remediation and follow-up verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

# Remediation Roadmap

The following prioritized remediation roadmap groups findings by urgency band — the action timeline that matters for your release schedule.

## Release Blockers — Fix Before Any Deploy

**Insecure Storage of Third-Party API Key in UserDefaults**

0.5 hrs

Public summary: Insecure Storage of Third-Party API Key in UserDefaults. This public sample represents a validated security finding affecting a...

**Sensitive data stored in UserDefaults. Use Keychain instead.**

0.5 hrs

Public summary: Sensitive data stored in UserDefaults. Use Keychain instead.. This public sample represents a validated security finding affecting...

## Before Launch — Fix Before Public Release

**Sensitive User Data in Unprotected JSON Files Exposed via Device Backups**

0.5 hrs

Public summary: Sensitive User Data in Unprotected JSON Files Exposed via Device Backups. This public sample represents a validated security...

**Sensitive data stored in UserDefaults. Use Keychain instead.**

0.5 hrs

Public summary: Sensitive data stored in UserDefaults. Use Keychain instead.. This public sample represents a validated security finding affecting...

### Prompt Injection Via Unsanitized User Content in AI Prompts

2.0 hrs

Public summary: Prompt Injection Via Unsanitized User Content in AI Prompts. This public sample represents a validated security finding affecting...

### Monetization and Quota System Bypassed via User-Accessible "Beta Mode"

2.0 hrs

Public summary: Monetization and Quota System Bypassed via User-Accessible "Beta Mode". This public sample represents a validated security finding...

### Subscription Tier and Beta Mode Bypass via UserDefaults Manipulation

2.0 hrs

Public summary: Subscription Tier and Beta Mode Bypass via UserDefaults Manipulation. This public sample represents a validated security finding...

## Next Sprint — Plan for Next Dev Cycle

1 finding to address in the next development cycle. See the appendix for details on lower-priority items.

## Backlog — Track for Future Improvement

No backlog items identified.

# Conclusions

### Overall Assessment

This standard code audit of **Redacted iOS Application** identified **85** findings across the scanned codebase. The main report body highlights **8** prioritized items, while **20** additional items are grouped separately for follow-up planning. The **6 high-severity findings** should be remediated as a priority to reduce the attack surface.

## Immediate Actions Required

We strongly recommend addressing all critical and high-severity findings before the next production release. These findings represent exploitable vulnerabilities or significant security weaknesses that could lead to data breaches, unauthorized access, or service disruption.

## Positive Observations

- App Transport Security enforced (no NSAllowsArbitraryLoads)
- Biometric authentication uses proper Keychain binding (not boolean-only)

- Keychain access controls follow best practices (no kSecAttrAccessibleAlways)
- No deprecated cryptographic algorithms detected (MD5/SHA-1)

### Next Steps

- Review and prioritize findings using the Remediation Roadmap in this report
- Address all critical and high-severity findings within the recommended timeframes
- Schedule a follow-up verification review after remediation is complete
- Consider a remediation engagement with Pixelwright Digital for guided resolution

## Optional Remediation Support

---

If requested, Pixelwright Digital can scope and implement follow-up remediation work based on the findings in this report. The audit remains a standalone assessment deliverable; remediation is handled as a separate engagement with its own scope, pricing, and acceptance criteria.

## Typical Support Workflow

STEP 1

### Scope & Prioritize

Confirm which findings will be addressed first, define success criteria, and map the work to the client's release schedule.

STEP 2

### Implement & Review

Implement the agreed remediation changes, document material decisions, and review the resulting code for correctness and side effects.

STEP 3

### Verify & Document

Re-run the relevant checks, confirm the agreed findings were addressed, and provide a verification summary for the completed scope.

## Typical Deliverables

- ✓ **Remediation branch or patch set** for the findings included in the agreed scope
- ✓ **Verification summary** describing what was re-checked and what was resolved
- ✓ **Regression coverage updates** where tests are part of the agreed remediation scope
- ✓ **CI or scanning workflow updates** when automation changes are part of scope
- ✓ **Change log and delivery notes** summarizing the completed remediation work

**SAMPLE PROPOSAL AVAILABLE**

This public sample includes a separate remediation proposal that illustrates how prioritized findings can be scoped into implementation work.

# Additional Findings

The following 20 findings are lower-priority items (next-sprint or backlog) that did not meet the threshold for the main report body. They are included for completeness, while implementation-specific evidence and working artifacts remain redacted in the public sample.

### Force try crashes on any error. Use do-catch or try? in production code. (12 occurrences)

MEDIUM NEXT SPRINT PWD-2026-010

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| corroborated | CWE-755 | crash_risk |

LOCATION: App/Source-03.swift

DESCRIPTION

Public summary: Force try crashes on any error. Use do-catch or try? in production code.. This public sample represents a validated runtime-stability issue that can lead to crashes or undefined behavior.

AFFECTED FILES (12)

```
App/Source-03.swift
App/Source-01.swift
App/Source-04.swift
App/Source-07.swift
App/Source-08.swift
App/Source-09.swift
App/Source-10.swift
App/Source-11.swift
App/Source-12.swift
```

App/Source-13.swift
App/Source-14.swift
App/Source-17.swift

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted stability fix and regression test pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## DataStore Silently Swallows Persistence Errors Causing Silent Data Loss

**MEDIUM** **NEXT SPRINT** PWD-2026-011

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| corroborated | CWE-755 | data_integrity |

LOCATION: App/Source-03.swift

DESCRIPTION

Public summary: DataStore Silently Swallows Persistence Errors Causing Silent Data Loss. This public sample represents a validated data-integrity issue that can corrupt, lose, or mis-handle application state.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted data-handling correction and verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## File should contain 500 lines or less: currently contains 554

**MEDIUM** **NEXT SPRINT** PWD-2026-037

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-01.swift`

DESCRIPTION

Public summary: File should contain 500 lines or less: currently contains 554. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Function body should span 50 lines or less excluding comments and whitespace: currently spans 55 lin

**MEDIUM** **NEXT SPRINT** PWD-2026-040

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | maintainability |

LOCATION: `App/Source-02.swift`

DESCRIPTION

Public summary: Function body should span 50 lines or less excluding comments and whitespace: currently spans 55 lin. This public sample represents a validated maintainability issue that can slow remediation and increase defect risk.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A focused cleanup pass and verification review were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## File should contain 500 lines or less: currently contains 565

**MEDIUM** **NEXT SPRINT** PWD-2026-041

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-02.swift`

DESCRIPTION

Public summary: File should contain 500 lines or less: currently contains 565. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Class body should span 300 lines or less excluding comments and whitespace: currently spans 339 line

**MEDIUM** **NEXT SPRINT** PWD-2026-042

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-03.swift`

DESCRIPTION

Public summary: Class body should span 300 lines or less excluding comments and whitespace: currently spans 339 line. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Function body should span 50 lines or less excluding comments and whitespace: currently spans 51 lin

**MEDIUM** **NEXT SPRINT** PWD-2026-044

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| tool | N/A | maintainability |

LOCATION: `App/Source-03.swift`

DESCRIPTION

Public summary: Function body should span 50 lines or less excluding comments and whitespace: currently spans 51 lin. This public sample represents a validated maintainability issue that can slow remediation and increase defect risk.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A focused cleanup pass and verification review were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## File should contain 500 lines or less: currently contains 518

**MEDIUM** **NEXT SPRINT** PWD-2026-045

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-03.swift`

DESCRIPTION

Public summary: File should contain 500 lines or less: currently contains 518. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Struct body should span 300 lines or less excluding comments and whitespace: currently spans 319 lin

**MEDIUM** **NEXT SPRINT** PWD-2026-047

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-07.swift`

DESCRIPTION

Public summary: Struct body should span 300 lines or less excluding comments and whitespace: currently spans 319 lin. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## File should contain 500 lines or less: currently contains 622

**MEDIUM** **NEXT SPRINT** PWD-2026-050

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-07.swift`

DESCRIPTION

Public summary: File should contain 500 lines or less: currently contains 622. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Struct body should span 500 lines or less excluding comments and whitespace: currently spans 604 lin

**MEDIUM** **NEXT SPRINT** PWD-2026-081

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-15.swift`

DESCRIPTION

Public summary: Struct body should span 500 lines or less excluding comments and whitespace: currently spans 604 lin. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## File should contain 1000 lines or less: currently contains 1267

**MEDIUM** **NEXT SPRINT** PWD-2026-083

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-15.swift`

DESCRIPTION

Public summary: File should contain 1000 lines or less: currently contains 1267. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Struct body should span 300 lines or less excluding comments and whitespace: currently spans 363 lin

**MEDIUM** **NEXT SPRINT** PWD-2026-085

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-17.swift`

DESCRIPTION

Public summary: Struct body should span 300 lines or less excluding comments and whitespace: currently spans 363 lin. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Optional should be implicitly initialized without nil

**MEDIUM** **NEXT SPRINT** PWD-2026-087

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | crash_risk |

LOCATION: `App/Source-17.swift`

DESCRIPTION

Public summary: Optional should be implicitly initialized without nil. This public sample represents a validated runtime-stability issue that can lead to crashes or undefined behavior.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted stability fix and regression test pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## File should contain 1000 lines or less: currently contains 1050

**MEDIUM** **NEXT SPRINT** PWD-2026-088

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-17.swift`

DESCRIPTION

Public summary: File should contain 1000 lines or less: currently contains 1050. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Struct body should span 300 lines or less excluding comments and whitespace: currently spans 427 lin

**MEDIUM** **NEXT SPRINT** PWD-2026-089

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-18.swift`

DESCRIPTION

Public summary: Struct body should span 300 lines or less excluding comments and whitespace: currently spans 427 lin. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## File should contain 500 lines or less: currently contains 669

**MEDIUM** **NEXT SPRINT** PWD-2026-091

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| tool | N/A | code_quality |

LOCATION: `App/Source-18.swift`

DESCRIPTION

Public summary: File should contain 500 lines or less: currently contains 669. This public sample represents a validated code-quality concern that can create maintainability or correctness risk over time.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was prioritized for scheduled remediation as part of normal hardening work.

REMEDIATION

A targeted refactor or guard-rail change was recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

### Force try crashes on any error. Use do-catch or try? in production code. (5 occurrences)

LOW BACKLOG PWD-2026-001

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| corroborated | CWE-755 | crash_risk |

LOCATION: `App/Source-01.swift`

DESCRIPTION

Public summary: Force try crashes on any error. Use do-catch or try? in production code.. This public sample represents a validated runtime-stability issue that can lead to crashes or undefined behavior.

AFFECTED FILES (5)

```
App/Source-01.swift
App/Source-02.swift
App/Source-04.swift
App/Source-05.swift
App/Source-10.swift
```

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was recorded for backlog hardening and follow-up engineering cleanup.

REMEDIATION

A targeted stability fix and regression test pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

### Force unwrap is a crash risk in production. Use optional binding or nil coalescing. (2 occurrences)

LOW BACKLOG PWD-2026-009

| CONFIDENCE | CWE ID | CATEGORY |
|---|---|---|
| corroborated | CWE-476 | crash_risk |

LOCATION: App/Source-03.swift

DESCRIPTION

Public summary: Force unwrap is a crash risk in production. Use optional binding or nil coalescing.. This public sample represents a validated runtime-stability issue that can lead to crashes or undefined behavior.

AFFECTED FILES (2)

```
App/Source-03.swift
App/Source-07.swift
```

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was recorded for backlog hardening and follow-up engineering cleanup.

REMEDIATION

A targeted stability fix and regression test pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

## Sensitive Data Stored in UserDefaults

LOW BACKLOG PWD-2026-034

| CONFIDENCE | CWE ID | CATEGORY |
| --- | --- | --- |
| tool | CWE-921 | security |

COMPLIANCE

PCI_DSS_4.0: 3.5.1, 3.6.1; HIPAA: 164.312(a)(1); GDPR: Art.32(1)(b)

LOCATION: `Docs/Document-01.md`

DESCRIPTION

Public summary: Sensitive Data Stored in UserDefaults. This public sample represents a validated security finding affecting a production code path.

TECHNICAL DETAIL

Technical implementation details redacted in public sample.

IMPACT

This issue was recorded for backlog hardening and follow-up engineering cleanup.

REMEDIATION

A targeted security remediation and follow-up verification pass were recommended. Detailed implementation steps are withheld in this public sample.

VERIFICATION

Follow-up verification and regression review were part of the original engagement. Detailed verification notes are withheld in this public sample.

VERIFICATION EVIDENCE

Corroborating evidence redacted in public sample.

# Appendix

## Tools & Versions

| | |
|---|---|
| scc | v3.7.0 |
| gitleaks | v8.30.0 |
| semgrep | v1.154.0 |
| swiftlint | v0.63.2 |
| trivy | v0.69.3 |

## Severity Classification

| SEVERITY | DESCRIPTION |
| --- | --- |
| CRITICAL | Immediate exploitation likely; severe business impact |
| HIGH | Exploitation probable; significant business impact |
| MEDIUM | Exploitation possible; moderate business impact |
| LOW | Limited exploitation likelihood; minimal business impact |
| INFO | Informational; no security risk but worth noting |

## Methodology References

- **OWASP Top 10:** https://owasp.org/www-project-top-ten/
- **CWE/SANS:** https://cwe.mitre.org/
- **NIST SP 800-115:** https://csrc.nist.gov/pubs/sp/800/115/final

## Disclaimer

This audit report represents the findings and analysis conducted as of the date specified. The identified findings represent security issues discovered through a combination of automated static analysis tools, AI-assisted adversarial review, and automated scoring with signal classification. AI-powered large language models are used as part of our analysis methodology to augment — not replace — professional security assessment. Findings included in any client-delivered final report must be reviewed against the available evidence before publication.

No point-in-time assessment can guarantee identification of every issue. Items outside the stated scope, changes made after the assessment date, runtime-only conditions, and environment-specific behaviors may introduce additional risk not reflected in this report. This public sample has been redacted for portfolio and marketing use. Project identity, repository metadata, and proprietary implementation details have been intentionally withheld.